Protection des données personnelles
Référentiel légal et réglementaire

Tome 2

Lignes directrices et avis du CEPD (anciennement G29)

publiés en complément
du Règlement (UE) 2016/679
du Parlement européen et du Conseil
du 27 avril 2016

AFCDP
Association Française
des Correspondants à la protection
des Données à caractère Personnel

Chers amis, chers adhérents,

Après vous avoir proposé le RGPD en version indexée et annotée, l'association qui regroupe et représente les DPO est fière de mettre à votre disposition les lignes directrices du Comité européen de la protection des données. Plusieurs d'entre elles sont issues des travaux du G29, que le CEPD a remplacé.

Ces textes sont particulièrement importants pour tout Délégué à la protection des données, car ils apportent des clarifications et précisions précieuses. L'AFCDP, qui a fait entendre au niveau européen la voix des professionnels concernés dès 2012, est fière de retrouver dans plusieurs de ces lignes directrices des suggestions qu'elle a formulées à l'occasion des appels à contributions.

Ce fascicule constitue donc le deuxième tome (le premier étant consacré au RGPD) d'une série.

Un troisième tome comprendra le « Code de la donnée » issu de la réécriture de la loi Informatique et Libertés par ordonnance, et les principaux décrets d'application.

Ce tome, enrichi d'un index, a été préparé par Bruno Rasle (Délégué général de l'AFCDP) et par moi-même. Les fautes sont nôtres… mais merci d'avance de nous aider à les corriger en nous les signalant par simple courriel.

Confraternellement.

Patrick BLUM
Vice-président de l'AFCDP, Animateur de la Commission " Métier "
DPO et RSSI de l'ESSEC

AFCDP
Association Française des Correspondants à la protection des Données à caractère Personnel

TABLE DES MATIÈRES

Commentaires

Dès juin 2016, l'AFCDP a mis à disposition une version annotée, commentée et indexée du RGPD (tome 1).

Le présent document, réalisée à l'attention des Membres de l'AFCDP, vient la compléter et constitue le tome 2.

Il regroupe les « lignes directrices » publiées par le CEPD (anciennement G29) en complément du RGPD.

Ce tome est assorti d'un index.

Ce document est un guide pratique destiné aux adhérents de l'AFCDP. Il ne constitue pas une référence légale.

Vous avez remarqué une erreur ou une correction à apporter ?
Merci de nous aider à améliorer ce document, par courriel adressé à delegue.general@afcdp.net

Les autres ressources de l'AFCDP

L'AFCDP met également diverses ressources à la disposition des professionnels :

- un « job board » dédié aux professionnels de la conformité au RGPD

- un modèle de fiche de poste de DPD

- un modèle de lettre de mission de DPD

- une Charte de déontologie du DPD

- une place de marché RGPD

- une lettre de veille mensuelle et gratuite, "L'Actualité des données personnelles"

Ces ressources sont accessibles sur le site Web de l'AFCDP : www.afcdp.net

Les lignes directrices du CEPD (anciennement G29)

Le CEPD (Comité européen de la protection des données) est le comité créé par l'article 68 du Règlement général sur la protection des données, ou plus précisément Règlement 2016/679 du Parlement et du Conseil européens du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD). Il s'agit d'un organe indépendant de l'Union européenne dédié essentiellement à l'application cohérente du RGPD. Il est composé des représentants de chacune des autorités de contrôle de pays membres de l'Union européenne (la CNIL en France) et du Contrôleur européen de la protection des données. Ses missions et son mode de fonctionnement sont décrits aux article 70 à 76 du RGPD.

Périodiquement, le CEPD publie des opinions et des lignes directrices concernant l'application des textes européens relatifs à la protection des données.

Depuis l'adoption définitive du RGPD, le CEPD publie diverses lignes directrices destinées à accompagner ou compléter le règlement.

Ces lignes directrices constituent l'analyse du CEPD, et ne reflètent pas l'opinion de la Commission européenne.

Depuis l'entrée en application du RGPD le 25 mai 2018, le CEPD remplace le G29 qui avait été institué par la Directive 95/46/CE.

Compte tenu de l'importance des lignes directrices du CEPD dans la compréhension et l'analyse du RGPD, nous avons décidé de réunir ces documents dans un volume spécifique de notre édition du Règlement.

Ces documents font généralement l'objet d'une publication par étapes : une première version est adoptée par le CEPD, en anglais uniquement. Elle est alors soumise à un appel public à commentaires. À l'issue de la consultation, une version définitive est adoptée par le CEPD, toujours en anglais. Il faut ensuite attendre un certain temps avant la publication des traductions dans toutes les langues de l'Union.

Nous avons donc pris le parti de publier ici les Lignes directrices dans leur version disponible à la date d'édition du présent volume.

Pour l'AFCDP,
L'équipe de publication

Avis sur les notions de « responsables du traitement » et de « sous-traitant » (WP169)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

00264/10/FR
WP 169

Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant»

Adopté le 16 février 2010

Ce groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Son secrétariat est assuré par la direction D (Droits fondamentaux et citoyenneté) de la direction générale «Justice, liberté et sécurité» de la Commission européenne, B-1049 Bruxelles, Belgique, bureau LX-46 01/190.

Site: http://ec.europa.eu/justice_home/fsj/privacy/index_fr.htm

TABLE DES MATIÈRES

Résumé

La notion de responsable du traitement des données et son interaction avec la notion de sous-traitant des données jouent un rôle central dans l'application de la directive 95/46/CE, car elles déterminent la ou les personnes chargées de faire respecter les règles de protection des données, la manière dont les personnes concernées peuvent exercer leurs droits, le droit national applicable, et le degré d'efficacité des autorités chargées de la protection des données.

Les modes d'organisation différenciés dans les secteurs public et privé, le développement des TIC ainsi que la mondialisation du traitement des données rendent plus complexe le traitement des données à caractère personnel et appellent à préciser ces notions, pour garantir la bonne application et le respect de la directive dans la pratique.

La notion de responsable du traitement est autonome, en ce sens que son interprétation relève principalement de la législation européenne sur la protection des données, et fonctionnelle, car elle vise à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle repose par conséquent sur une analyse factuelle plutôt que formelle.

La définition énoncée dans la directive s'articule en trois volets:
- l'aspect individuel («*la personne physique ou morale, l'autorité publique, le service ou tout autre organisme*»);
- la possibilité d'une responsabilité pluraliste («*qui seul ou conjointement avec d'autres*»); et
- les éléments essentiels qui permettent de distinguer le responsable du traitement des autres acteurs («*détermine les finalités et les moyens du traitement de données à caractère personnel*»).

L'analyse de ces volets conduit à plusieurs conclusions, résumées au point IV de l'avis.

Le présent avis analyse également la notion de sous-traitant, dont l'existence dépend d'une décision prise par le responsable du traitement, lequel peut choisir de traiter les données au sein de son organisation ou de déléguer tout ou partie des activités de traitement à une organisation extérieure. Pour agir en qualité de sous-traitant, il convient, d'une part, d'être une personne morale distincte du responsable du traitement et, d'autre part, de traiter les données à caractère personnel pour le compte de ce dernier.

Le groupe de travail reconnaît la difficulté d'appliquer les définitions de la directive dans un environnement complexe, qui permet d'envisager maints scénarios faisant intervenir des responsables du traitement et des sous-traitants, seuls ou conjointement avec d'autres, avec différents degrés d'autonomie et de responsabilité.

Dans son analyse, il souligne la nécessité d'attribuer les responsabilités de sorte à garantir comme il se doit le respect des règles de protection des données dans la pratique. Il estime cependant n'avoir aucune raison de penser que la distinction actuelle entre responsables du traitement et sous-traitants n'est plus pertinente ni réaliste dans cette perspective.

Par conséquent, le groupe de travail espère que les explications figurant dans le présent avis, illustrées par des exemples concrets tirés de l'expérience quotidienne des autorités chargées de la protection des données, donneront des indications utiles pour l'interprétation de ces définitions fondamentales de la directive.

1

Le groupe de travail sur la protection des personnes à l'égard du traitement des données à caractère personnel

établi par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu l'article 29 et l'article 30, paragraphe 1, point a), et paragraphe 3, de ladite directive, et l'article 15, paragraphe 3, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002,

vu son règlement intérieur,

a adopté l'avis suivant:

I. Introduction

La notion de responsable du traitement des données et son interaction avec la notion de sous-traitant des données jouent un rôle central dans l'application de la directive 95/46/CE, car elles déterminent la ou les personnes chargées de faire respecter les règles en matière de protection des données et la manière dont les personnes concernées peuvent exercer leurs droits dans la pratique. Cette notion est également essentielle pour déterminer le droit national applicable et assurer la bonne exécution des missions de contrôle confiées aux autorités chargées de la protection des données.

Il est donc capital que le sens précis de ces notions et que les critères assurant leur utilisation correcte soient suffisamment clairs et partagés par tous ceux qui, dans les États membres, participent à la mise en œuvre de la directive et à l'application, à l'évaluation et à l'exécution des dispositions nationales qui la transposent.

Or il semble que cette clarté fasse défaut, du moins en ce qui concerne certains aspects de ces notions, et que des divergences de vue entre les praticiens de divers États membres puissent donner lieu à différentes interprétations des principes et définitions identiques introduits pour parvenir à une harmonisation au niveau européen. C'est la raison pour laquelle le Groupe de travail «Article 29» (ci-après, «le groupe de travail») a décidé, dans le cadre de son programme de travail stratégique 2008-2009, de se consacrer à l'élaboration d'un document exposant une approche commune de ces questions.

Le groupe de travail reconnaît que l'application concrète des notions de responsable du traitement et de sous-traitant pose de plus en plus de difficultés, principalement du fait de la complexité croissante de l'environnement dans lequel ces notions sont utilisées, et en particulier d'une tendance de plus en plus nette, tant dans le secteur privé que le secteur public, à la différenciation organisationnelle, associée au développement des TIC et à la mondialisation, au point de pouvoir créer de nouveaux problèmes et d'aboutir parfois à l'affaiblissement de la protection des personnes concernées.

Si les dispositions de la directive ont été formulées en termes neutres du point de vue technique et ont, jusqu'à présent, bien résisté aux évolutions, ces difficultés risquent fort de rendre incertains l'attribution des responsabilités et le champ d'application des législations nationales applicables. Ces incertitudes pourraient compromettre le respect des règles de protection des données dans des domaines essentiels, ainsi que l'efficacité de la législation sur la protection des données dans son ensemble. Le groupe de travail a

certes déjà examiné certains de ces aspects dans le cadre de questions concrètes[1], mais il estime à présent nécessaire de donner des orientations plus détaillées et des recommandations bien précises afin de garantir une approche cohérente et harmonisée.

Par conséquent, dans le présent avis, le groupe de travail a décidé (comme il l'avait fait dans son avis sur le concept des données à caractère personnel[2]) de préciser et d'illustrer par des exemples concrets[3] les notions de responsable du traitement et de sous-traitant.

II. Observations générales et principaux enjeux

La directive renvoie explicitement à la notion de responsable du traitement dans plusieurs de ses dispositions. Les définitions de «responsable du traitement» et de «sous-traitant» énoncées à l'article 2, points d) et e), de la directive 95/46/CE (ci-après «la directive») sont libellées comme suit:

> *On entend par «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire;*
>
> *Par «sous-traitant», on entend la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.*

Ces définitions ont été rédigées pendant les négociations sur le projet de proposition de directive, au début des années 90, et la notion de «responsable du traitement» a été essentiellement reprise de la convention 108 du Conseil de l'Europe conclue en 1981. Des changements importants ont été apportés pendant ces négociations.

En premier lieu, le terme «maître du fichier» employé dans la convention 108 a été remplacé par «responsable du traitement» en ce qui concerne le «traitement de données à caractère personnel». Il s'agit d'une notion large, que l'article 2, point b), de la directive définit comme «toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction». Ainsi, la notion de «responsable du traitement» n'était plus associée à un objet statique («le fichier») mais à des activités illustrant le cycle de vie de l'information, de la collecte à la

1 Voir par exemple l'Avis 10/2006 sur le traitement des données à caractère personnel par la Society for Worldwide Interbank Financial Telecommunication (SWIFT), adopté le 22 novembre 2006 (WP 128), et plus récemment l'Avis 5/2009 sur les réseaux sociaux en ligne, adopté le 12 juin 2009 (WP 163).

2 Avis 4/2007 sur le concept des données à caractère personnel, adopté le 20 juin 2007 (WP 136)

3 Ces exemples sont tirés de cas pratiques nationaux ou européens actuels et sont susceptibles d'avoir été modifiés ou adaptés dans un souci de clarté.

destruction, et cet aspect devait être envisagé à la fois dans le détail et dans sa globalité («opération ou ensemble d'opérations»). Même si le résultat aurait sans doute été le même dans de nombreux cas, la notion a de ce fait acquis un sens et une portée bien plus larges et plus dynamiques.

D'autres modifications ont introduit la possibilité d'une «responsabilité pluraliste» («seul ou conjointement avec d'autres»), l'obligation pour le responsable du traitement de «déterminer les finalités et les moyens du traitement de données à caractère personnel», et l'idée selon laquelle cette détermination peut être fixée par le droit national ou communautaire ou d'une autre façon. La directive a en outre créé la notion de «sous-traitant», qui ne figurait pas dans la convention 108. Ces adaptations ainsi que d'autres évolutions seront étudiées plus en détail ci-après.

II.1. Rôle des notions

Si la notion de responsable du traitement (maître du fichier) jouait un rôle très limité[4] dans la convention 108, il en est tout autrement dans la directive. L'article 6, paragraphe 2, prévoit explicitement qu'«il incombe au responsable du traitement d'assurer le respect du paragraphe 1». Cette disposition renvoie aux principes généraux concernant la qualité des données, notamment celui prévu à l'article 6, paragraphe 1, point a), selon lequel «les données à caractère personnel doivent être traitées loyalement et licitement». Ce qui signifie en pratique que toutes les dispositions établissant des conditions d'un traitement licite visent essentiellement le responsable du traitement, même si ce n'est pas toujours clairement indiqué.

En outre, les dispositions relatives aux droits de la personne concernée, à savoir le droit d'information, d'accès, de rectification, d'effacement, de verrouillage et d'opposition au traitement de données à caractère personnel (articles 10 à 12 et article 14), ont été formulées de telle sorte qu'elles créent des obligations pour le responsable du traitement. Ce dernier occupe également une place centrale dans les dispositions consacrées à la notification et aux contrôles préalables (articles 18 à 21). Enfin, il n'est pas surprenant que le responsable du traitement soit également tenu pour responsable, en principe, de tout dommage consécutif à un traitement illicite (article 23).

Ainsi, le rôle premier de la notion de responsable du traitement est de déterminer qui est chargé de faire respecter les règles de protection des données, et comment les personnes concernées peuvent exercer leurs droits dans la pratique.[5] En d'autres termes, il s'agit d'attribuer les responsabilités.

Ce qui nous renvoie au cœur de la directive, son objectif principal étant de «protéger les personnes physiques à l'égard du traitement des données à caractère personnel». Cet objectif ne peut être réalisé et mis en pratique que si les personnes chargées du traitement

[4] Elle n'est citée dans aucune des dispositions de fond, excepté à l'article 8.a., concernant le droit d'être informé (principe de transparence). La notion de maître du fichier en tant que tiers responsable n'apparaît que dans certaines parties du rapport explicatif.

[5] Voir également le considérant 25 de la directive 95/46/CE: *«Considérant que les principes de la protection doivent trouver leur expression, d'une part, dans les obligations mises à la charge des personnes, autorités publiques, entreprises, agences ou autres organismes qui traitent des données, ces obligations concernant en particulier la qualité des données, la sécurité technique, la notification à l'autorité de contrôle, les circonstances dans lesquelles le traitement peut être effectué, et, d'autre part, dans les droits donnés aux personnes dont les données font l'objet d'un traitement d'être informées sur celui-ci, de pouvoir accéder aux données, de pouvoir demander leur rectification, voire de s'opposer au traitement dans certaines circonstances».*

des données sont suffisamment incitées par des dispositifs juridiques et d'autres moyens à prendre toutes les mesures nécessaires pour garantir que cette protection soit effective. Ce point est confirmé par l'article 17, paragraphe 1, de la directive, aux termes duquel le responsable du traitement «*doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite*.»

Les mesures destinées à favoriser la responsabilité peuvent être de nature proactive et réactive. Dans le premier cas, elles visent à garantir la bonne application des mesures de protection des données et des moyens suffisants pour obliger les responsables du traitement à rendre des comptes. Dans le second cas, elles peuvent prévoir une responsabilité civile et des sanctions, de sorte que tout dommage soit réparé et que des mesures appropriées soient prises pour corriger toute erreur ou tout comportement illicite.

La notion de responsable du traitement joue également un rôle essentiel pour déterminer le droit national applicable à une opération de traitement ou à un ensemble d'opérations de traitement. La principale règle concernant le droit applicable, aux termes de l'article 4, paragraphe 1, point a), de la directive est que chaque État membre applique ses dispositions nationales aux «*traitements de données à caractère personnel, lorsque (...) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre*». Cette disposition poursuit de la manière suivante: «*si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable*». Ce qui signifie que le ou les établissements du responsable du traitement déterminent également le ou les droits nationaux applicables, et éventuellement un certain nombre de droits nationaux applicables ainsi que les relations entre ces derniers.[6]

Enfin, il convient de noter que, dans de nombreuses dispositions de la directive, la notion de responsable du traitement est un élément de leur champ d'application ou d'une condition particulière applicable en vertu de ces dispositions. Ainsi, l'article 7 dispose que le traitement de données à caractère personnel ne peut être effectué que si: «*(c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, (e) il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou (f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt …*». L'identité du responsable du traitement est également un aspect important de l'information de la personne concernée, imposée par les articles 10 et 11.

La notion de «sous-traitant» joue un rôle déterminant dans le cadre de la confidentialité et de la sécurité des traitements (articles 16 et 17), puisqu'elle a pour effet de déterminer

[6] Le groupe de travail prévoit d'adopter un avis distinct sur la notion de «droit applicable» courant 2010. Lorsque les institutions et organes de l'Union européenne traitent des données à caractère personnel, il est également nécessaire de déterminer le responsable du traitement eu égard à l'application potentielle du règlement (CE) 45/2001 ou d'autres instruments juridiques pertinents de l'Union européenne.

les obligations des personnes qui interviennent plus directement dans le traitement des données à caractère personnel, soit sous l'autorité directe du responsable du traitement soit pour son compte. La distinction opérée entre «responsable du traitement» et «sous-traitant» sert avant tout à distinguer les intervenants qui assument la responsabilité du traitement de ceux qui ne font qu'agir pour le compte des premiers. Là encore, il s'agit principalement d'une question d'attribution des responsabilités. D'autres conséquences, au regard du droit applicable ou d'autres considérations, peuvent en découler.

Toutefois, dans le cas d'un sous-traitant, il en résulte une conséquence supplémentaire, tant pour le responsable du traitement que pour le sous-traitant: en vertu de l'article 17 de la directive, le droit applicable à la sécurité du traitement est le droit national de l'État membre dans lequel le sous-traitant est établi.[7]

Enfin, selon la définition de l'article 2, point f), «*on entend par 'tiers' la personne physique ou morale, l'autorité publique, le service ou tout autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données*.» Le responsable du traitement et le sous-traitant ainsi que les personnes qui sont placées sous leur autorité sont donc considérés comme le «cercle restreint du traitement des données» et ne sont pas soumis aux dispositions particulières relatives aux tiers.

II.2. Contexte

Du fait des différentes évolutions intervenues dans l'environnement concerné, ces questions sont devenues plus urgentes et aussi plus complexes qu'auparavant. À l'époque de la signature de la convention 108 et, dans une large mesure, lors de l'adoption de la directive 95/46/CE, le contexte du traitement des données était encore relativement clair et simple. Ce n'est plus le cas aujourd'hui.

Cette situation s'explique tout d'abord par une tendance de plus en plus nette à appliquer des modes d'organisation différenciés dans la plupart des secteurs concernés. Dans le privé, la répartition des risques, financiers ou autres, s'est traduite par une diversification constante des entreprises, d'autant plus exacerbée par les fusions et les acquisitions. Dans la sphère publique, on assiste à une différenciation similaire dans le cadre de la décentralisation ou de la scission entre les services chargés de l'élaboration des politiques et les agences exécutives. Dans les deux secteurs, une place croissante est accordée au développement de circuits de distribution ou de la prestation de services au sein des organisations, et au recours à la sous-traitance ou à l'externalisation des services afin de bénéficier de la spécialisation et d'éventuelles économies d'échelle. Il y a dès lors une multiplication des services proposés par des prestataires qui ne s'estiment pas toujours responsables ou tenus de rendre des comptes. En raison des choix organisationnels opérés par les entreprises (et par leurs contractants ou sous-traitants), les bases de données concernées peuvent se trouver dans un ou plusieurs pays de l'Union européenne ou en dehors de celle-ci.

L'essor des technologies de l'information et de la communication («TIC») a largement contribué à ces mutations organisationnelles, apportant même ses propres évolutions. Les responsabilités exercées à différents niveaux, souvent le fruit d'un contexte

[7] Voir l'article 17, paragraphe 3, deuxième tiret: «les obligations …. telles que définies par la législation de l'État membre dans lequel le sous-traitant est établi, incombent également à celui-ci».

organisationnel différencié, rendent les TIC indispensables et favorisent leur généralisation. Le développement et la diffusion des produits et services informatiques créent en outre de nouvelles fonctions et responsabilités autonomes, dont l'interaction avec les responsabilités existantes ou en développement chez les clients n'est pas toujours évidente. Il importe dès lors de connaître ces différences et de préciser les responsabilités lorsque c'est nécessaire. L'adoption des microtechnologies, comme les puces RFID dans les produits de grande consommation, soulève des questions analogues en matière de transfert de responsabilités. Par ailleurs, le recours à l'informatique répartie, notamment à l'«informatique dématérialisée» et aux «grilles», soulève également de nouvelles difficultés.[8]

La mondialisation complique encore davantage la situation. Lorsque les modes d'organisation différenciés et le développement des TIC font intervenir de multiples pays, comme c'est souvent le cas sur internet, le problème du droit applicable se pose inévitablement, non seulement dans l'UE ou l'EEE mais également par rapport aux pays tiers. La lutte contre le dopage en fournit un exemple: l'Agence mondiale antidopage (AMA), établie en Suisse, tient une base de données contenant des informations sur les athlètes (ADAMS) qui est gérée depuis le Canada, en coopération avec les organisations nationales antidopage du monde entier. Le groupe de travail a eu l'occasion de souligner que le partage des responsabilités et l'attribution de la responsabilité du traitement présentaient des difficultés particulières.[9]

Dès lors, les questions centrales examinées ici présentent un intérêt certain sur le plan pratique et sont susceptibles d'avoir de grandes conséquences.

II.3. Quelques enjeux clés

En ce qui concerne les objectifs de la directive, il est essentiel que la responsabilité du traitement de données soit clairement définie et qu'elle puisse être bien appliquée.

En effet, lorsqu'on ne sait pas exactement qui doit faire quoi (par exemple, en l'absence de responsable ou en présence d'une multitude de responsables potentiels du traitement), le risque évident est que la directive ait peu, voire pas d'effets et que ses dispositions restent lettre morte. Il se peut également que certaines ambiguïtés d'interprétation donnent lieu à des thèses contradictoires et à d'autres controverses, auquel cas les effets positifs seront moins nombreux qu'escomptés, quand ils ne seront pas diminués ou surpassés par des conséquences négatives imprévues.

En tout état de cause, le défi essentiel consiste dès lors à apporter suffisamment de précision pour permettre et garantir une bonne application et le respect de la directive dans la pratique. En cas de doute, la solution la plus à même de favoriser de tels effets serait à privilégier.

---

8 «L'informatique dématérialisée» (*cloud computing*) consiste à offrir des capacités informatiques extensibles et élastiques à de multiples utilisateurs de technologies sur internet. Les services d'informatique dématérialisée proposent des applications professionnelles communes en ligne, accessibles depuis un navigateur web, tandis que le logiciel et les données sont stockés sur les serveurs. En ce sens, le «nuage» (*cloud*) n'est pas une île mais un connecteur global de l'information et des utilisateurs mondiaux. En ce qui concerne les «grilles», voir l'exemple 19 ci-dessous.

9 Avis 3/2008 du 1er août 2008 sur le projet de norme internationale de protection de la vie privée du code mondial antidopage, WP156.

Cependant, les mêmes critères qui permettront d'apporter suffisamment de précision pourraient également compliquer davantage la situation et produire des conséquences indésirables. Par exemple, la répartition du contrôle entre plusieurs niveaux, pour s'aligner sur les réalités de l'organisation, peut rendre la détermination du droit national applicable plus difficile lorsque divers pays sont concernés.

L'analyse doit donc mettre en évidence la différence entre les conséquences acceptables au regard des règles actuelles et l'éventuelle nécessité d'adapter ces règles afin de garantir leur efficacité à long terme et d'éviter des conséquences indues, en cas d'évolution de la situation.

Par conséquent, la présente analyse revêt une grande importance stratégique et elle doit être appliquée avec prudence, en toute connaissance des interconnexions possibles entre les différents aspects.

III. Analyse des définitions

III.1. Définition du responsable du traitement

La définition du responsable du traitement énoncée dans la directive s'articule autour de trois composantes principales, analysées séparément aux fins du présent avis :

- «la personne physique ou morale, l'autorité publique, le service ou tout autre organisme»
- «qui seul ou conjointement avec d'autres»
- «détermine les finalités et les moyens du traitement de données à caractère personnel».

La première composante a trait à l'aspect individuel de la définition. La troisième composante contient les éléments essentiels qui permettent de distinguer le responsable du traitement d'autres acteurs, tandis que la deuxième envisage la possibilité d'une «responsabilité pluraliste». Les trois composantes sont étroitement liées mais, pour respecter la méthodologie suivie dans le présent avis, chacune sera examinée séparément.

Pour des raisons pratiques, il convient de commencer par le *premier élément* de la troisième composante, à savoir le sens du mot «détermine», puis de poursuivre avec ses autres éléments, avant d'examiner la première et la deuxième composantes.

III.1.a) Élément préliminaire: «détermine»

Comme il a déjà été mentionné précédemment, la notion de responsable du traitement jouait un rôle mineur dans la convention 108. Son article 2 définissait le «maître du fichier» comme l'organisme «qui est compétent ... pour décider». La convention soulignait la nécessité d'une compétence, déterminée «selon la loi nationale». Elle renvoyait donc aux législations nationales sur la protection des données, lesquelles, selon le rapport explicatif, contiendraient «des critères précis pour l'identification de la personne compétente».

Alors que cette disposition trouvait son pendant dans la première proposition de la Commission, la proposition modifiée de cette dernière fait mention de l'organisme «qui décide», éliminant de ce fait la nécessité que la compétence de décider soit donnée par la loi: la définition par la loi est certes toujours possible mais non nécessaire. C'est ce qui ressort de la position commune du Conseil et du texte adopté par la suite, qui mentionnent tous deux l'organisme «qui détermine».

Dans ce contexte, l'évolution de la définition met en lumière deux éléments importants: d'une part, il est possible d'être responsable du traitement indépendamment d'une compétence ou d'un pouvoir spécifique conférés par la loi pour contrôler des données; d'autre part, dans le processus d'adoption de la directive 95/46, la détermination du responsable du traitement devient une notion communautaire, qui revêt son propre sens indépendant dans le droit communautaire et ne varie pas au gré des dispositions législatives nationales potentiellement divergentes. Ce second élément est essentiel si l'on veut garantir la bonne application de la directive et un niveau élevé de protection dans les États membres, ce qui suppose une interprétation uniforme et donc autonome de cette notion clé qu'est le «responsable du traitement» qui, dans la directive, prend une dimension qu'elle n'avait pas dans la convention 108.

Dans cette perspective, la directive parachève cette évolution en consacrant que, même si la capacité de «déterminer» peut procéder d'une attribution faite expressément par la loi, elle se déduira généralement d'une analyse des éléments factuels ou des circonstances de l'espèce: il conviendra d'examiner les opérations de traitement en question et de comprendre qui les détermine, en répondant dans un premier temps aux questions «pourquoi ce traitement a-t-il lieu? » et «qui l'a entrepris?».

Être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres. C'est pourquoi un critère purement formel ne suffirait pas, pour au moins deux raisons: dans certains cas, la désignation officielle d'un responsable du traitement (prévue, par exemple, par la loi, dans un contrat ou dans une notification à l'autorité chargée de la protection des données) fera tout simplement défaut; dans d'autres cas, il se peut que la désignation officielle ne reflète pas la réalité, les fonctions de responsable du traitement étant confiées à un organisme qui, dans les faits, n'est pas en mesure de «déterminer».

L'affaire SWIFT démontre bien l'importance de l'influence de fait[10]: la société SWIFT était officiellement considérée comme le sous-traitant des données alors qu'en réalité, elle intervenait, au moins dans une certaine mesure, en tant que responsable du traitement des données. Il a ainsi été clairement établi que, même si la désignation d'une entité en tant que responsable du traitement ou sous-traitant des données dans un contrat pouvait révéler des informations intéressantes sur le statut juridique de l'entité, cette désignation contractuelle ne permet cependant pas de déterminer avec certitude son véritable statut, qui doit être déduit de circonstances concrètes.

Cette approche factuelle est du reste corroborée par le fait que, selon la directive, le responsable du traitement est celui qui «détermine» plutôt que celui qui «détermine licitement» les finalités et les moyens. C'est l'identification même de la responsabilité du traitement qui est primordiale, quand bien même la désignation se révèlerait irrégulière

[10] L'affaire concerne le transfert aux autorités américaines, dans le but de lutter contre le financement du terrorisme, de données bancaires collectées par la SWIFT en vue de réaliser des transactions financières pour le compte de banques et d'établissements financiers.

ou le traitement des données serait réalisé de manière illicite. Peu importe que la décision de traiter des données soit «licite», au sens où l'entité qui a pris la décision y était juridiquement habilitée ou qu'un responsable du traitement a été officiellement désigné selon la procédure requise. La question de la licéité du traitement des données à caractère personnel revêtira encore son importance à un stade ultérieur et sera examinée à la lumière d'autres articles (notamment les articles 6 à 8) de la directive. En d'autres termes, il importe de faire en sorte que, même en cas de traitement illicite des données, un responsable du traitement puisse être facilement identifié et désigné comme tel.

Une dernière caractéristique de la notion de responsable du traitement est son autonomie, dans le sens où, même si des sources juridiques externes peuvent aider à identifier le responsable du traitement, elle doit être interprétée essentiellement à la lumière de la législation sur la protection des données. [11] La notion de responsable du traitement ne doit pas être altérée par d'autres notions, parfois contradictoires ou redondantes, issues d'autres domaines du droit, comme celles de créateur ou de titulaire de droits de propriété intellectuelle. Le fait d'être titulaire de droits de propriété intellectuelle n'exclut en effet pas la possibilité d'être également «responsable du traitement» et, dès lors, d'être soumis aux obligations imposées par la législation sur la protection des données.

La nécessité d'une typologie

La notion de responsable du traitement est une notion fonctionnelle, visant à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle s'appuie donc sur une analyse factuelle plutôt que formelle. Par conséquent, un examen long et approfondi sera parfois nécessaire pour déterminer cette responsabilité. L'impératif d'efficacité impose cependant d'adopter une approche pragmatique pour assurer une prévisibilité de la responsabilité. À cet égard, des règles empiriques et des présomptions concrètes sont nécessaires pour guider et simplifier l'application de la législation en matière de protection des données.

Ceci implique une interprétation de la directive garantissant que «l'organisme qui détermine» puisse être facilement et clairement identifié dans la plupart des cas, en s'appuyant sur les éléments de droit et/ou de fait à partir desquels l'on peut normalement déduire une influence de fait, en l'absence d'indices contraires.

Ces contextes peuvent être analysés et classés selon les trois catégories de situations suivantes, qui permettent d'aborder ces questions de façon systématique:

1) *Responsabilité découlant d'une compétence explicitement donnée par la loi*. Il s'agit notamment du cas visé dans la seconde partie de la définition, à savoir lorsque le responsable du traitement ou les critères spécifiques pour le désigner sont fixés par le droit national ou communautaire. La désignation explicite du responsable du traitement par le droit n'est pas courante et ne présente généralement pas de grandes difficultés. Dans certains pays, le droit national prévoit que les pouvoirs publics assument la responsabilité du traitement des données à caractère personnel effectué dans le cadre de leurs fonctions.

[11] Voir ci-dessous, l'interférence avec les notions existant dans d'autres domaines du droit (par exemple, la notion de titulaire de droits de propriété intellectuelle ou de recherche scientifique, ou de responsabilité en vertu du droit civil).

Il est cependant plus fréquent que la législation, plutôt que de désigner directement le responsable du traitement ou de fixer les critères de sa désignation, charge une personne, ou lui impose, de collecter et traiter certaines données. Cela pourrait être le cas d'une entité qui se voit confier certaines missions publiques (par exemple, la sécurité sociale) ne pouvant être réalisées sans collecter au moins quelques données à caractère personnel, et qui crée un registre afin de s'en acquitter. Dans ce cas, c'est donc le droit qui détermine le responsable du traitement. De façon plus générale, la loi peut obliger des entités publiques ou privées à conserver ou fournir certaines données. Ces entités seraient alors normalement considérées comme responsables de tout traitement de données à caractère personnel intervenant dans ce cadre.

2) *Responsabilité découlant d'une compétence implicite*. Il s'agit du cas où le pouvoir de déterminer n'est pas explicitement prévu par le droit, ni la conséquence directe de dispositions juridiques explicites, mais découle malgré tout de règles juridiques générales ou d'une pratique juridique établie relevant de différentes matières (droit civil, droit commercial, droit du travail, etc.). Dans ce cas, les rôles traditionnels qui impliquent normalement une certaine responsabilité permettront d'identifier le responsable du traitement: par exemple, l'employeur pour les informations sur ses salariés, l'éditeur pour les informations sur ses abonnés, l'association pour les informations sur ses membres ou adhérents.

Dans tous ces exemples, le pouvoir de déterminer les activités de traitement peut être considéré comme naturellement lié au rôle fonctionnel d'une organisation (privée), entraînant au final également des responsabilités en matière de protection des données. Du point de vue juridique, peu importerait que le pouvoir de déterminer soit confié aux entités juridiques mentionnées, qu'il soit exercé par les organes appropriés agissant pour leur compte, ou par une personne physique dans le cadre de fonctions similaires (voir l'explication ci-dessous sur le premier élément du point c)). Il en serait néanmoins de même pour une entité publique chargée de certaines tâches administratives, dans un pays où la législation ne prévoirait pas explicitement sa responsabilité en matière de protection des données.

Exemple n° 1: Opérateurs de télécommunications

Le rôle des opérateurs de télécommunications constitue un exemple intéressant de recommandations juridiques adressées au secteur privé : le considérant 47 de la directive 95/46/CE précise que «*lorsqu'un message contenant des données à caractère personnel est transmis via un service de télécommunications ou de courrier électronique dont le seul objet est de transmettre des messages de ce type, c'est la personne dont émane le message, et non celle qui offre le service de transmission, qui sera normalement considérée comme responsable du traitement de données à caractère personnel contenues dans le message; (...) toutefois, les personnes qui offrent ces services seront normalement considérées comme responsables du traitement des données à caractère personnel supplémentaires nécessaires au fonctionnement du service».*

Le fournisseur de services de télécommunications ne doit donc, en principe, être considéré comme responsable du traitement que pour les données relatives au trafic et à la facturation, et non pour les données transmises[12]. Ces recommandations juridiques du législateur de l'Union cadrent totalement avec l'approche fonctionnelle adoptée dans le présent avis.

3) *Responsabilité découlant d'une influence de fait*. Il s'agit du cas où la responsabilité du traitement est attribuée après une évaluation des circonstances factuelles. Un examen des relations contractuelles entre les différentes parties concernées sera bien souvent nécessaire. Cette évaluation permet de tirer des conclusions externes, attribuant le rôle et les obligations de responsable du traitement à une ou plusieurs parties. Elle peut s'avérer particulièrement utile dans des environnements complexes, exploitant les nouvelles technologies de l'information, dans lesquels les acteurs concernés ont fréquemment tendance à se considérer comme des «médiateurs» et non comme des responsables du traitement consciencieux.

Il peut arriver qu'un contrat ne désigne aucun responsable du traitement mais qu'il contienne suffisamment d'éléments pour attribuer cette responsabilité à une personne qui exerce apparemment un rôle prédominant à cet égard. Il se peut également que le contrat soit plus explicite en ce qui concerne le responsable du traitement. S'il n'y a aucune raison de penser que les clauses contractuelles ne reflètent pas exactement la réalité, rien ne s'oppose à leur application. Les clauses d'un contrat ne sont toutefois pas toujours déterminantes, car les parties auraient alors la possibilité d'attribuer la responsabilité à qui elles l'entendent.

Le fait même qu'une personne détermine comment les données à caractère personnel sont traitées peut entraîner la qualification de responsable du traitement, même si cette qualification sort du cadre d'une relation contractuelle ou si elle est expressément exclue par un contrat. L'affaire SWIFT en est un exemple éloquent: cette société a pris la décision de mettre à disposition certaines données à caractère personnel (lesquelles étaient initialement traitées à des fins commerciales pour le compte d'établissements financiers) également pour lutter contre le financement du terrorisme, comme le demandaient les injonctions adressées par le Trésor américain.

En cas de doute, d'autres éléments que les clauses d'un contrat peuvent servir à identifier le responsable du traitement, tel que le degré de contrôle réel exercé par une partie, l'image donnée aux personnes concernées et les attentes raisonnables que cette visibilité peut susciter chez ces dernières (voir également les explications ci-dessous concernant le troisième élément du point b)). Cette catégorie est particulièrement importante puisqu'elle permet d'examiner les responsabilités et de les attribuer également en cas de comportement illicite consistant à traiter des données contre les intérêts et la volonté de certaines des parties.

[12] Une autorité chargée de la protection des données a examiné la responsabilité dans une affaire soumise par une personne concernée se plaignant de recevoir par courrier électronique de la publicité non sollicitée. Dans sa plainte, la personne concernée demandait au fournisseur du réseau de communication de confirmer ou de démentir qu'il était l'expéditeur du courrier électronique publicitaire. L'autorité chargée de la protection des données a indiqué que la société qui se contentait de fournir au client un accès au réseau de communication, sans procéder à la transmission des données, sélectionner les destinataires ni modifier les informations contenues dans la transmission, ne pouvait être considérée comme responsable du traitement des données.

Conclusion préliminaire

Parmi ces catégories, les deux premières permettent, en principe, de désigner «l'organisme qui détermine» avec davantage de fiabilité et peuvent facilement couvrir plus de 80 % des situations dans la pratique. Une désignation officielle par la loi n'en doit pas moins être conforme aux règles de protection des données, en veillant à ce que l'organisme désigné ait un contrôle effectif sur les opérations de traitement ou, en d'autres termes, que la désignation par la loi reflète la réalité de la situation.

La troisième catégorie nécessite une analyse plus poussée et est davantage susceptible de donner lieu à des interprétations divergentes. En effet, les clauses d'un contrat aident souvent à faire la lumière sur ce point, mais elles ne sont pas toujours déterminantes. Un nombre croissant d'acteurs considèrent qu'ils ne déterminent pas les activités de traitement et ils estiment donc ne pas en être responsables. Dans ce cas, la seule solution envisageable est d'examiner qui exerce une influence de fait. La question de la licéité de ce traitement sera analysée plus loin à la lumière d'autres articles (6 à 8).

Lorsqu'aucune des catégories susmentionnées ne peut être appliquée, la désignation d'un responsable du traitement doit être considérée comme «nulle». En effet, un organisme qui n'exerce ni influence de droit ni influence de fait pour déterminer la manière dont les données à caractère personnel seront traitées ne saurait être considéré comme le responsable du traitement.

Du point de vue formel, cette approche est corroborée par le fait que la définition de responsable du traitement doit être considérée comme une disposition juridique obligatoire, à laquelle les parties ne peuvent pas déroger. D'un point de vue stratégique, une telle désignation nuirait à la bonne application de la législation relative à la protection des données et annulerait la responsabilité qu'implique le traitement des données.

III.1.b) Troisième élément: «finalités et moyens du traitement»

Le troisième élément représente la partie essentielle de l'analyse: ce qu'une partie doit déterminer pour pouvoir être qualifiée de responsable du traitement.

Cette disposition a connu maintes évolutions. La convention 108 faisait mention de la finalité du fichier automatisé, des catégories de données à caractère personnel et des opérations qui leur sont appliquées. La Commission avait repris ces éléments fondamentaux, en modifiant légèrement leur formulation, et avait ajouté la compétence de décider quels tiers auront accès aux données. La proposition modifiée de la Commission faisait un pas supplémentaire en remplaçant «la finalité du fichier» par les «finalités et objectif du traitement», passant ainsi d'une définition statique liée à un fichier à une définition dynamique associée à l'activité de traitement. Cette proposition modifiée mentionnait donc quatre éléments (finalités/objectif, données à caractère personnel, opérations et tiers ayant accès aux données), qui ont été réduits à seulement deux («finalités et moyens») par la position commune du Conseil.

Selon les dictionnaires, le terme «finalité» désigne «un résultat attendu qui est recherché ou qui guide les actions prévues», et le mot «moyen», «la façon de parvenir à un résultat ou d'arriver à une fin».

Par ailleurs, la directive prévoit que les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. La détermination des «finalités» du traitement et des «moyens» pour les atteindre revêt dès lors une importance particulière.

On peut en outre affirmer que la détermination des finalités et des moyens revient à établir respectivement le «pourquoi» et le «comment» de certaines activités de traitement. Dans cette optique, et puisque ces deux éléments sont indissociables, il est nécessaire de donner des indications sur le degré d'influence qu'une entité doit avoir sur le «pourquoi» et le «comment» pour être qualifiée de responsable du traitement.

Lorsqu'il s'agit d'évaluer la détermination des finalités et des moyens en vue d'attribuer le rôle de responsable du traitement, la question centrale qui se pose est donc le degré de précision auquel une personne doit déterminer les finalités et les moyens afin d'être considérée comme un responsable du traitement et, en corollaire, la marge de manœuvre que la directive laisse à un sous-traitant. Ces définitions prennent tout leur sens lorsque divers acteurs interviennent dans le traitement de données à caractère personnel et qu'il est nécessaire de déterminer lesquels d'entre eux sont responsables du traitement (seuls ou conjointement avec d'autres) et lesquels sont à considérer comme des sous-traitants, le cas échéant.

L'importance à accorder aux finalités ou aux moyens peut varier en fonction du contexte particulier dans lequel intervient le traitement.

Il convient d'adopter une approche pragmatique mettant davantage l'accent sur le pouvoir discrétionnaire de déterminer les finalités et sur la latitude laissée pour prendre des décisions. Les questions qui se posent alors sont celle du motif du traitement et celle du rôle d'éventuels acteurs liés, tels que les sociétés d'externalisation de services: la société qui a confié ses services à un prestataire extérieur aurait-elle traité les données si le responsable du traitement ne le lui avait pas demandé, et à quelles conditions? Un sous-traitant pourrait suivre les indications générales données principalement sur les finalités et ne pas entrer dans les détails en ce qui concerne les moyens.

Exemple n° 2: Publipostage

La société ABC passe des contrats avec différentes organisations pour réaliser ses campagnes de publipostage et gérer la paie. Elle donne des instructions claires (quels documents publicitaires envoyer et à qui, et qui payer, quels montants, à quelle date etc.). Même si les organisations disposent d'une certaine latitude (y compris pour les logiciels à utiliser), leurs tâches sont clairement et précisément définies. En outre, si la société de publipostage peut proposer ses conseils (en recommandant, par exemple, de ne pas faire d'envois au mois d'août), elle est clairement tenue d'agir selon les instructions d'ABC. De plus, une seule entité, à savoir la société ABC, a le droit d'utiliser les données qui sont traitées. Toutes les autres entités doivent s'appuyer sur la base juridique de la société ABC si leur habilitation juridique à traiter les données est mise en cause. Dans cet exemple, il apparaît donc clairement que la société ABC est le responsable du traitement et que chacune des structures distinctes peut être considérée comme un sous-traitant en ce qui concerne le traitement spécifique des données réalisé pour son compte.

14

S'agissant de la détermination des «moyens», ce terme comprend de toute évidence des éléments très divers, ce qu'illustre d'ailleurs l'évolution de la définition. Ainsi, dans la proposition initiale, le rôle de responsable du traitement découlait de quatre éléments déterminants (finalités/objectif, données à caractère personnel, opérations et tiers ayant accès aux données). La formulation définitive de la disposition, qui mentionne uniquement les «finalités et moyens», ne saurait cependant être interprétée comme étant en contradiction avec l'ancienne version, puisqu'il n'y a aucun doute sur le fait que, par exemple, le responsable du traitement doit déterminer les données qui seront traitées pour la ou les finalités envisagées. Partant, la définition finale doit plutôt être comprise comme une version abrégée intégrant néanmoins le sens de l'ancienne version. En d'autres termes, «moyens» ne désigne pas seulement les moyens techniques de traiter des données à caractère personnel, mais également le «comment» du traitement, qui comprend des questions comme «quelles données seront traitées», «quels sont les tiers qui auront accès à ces données», «à quel moment les données seront-elles effacées», etc.

La détermination des «moyens» englobe donc à la fois des questions techniques et d'organisation, auxquelles les sous-traitants peuvent tout aussi bien répondre (par exemple, «quel matériel informatique ou logiciel utiliser?»), et des aspects essentiels qui sont traditionnellement et intrinsèquement réservés à l'appréciation du responsable du traitement, tels que «quelles sont les données à traiter?», «pendant combien de temps doivent-elles être traitées?», «qui doit y avoir accès», etc.

Dans ce contexte, alors que la détermination de la finalité du traitement emporterait systématiquement la qualification de responsable du traitement, la détermination des moyens impliquerait une responsabilité uniquement lorsqu'elle concerne les éléments essentiels des moyens.

Dans cette optique, il est tout à fait possible que les moyens techniques et d'organisation soient déterminés exclusivement par le sous-traitant des données.

Dans ce cas, lorsque les finalités sont bien définies mais qu'il existe peu, voire aucune indication sur les moyens techniques et d'organisation, les moyens devraient représenter une façon raisonnable d'atteindre la ou les finalités, et le responsable du traitement devrait être parfaitement informé des moyens utilisés. Si un contractant avait une influence sur la finalité et qu'il procédait au traitement (également) à des fins personnelles, par exemple en utilisant les données à caractère personnel reçues en vue de créer des services à valeur ajoutée, il deviendrait alors responsable du traitement (ou éventuellement coresponsable du traitement) pour une autre activité de traitement et serait donc soumis à toutes les obligations prévues par la législation applicable en matière de protection des données.

Exemple n° 3: Société désignée comme sous-traitant de données mais agissant comme un responsable du traitement

La société MarketinZ propose des services de publicité promotionnelle et de marketing direct à différentes sociétés. La société GoodProductZ conclut un contrat avec MarketinZ, aux termes duquel cette dernière assure la publicité commerciale des clients de GoodProductZ et est désignée comme sous-traitant de données. Cependant, MarketinZ décide d'utiliser également la base de données des clients de GoodProducts pour promouvoir les produits d'autres clients. Cette décision d'ajouter une finalité supplémentaire à celle pour laquelle les données à caractère personnel ont été transmises

15

fait de MarketinZ le responsable de cette opération de traitement. La question de la licéité de ce traitement sera examinée plus loin à la lumière d'autres articles (6 à 8).

Dans certains systèmes juridiques, les décisions relatives aux mesures de sécurité ont une importance particulière car ces mesures sont explicitement considérées comme une caractéristique essentielle qui doit être définie par le responsable du traitement. Se pose ici la question de savoir quelles décisions en matière de sécurité entraînent la qualification de responsable du traitement pour une société à laquelle le traitement a été confié.

Conclusion préliminaire

La détermination de la «finalité» du traitement est réservée au «responsable du traitement». Toute personne qui prend cette décision est donc un responsable du traitement (de fait). En revanche, la détermination des «moyens» du traitement peut être déléguée par le responsable du traitement, pour autant qu'elle concerne des questions techniques ou d'organisation. Les questions sensibles qui sont fondamentales pour la licéité du traitement sont réservées au responsable du traitement. Une personne ou une entité qui décide, par exemple, de la durée de conservation des données ou des personnes qui auront accès aux données traitées agit en «responsable du traitement» pour cette partie de l'utilisation des données, et doit donc se conformer à toutes les obligations qui incombent au responsable du traitement.

III.1.c) Premier élément: «personne physique, personne morale ou tout autre organisme»

Le premier élément de la définition a trait à l'aspect personnel: qui peut être responsable du traitement, et donc considéré comme responsable en dernier ressort des obligations découlant de la directive. La définition reproduit exactement le libellé de l'article 2 de la convention 108 et n'a fait l'objet d'aucun débat particulier lors du processus d'adoption de la directive. Elle renvoie à un vaste éventail de sujets susceptibles de jouer le rôle de responsable du traitement, de la personne physique à la personne morale, en passant par «tout autre organisme».

Il importe que l'interprétation de ce point garantisse la bonne application de la directive, en favorisant autant que possible une identification claire et univoque du responsable du traitement en toutes circonstances, même si aucune désignation officielle n'a été faite et rendue publique.

Il convient avant tout de s'écarter le moins possible de la pratique établie dans les secteurs public et privé par d'autres domaines du droit, tels que le droit civil, le droit administratif et le droit pénal. Dans la plupart des cas, ces dispositions indiqueront à quelles personnes ou à quels organismes les responsabilités doivent être attribuées et permettront, en principe, d'identifier le responsable du traitement.

Dans la perspective stratégique d'attribution des responsabilités, et afin que les personnes concernées puissent s'adresser à une entité plus stable et plus fiable lorsqu'elles exercent les droits qui leurs sont conférés par la directive, il serait préférable de considérer comme responsable du traitement la société ou l'organisme en tant que tel, plutôt qu'une personne en son sein. C'est en effet la société ou l'organisme qu'il convient de considérer, en dernier ressort, comme responsable du traitement des données et des obligations énoncées par la législation relative à la protection des données, à moins que

16

certains éléments précis n'indiquent qu'une personne physique doit être responsable. D'une manière générale, on partira du principe qu'une société ou un organisme public est responsable en tant que tel des opérations de traitement qui se déroulent dans son domaine d'activités et de risques.

Parfois, les sociétés et les organismes publics désignent une personne précise pour être responsable de l'exécution des opérations de traitement. Cependant, même lorsqu'une personne physique est désignée pour veiller au respect des principes de protection des données ou pour traiter des données à caractère personnel, elle n'est pas responsable du traitement mais agit pour le compte de la personne morale (société ou organisme public), qui demeure responsable en cas de violation des principes, en sa qualité de responsable du traitement.[13]

Il s'agit là, surtout pour les grandes structures complexes, d'une question fondamentale de «gouvernance en matière de protection des données»: garantir à la fois une responsabilité sans équivoque de la personne physique représentant la société et des responsabilités fonctionnelles concrètes au sein de la structure, par exemple en demandant à d'autres personnes d'assumer les fonctions de représentants ou de points de contact pour les personnes concernées.

Une analyse distincte s'impose dans le cas où une personne physique agissant au sein d'une personne morale utilise des données à des fins personnelles, en dehors du cadre et de l'éventuel contrôle des activités de la personne morale. Dans ce cas, la personne physique en cause serait responsable du traitement décidé, et assumerait la responsabilité de cette utilisation de données à caractère personnel. Le responsable du traitement initial pourrait néanmoins conserver une certaine part de responsabilité si le nouveau traitement a eu lieu du fait d'une insuffisance des mesures de sécurité.

Ainsi qu'il a été dit précédemment, le rôle du responsable du traitement est décisif et revêt une importance particulière lorsqu'il s'agit de déterminer les responsabilités et d'infliger des sanctions. Même si celles-ci varient d'un État membre à l'autre parce qu'elles sont imposées selon les droits nationaux, la nécessité d'identifier clairement la personne physique ou morale responsable des infractions à la législation sur la protection des données est sans nul doute un préalable indispensable à la bonne application de la directive.

Sous l'angle de la protection des données, l'identification du «responsable du traitement» sera guidée, dans la pratique, par les règles du droit civil, administratif ou pénal régissant l'attribution des responsabilités ou l'imposition de sanctions à une personne physique ou morale[14].

---

13 Un raisonnement analogue a été suivi au sujet du règlement (CE) 45/2001, dont l'article 2, point d), mentionne «l'institution ou l'organe communautaire, la direction générale, l'unité ou toute autre entité organisationnelle». La pratique en matière de surveillance a clairement établi que les fonctionnaires des institutions et des organes de l'UE, qui ont été désignés «responsables du traitement», agissent pour le compte de l'organe pour lequel ils travaillent.

14 Voir l'étude comparative de la Commission intitulée «Comparative Study on the Situation in the 27 Member States as regards the Law Applicable to Non-contractual Obligations Arising out of Violations of Privacy and Rights relating to Personality», *[Étude comparative de la situation dans les 27 États membres concernant le droit applicable aux obligations non contractuelles résultant d'atteintes à la vie privée et aux droits de la personnalité]*, février 2009, disponible (en anglais) à l'adresse http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

17

La responsabilité civile ne devrait pas soulever de problème particulier dans ce contexte puisqu'elle s'applique, en principe, aux personnes physiques et morales. En revanche, certains droits nationaux ne reconnaissent la responsabilité pénale et/ou administrative qu'à l'égard des personnes physiques. Cependant, si un droit national prévoit des sanctions pénales ou administratives en cas d'infraction à la protection des données, ce même droit déterminera également qui est responsable: si la responsabilité pénale ou administrative des personnes morales n'est pas reconnue, elle sera éventuellement assumée par des employés des personnes morales en vertu de dispositions spéciales du droit national[15].

Le droit européen comprend des exemples utiles de critères d'attribution de la responsabilité pénale[16], notamment lorsqu'une infraction est commise au profit de la personne morale: peut être tenue pour responsable toute personne, «agissant soit individuellement soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de décision en son sein, sur les bases suivantes:
(a) un pouvoir de représentation de la personne morale;
(b) une autorité pour prendre des décisions au nom de la personne morale;
(c) une autorité pour exercer un contrôle au sein de la personne morale.»

Conclusion préliminaire

Pour résumer les réflexions qui viennent d'être exposées, il apparaît que la personne responsable en cas de non-respect de la protection des données est toujours le responsable du traitement, à savoir la personne morale (société ou organisme public) ou la personne physique formellement identifiée selon les critères de la directive. Si une personne physique travaillant dans une société ou un organisme public utilise des données à des fins personnelles, en dehors des activités de la société, elle doit être considérée comme un responsable du traitement de fait et assumer la responsabilité pénale en tant que tel.

Exemple n° 4: Surveillance secrète des employés

Un membre du conseil d'administration d'une société décide de surveiller secrètement les employés de la société, alors que cette décision n'a pas officiellement reçu l'aval du conseil d'administration. La société doit être considérée comme responsable du traitement et faire face aux éventuelles réclamations et poursuites des employés dont les données à caractère personnel ont été utilisées abusivement.

La responsabilité juridique de la société est notamment due au fait qu'en tant que responsable du traitement, elle a l'obligation de garantir le respect des règles de sécurité et de confidentialité. Une utilisation abusive par un dirigeant de la société ou un employé pourrait être considérée comme le résultat de mesures de sécurité inappropriées.

15 Cela n'exclut pas que les droits nationaux puissent prévoir une responsabilité pénale ou administrative non seulement pour le responsable du traitement mais également pour toute personne qui enfreint la législation relative à la protection des données.

16 Voir par exemple la directive 2008/99/CE du 19 novembre 2008 relative à la protection de l'environnement par le droit pénal, la décision-cadre du Conseil du 13 juin 2002 relative à la lutte contre le terrorisme. Les instruments juridiques se basent sur l'article 29, l'article 31, point e), et l'article 34, paragraphe 2, point b), du TUE ou correspondent aux bases juridiques des instruments utilisés dans le premier pilier, résultant de la jurisprudence de la CJCE dans les affaires C-176/03, COM/Conseil, Recueil 2005, p. I-7879, et C-440/05, COM/Conseil, Recueil 2007, p. I-9097. Voir également la communication de la Commission COM (2005) 583 final).

Il importe à cet égard que le membre du conseil d'administration ou d'autres personnes physiques dans la société soient ultérieurement tenues pour responsables, tant en matière civile (également envers la société) que pénale. Cela pourrait notamment être le cas si le membre du conseil s'est servi des données collectées pour obtenir des faveurs personnelles des employés: il devrait alors être considéré comme «responsable du traitement» et voir sa responsabilité engagée pour cette utilisation des données.

III.1.d) Deuxième élément: «seul ou conjointement avec d'autres»

Ce paragraphe, qui s'appuie sur l'analyse susmentionnée des caractéristiques types du responsable du traitement, examinera les situations où de multiples acteurs interviennent dans le traitement de données à caractère personnel. Il est en effet de plus en plus fréquent que différents acteurs agissent en tant que responsables du traitement, un cas de figure envisagé par la définition énoncée dans la directive.

La possibilité que le responsable du traitement agisse «seul ou conjointement avec d'autres» n'était pas mentionnée dans la convention 108 et n'a été introduite que par le Parlement européen, avant l'adoption de la directive. Dans son avis sur cet amendement du Parlement européen, la Commission prévoit la possibilité que «*pour un même traitement, il peut y avoir plusieurs coresponsables décidant conjointement de la finalité du traitement et des moyens à mettre en œuvre pour l'effectuer*» et que «*dans un tel cas, chacun des coresponsables doit être considéré comme tenu au respect des obligations posées par la directive en vue de protéger les personnes physiques dont les données sont traitées*».

L'avis de la Commission ne rendait pas totalement compte des complexités de la réalité actuelle du traitement des données, puisqu'il n'envisageait que le cas où tous les responsables du traitement décident de façon égale et sont responsables de façon égale d'un même traitement. Or la réalité montre qu'il ne s'agit là que d'une des facettes de la «responsabilité pluraliste». Dans cette optique, «conjointement» doit être interprété comme signifiant «ensemble avec» ou «pas seul», sous différentes formes et associations.

Il convient tout d'abord de noter que la probabilité de voir de multiples acteurs participer au traitement de données à caractère personnel est naturellement liée à la multiplicité des activités qui, selon la directive, peuvent constituer un «traitement» devenant, au final, l'objet de la «coresponsabilité». La définition du traitement énoncée à l'article 2, point b), de la directive n'exclut pas la possibilité que différents acteurs participent à plusieurs opérations ou ensembles d'opérations appliquées à des données à caractère personnel. Ces opérations peuvent se dérouler simultanément ou en différentes étapes.

Dans un environnement aussi complexe, il importe d'autant plus que les rôles et les responsabilités puissent facilement être attribués, pour éviter que les complexités de la coresponsabilité n'aboutissent à un partage des responsabilités impossible à mettre en œuvre, qui compromettrait l'efficacité de la législation sur la protection des données. Malheureusement, en raison de la multitude d'accords envisageables, il est impossible de dresser une liste exhaustive des différents types de «coresponsabilité» ou de les classer. Il est cependant utile, dans ce contexte également, d'apporter des indications en citant quelques catégories et exemples de coresponsabilité et en précisant quelques éléments factuels à partir desquels il est possible de déduire ou de supposer une coresponsabilité.

19

D'une manière générale, l'évaluation de la coresponsabilité doit être calquée sur celle de la responsabilité «unique» développée plus haut, au paragraphe III.1, points a) à c). Dans le même esprit, l'évaluation de la coresponsabilité devrait, elle aussi, reposer sur une approche concrète et pratique, illustrée précédemment, pour établir si les finalités et les moyens sont déterminés par plus d'une partie.

Exemple n° 5: Installation de caméras de vidéosurveillance

Le propriétaire d'un immeuble passe un contrat avec une société de sécurité, afin que cette dernière installe des caméras dans différentes parties de l'immeuble pour le compte du responsable du traitement. Les finalités de la vidéosurveillance et la manière dont les images sont collectées et conservées sont exclusivement déterminées par le propriétaire de l'immeuble, qui doit dès lors être considéré comme l'unique responsable du traitement pour cette opération de traitement.

Dans ce contexte également, les accords contractuels peuvent certes être utiles à l'évaluation de la coresponsabilité, mais doivent toujours être confrontés aux circonstances factuelles de la relation entre les parties.

Exemple n° 6: Chasseurs de têtes

La société Headhunterz Ltd aide Enterprize Inc à recruter de nouveaux personnels. Le contrat stipule expressément que «Headhunterz Ltd agira pour le compte de Enterprize et, pour le traitement des données à caractère personnel, en tant que sous-traitant de données. Enterprize est l'unique responsable du traitement des données». Headhunterz Ltd se trouve néanmoins dans une position ambiguë: d'une part, elle joue le rôle de responsable du traitement à l'égard des demandeurs d'emploi et, d'autre part, elle assume la fonction de sous-traitant agissant pour le compte des responsables du traitement, tels que Enterprize Inc et les autres sociétés qui cherchent à recruter du personnel par son intermédiaire. En outre, Headhunterz, offrant son célèbre service à valeur ajoutée «global matchz», recherche des candidats qualifiés tant parmi les CV reçus directement par Enterprize que parmi ceux qu'elle détient déjà dans sa base de données très fournie. Cela permet à Headhunterz qui, selon le contrat, est uniquement rémunérée pour les contrats signés, d'accroître la correspondance entre offres et demandeurs d'emploi, augmentant de ce fait ses revenus. D'après les éléments susmentionnés, on peut dire que, malgré la qualification contractuelle, Headhunterz Ltd doit être considérée comme un responsable du traitement, et qu'elle contrôle, conjointement avec Enterprize Inc, au moins les ensembles d'opérations concernant le recrutement entrepris par cette dernière.

Ainsi, une coresponsabilité naît lorsque plusieurs parties déterminent, pour certaines opérations de traitement, soit la finalité soit les éléments essentiels des moyens qui caractérisent un responsable du traitement (voir ci-dessus le paragraphe III.1, points a) à c)).

Cependant, dans le cadre d'une coresponsabilité, la participation des parties à la détermination conjointe peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale. En effet, lorsqu'il y a pluralité d'acteurs, ils peuvent entretenir une relation très proche (en partageant, par exemple, l'ensemble des finalités et des moyens d'une opération de traitement) ou, au contraire, plus distante (en ne partageant que les finalités ou les moyens, ou une partie de ceux-ci). Dès lors, un large éventail de

20

typologies de la coresponsabilité doit être examiné, et leurs conséquences juridiques évaluées, avec une certaine souplesse pour tenir compte de la complexité croissante de la réalité actuelle du traitement de données.

Dans ce contexte, il y a lieu d'examiner les différents degrés auxquels les diverses parties peuvent échanger ou être liées entre elles lors du traitement de données à caractère personnel.

Tout d'abord, le simple fait que différentes parties coopèrent dans le traitement de données à caractère personnel, par exemple dans une chaîne, ne signifie pas qu'elles sont coresponsables dans tous les cas. En effet, un échange de données entre deux parties, sans partage des finalités ou des moyens dans un ensemble commun d'opérations, doit être considéré uniquement comme un transfert de données entre des responsables distincts.

Exemple n° 7: Agence de voyages (1)

Une agence de voyages envoie les données à caractère personnel de ses clients aux compagnies aériennes et à une chaîne d'hôtels, en vue de faire des réservations pour un voyage à forfait. La compagnie aérienne et l'hôtel confirment que les places et les chambres demandées sont disponibles. L'agence de voyages émet les documents de voyage et les bons pour ses clients. Dans cet exemple, l'agence de voyages, la compagnie aérienne et l'hôtel seront trois responsables du traitement différents, chacun étant soumis aux obligations de protection des données concernant son propre traitement de données à caractère personnel.

L'appréciation pourrait toutefois être différente si plusieurs acteurs décidaient de créer une infrastructure commune afin de poursuivre leurs propres finalités individuelles. En créant cette infrastructure, ces acteurs déterminent les éléments essentiels des moyens à utiliser et deviennent coresponsables du traitement des données, du moins dans cette mesure, même s'ils ne partagent pas nécessairement les mêmes finalités.

Exemple n° 8: Agence de voyages (2)

L'agence de voyages, la chaîne d'hôtels et la compagnie aérienne décident de créer une plateforme commune sur Internet pour améliorer leur coopération en ce qui concerne la gestion des réservations de voyages. Elles se mettent d'accord sur les principaux éléments des moyens à utiliser, par exemple les données qui seront enregistrées, la façon dont les réservations seront attribuées et confirmées, et les personnes qui pourront avoir accès aux informations conservées. Elles décident également de partager les données de leurs clients afin de réaliser des actions commerciales intégrées.

Dans cet exemple, l'agence de voyages, la compagnie aérienne et la chaîne d'hôtels contrôleront conjointement la façon dont les données à caractère personnel de leurs clients respectifs sont traitées, et elles seront donc coresponsables en ce qui concerne les opérations de traitement se rapportant à la plateforme de réservation commune sur Internet. Toutefois, chacune d'elles demeurera exclusivement responsable des autres activités de traitement, notamment celles ayant trait à la gestion de leurs ressources humaines.

21

Dans certains cas, différents acteurs traitent les mêmes données à caractère personnel les uns à la suite des autres. Dans ce cas, il est probable qu'au niveau individuel, les différentes opérations de traitement de la chaîne semblent déconnectées, chacune d'elles pouvant avoir une finalité différente. Il sera néanmoins nécessaire de vérifier si, d'un point de vue global, les opérations de traitement ne doivent pas être considérées comme un «ensemble d'opérations» poursuivant une finalité commune ou utilisant des moyens déterminés conjointement.

Les deux exemples suivants illustrent cette idée en présentant deux scénarios possibles.

Exemple n° 9: Transfert de données sur les employés à l'administration fiscale

La société XYZ collecte et traite les données à caractère personnel de ses employés pour gérer les salaires, les missions, les assurances-maladie, etc. Mais une loi oblige également la société à envoyer toutes les données concernant les salaires à l'administration fiscale, en vue de renforcer le contrôle fiscal.

Dans cet exemple, même si la société XYZ et l'administration fiscale traitent les mêmes données relatives aux salaires, l'absence de finalités ou de moyens communs concernant ce traitement de données fait que les deux entités sont deux responsables du traitement distincts.

Exemple n° 10: Transactions financières

Prenons maintenant l'exemple d'une banque qui a recours à un service de messagerie financière pour réaliser ses transactions financières. La banque et le service de messagerie conviennent des moyens du traitement des données financières. Le traitement des données à caractère personnel concernant les transactions financières est réalisé en premier lieu par l'établissement financier et, seulement après, par le service de messagerie financière. Cependant, même si au niveau individuel, chacune de ces entités poursuit sa propre finalité, au niveau global, les différentes phases, les finalités et les moyens du traitement sont étroitement liés. Dans cet exemple, la banque et le service de messagerie peuvent être considérés comme coresponsables.

Il est également possible que les différents acteurs concernés déterminent conjointement, parfois dans une mesure différente, les finalités et/ou les moyens d'une opération de traitement.

Dans certains cas, chaque responsable du traitement est chargé d'une partie du traitement seulement, mais les informations sont rassemblées et traitées via une plateforme.

Exemple n° 11: Portails des administrations en ligne

Les portails des administrations en ligne servent d'intermédiaires entre les citoyens et les services de l'État: le portail transfère les demandes des citoyens et conserve les documents des administrations publiques à l'usage des citoyens. Chaque administration publique demeure responsable du traitement des données traitées pour ses propres besoins. Néanmoins, le portail lui-même peut également être considéré comme un responsable du traitement.

22

En effet, il traite (en l'occurrence, il collecte et transfère au service compétent) les demandes des citoyens ainsi que les documents publics (il les conserve et régit leur accès, tel que le téléchargement par les citoyens) à des fins autres (facilitation des services d'administration en ligne) que celles pour lesquelles les données sont initialement traitées par chaque administration publique. Ces responsables du traitement devront, entre autres obligations, garantir la sécurité du système de transfert des données à caractère personnel depuis l'utilisateur vers l'administration concernée, puisqu'au niveau global, ce transfert est une composante essentielle de l'ensemble des opérations de traitement réalisées par l'intermédiaire du portail.

Une autre structure possible est «la méthode basée sur l'origine», dans laquelle chaque responsable du traitement est responsable des données qu'il introduit dans le système. C'est le cas de certaines bases de données européennes, où la responsabilité, et donc l'obligation de donner suite aux demandes d'accès et de rectification, est attribuée sur la base de l'origine nationale des données à caractère personnel.

Les réseaux sociaux en ligne sont un autre exemple intéressant.

Exemple n° 12: Réseaux sociaux

Les fournisseurs de réseaux sociaux proposent des plateformes de communication en ligne qui permettent aux utilisateurs de publier et d'échanger des informations avec d'autres utilisateurs. Ces fournisseurs de services sont des responsables du traitement car ils déterminent à la fois les finalités et les moyens du traitement de ces informations. Les utilisateurs de ces réseaux, qui chargent également les données à caractère personnel de tiers, pourraient être responsables du traitement à condition que leurs activités ne soient pas soumises à «l'exemption domestique»[17].

Après ces cas de détermination conjointe d'une partie seulement des finalités et des moyens, un exemple explicite et dépourvu de toute ambiguïté est celui dans lequel de multiples entités déterminent conjointement et partagent l'ensemble des finalités et des moyens des opérations de traitement, donnant naissance à une coresponsabilité à part entière.

Dans l'exemple, il est aisé de déterminer qui est compétent et en mesure de garantir les droits des personnes concernées, et tenu de respecter les obligations en matière de protection des données. En revanche, il devient bien plus difficile de déterminer quel responsable du traitement est compétent et responsable au regard de la loi, pour quels droits et obligations des personnes concernées, lorsque les différents coresponsables partagent les finalités et les moyens du traitement de façon inégale.

Nécessité d'une clarification du partage des responsabilités

Il convient avant tout de souligner que, surtout en cas de coresponsabilité, l'incapacité à s'acquitter directement de toutes les obligations qui incombent au responsable du traitement (garantir l'information, le droit d'accès, etc.) n'exclut pas la possibilité d'être responsable du traitement. Il se peut que, dans la pratique, ces obligations puissent facilement être assumées par d'autres parties, parfois plus proches de la personne concernée, pour le compte du responsable du traitement. Mais ce dernier demeurera toujours lié, en dernier ressort, par ses obligations et sa responsabilité pourra être engagée en cas de non-respect de ces dernières.

[17] Pour plus de détails et d'exemples, voir l'Avis 5/2009 du Groupe de travail «article 29» sur les réseaux sociaux en ligne, adopté le 12 juin 2009 (WP 163).

Selon un texte antérieur présenté par la Commission au cours du processus d'adoption de la directive, le fait d'avoir accès à certaines données à caractère personnel aurait entraîné la qualification de (co)responsable du traitement de ces données. Cette formulation n'a cependant pas été retenue dans le texte final et l'expérience démontre que, d'une part, l'accès aux données n'entraîne pas nécessairement une telle responsabilité, et que, d'autre part, le fait d'avoir accès aux données n'est pas une condition essentielle pour être responsable du traitement. Dès lors, dans des systèmes complexes qui font intervenir de multiples acteurs, l'accès aux données à caractère personnel et les autres droits des personnes concernées peuvent être garantis à différents niveaux par différents acteurs.

Les conséquences juridiques portent également sur la responsabilité des responsables du traitement, ce qui soulève notamment la question de savoir si la «coresponsabilité» prévue par la directive emporte toujours une responsabilité solidaire. L'article 23 sur la responsabilité mentionne l'expression «responsable du traitement» au singulier, laissant entendre que la réponse est positive. Cependant, comme cela a déjà été mentionné, il peut y avoir plusieurs façons d'agir «conjointement avec», c'est-à-dire «ensemble avec». Cela peut parfois se traduire par une responsabilité solidaire, mais pas systématiquement: bien souvent, les différents responsables du traitement peuvent être chargés, et donc responsables, du traitement de données à caractère personnel à différents stades et à différents degrés.

L'essentiel est de garantir, même dans des environnements complexes de traitement des données, où différents responsables du traitement jouent un rôle dans le traitement de données à caractère personnel, le respect des règles de protection des données et une attribution claire des responsabilités en cas d'infraction à ces dispositions, afin d'éviter que la protection des données à caractère personnel ne soit affaiblie ou qu'un «conflit négatif de compétence» et des failles n'apparaissent, auquel cas certaines obligations ou droits découlant de la directive ne seraient assumés par aucune des parties.

Dans cette éventualité, plus que jamais, il importe que des informations claires soient fournies aux personnes concernées, précisant les différentes étapes et acteurs du traitement. Il convient également de préciser si tous les responsables du traitement sont compétents pour faire respecter l'ensemble des droits des personnes concernées, ou d'indiquer le responsable du traitement compétent pour chaque droit.

Exemple n° 13: Banques et pools d'information sur les clients défaillants

Plusieurs banques peuvent mettre en place un «pool d'informations» commun (lorsque la législation nationale autorise sa création) dans lequel chacune d'elles consigne des informations (données) sur les clients défaillants et dispose d'un accès total. Certaines législations exigent que toutes les demandes des personnes concernées, par exemple les demandes d'accès ou d'effacement, puissent se faire à un «point d'entrée» unique, le fournisseur. Celui-ci est chargé de trouver le responsable du traitement approprié et de veiller à ce que les réponses correctes soient communiquées à la personne concernée. L'identité du fournisseur est publiée dans le registre du traitement des données. Dans d'autres pays, de tels pools d'informations peuvent être gérés par des personnes morales distinctes faisant office de responsable du traitement, tandis que les demandes d'accès sont gérées par les banques adhérentes qui agissent comme son intermédiaire.

24

Exemple n° 14: Publicité comportementale

La publicité comportementale utilise les informations collectées sur le comportement de navigation d'un internaute, comme les pages visitées ou les recherches effectuées, pour sélectionner les publicités qui lui seront présentées. Les diffuseurs, qui louent très souvent des espaces publicitaires sur leurs sites web, ainsi que les fournisseurs de réseaux publicitaires, qui remplissent ces espaces avec des publicités ciblées, peuvent ainsi collecter et échanger des informations sur les utilisateurs, selon les accords conclus.

Du point de vue de la protection des données, le diffuseur doit être considéré comme un responsable du traitement autonome puisqu'il collecte des données à caractère personnel auprès de l'utilisateur (profil utilisateur, adresse IP, emplacement de mémoire, langue du système d'exploitation, etc.) pour son propre compte. Le fournisseur de réseau publicitaire sera également responsable du traitement dès lors qu'il détermine les finalités (suivre les utilisateurs sur les différents sites web) ou les moyens essentiels du traitement de données. En fonction des conditions de collaboration qui ont été fixées entre le diffuseur et le fournisseur de réseau publicitaire, par exemple si le premier permet le transfert de données à caractère personnel vers le second, notamment en redirigeant l'utilisateur vers la page web du fournisseur de réseau publicitaire, ils peuvent être coresponsables du traitement pour l'ensemble des opérations de traitement conduisant à la publicité comportementale.

Dans tous les cas, les (co)responsables du traitement doivent veiller à ce que la complexité et les technicités du mécanisme de publicité comportementale ne les empêchent pas de trouver les moyens appropriées de se conformer aux obligations qui incombent aux responsables du traitement, et garantir le respect des droits des personnes concernées. Cela comprend notamment:

- *l'information* de l'utilisateur sur le fait que ses données sont accessibles par un tiers: cette information pourra être assurée plus efficacement par le diffuseur, qui est le principal interlocuteur de l'utilisateur, et
- les conditions d'*accès* aux données à caractère personnel: le fournisseur de réseau publicitaire devra répondre aux questions des utilisateurs sur la manière dont il exploite la base des données des utilisateurs pour sa publicité ciblée, et donner suite aux demandes de rectification et d'effacement.

En outre, les diffuseurs et les fournisseurs de réseau publicitaire peuvent être tenus de respecter d'autres obligations découlant du droit civil et du droit de la consommation, y compris en matière de responsabilité délictuelle et de pratiques commerciales déloyales.

Conclusion préliminaire

Les parties qui agissent conjointement disposent d'une certaine latitude pour attribuer et se répartir les obligations et les responsabilités, pour autant qu'elles en garantissent le respect absolu. Les conditions régissant l'exercice des responsabilités conjointes doivent en principe être déterminées par les responsables du traitement. Il convient cependant de prendre également en considération les circonstances de fait, afin de vérifier si ces accords reflètent bien la réalité du traitement des données qui en est l'objet.

25

Dans cette perspective, l'évaluation de la coresponsabilité doit tenir compte, d'une part, de la nécessité de garantir le plein respect des règles de protection des données et, d'autre part, du fait que la multiplication des responsables du traitement risque d'aboutir à une complexité non souhaitable et à un manque de clarté dans la répartition des responsabilités. L'intégralité du traitement pourrait en devenir illicite, par manque de transparence, et il en résulterait une violation du principe de traitement loyal.

Exemple n° 15: Plateformes de gestion des données médicales

Dans un État membre, une administration publique met en place un point d'échange national qui règle l'échange des données sur les patients entre les prestataires de soins de santé. La pléthore de responsables du traitement (plusieurs dizaines de milliers) se traduit par une situation tellement floue pour les personnes concernées (les patients) que la protection de leurs droits serait menacée. En effet, ces personnes ne sauraient pas vers qui se tourner pour introduire une réclamation, poser des questions ou demander des informations, une rectification ou l'accès à leurs données à caractère personnel. En outre, l'administration publique est chargée de la conception du traitement et de la façon dont il est utilisé. Compte tenu de ces éléments, l'administration publique ayant mis en place le point d'échange doit être considérée comme un coresponsable, mais également comme un point de contact pour les demandes des personnes concernées.

Dans ce contexte, on peut affirmer, et donc partir du principe, que la responsabilité solidaire de toutes les parties en cause doit être considérée comme un moyen de dissiper les incertitudes, pour autant qu'aucune autre attribution claire et tout aussi efficace des obligations et des responsabilités n'ait été décidée par les personnes en cause ou ne découle clairement des circonstances de fait.

III.2. Définition du sous-traitant

La notion de sous-traitant n'était pas définie dans la convention 108. Le rôle de sous-traitant a été reconnu pour la première fois dans la première proposition de la Commission, sans pour autant que cette notion soit introduite, en vue *«d'éviter qu'un traitement par un tiers pour le compte du responsable du fichier ait pour conséquence d'affaiblir la protection de la personne concernée»*. Ce n'est qu'avec la proposition modifiée de la Commission, et à la suite d'une proposition faite par le Parlement européen, que la notion de sous-traitant a été formulée de manière explicite et autonome, avant de prendre la forme actuelle dans la position commune du Conseil.

Tout comme la définition du responsable du traitement, celle du sous-traitant envisage un large éventail d'acteurs pour tenir ce rôle («… une personne physique ou morale, une autorité publique, une service ou tout autre organisme …»).

L'existence d'un sous-traitant dépend du responsable du traitement, qui peut décider soit de traiter les données au sein de son organisation, par exemple en habilitant des collaborateurs à traiter les données sous son autorité directe (voir, a contrario, l'article 2, point f)), soit de déléguer tout ou partie des activités de traitement à une organisation extérieure, comme l'indique l'exposé des motifs de la proposition modifiée de la Commission, par «une personne juridiquement distincte du responsable mais agissant pour son compte».

26

Par conséquent, les deux conditions fondamentales pour agir en qualité de sous-traitant sont, d'une part, d'être une entité juridique distincte du responsable du traitement et, d'autre part, de traiter les données à caractère personnel pour le compte de ce dernier. L'activité de traitement peut se limiter à une tâche ou un contexte bien précis, ou être plus générale et étendue.

En outre, le rôle de sous-traitant ne découle pas de la nature de l'entité traitant des données mais de ses activités concrètes dans un cadre précis. En d'autres termes, la même entité peut agir à la fois en qualité de responsable du traitement pour certaines opérations de traitement et en tant que sous-traitant pour d'autres opérations, et la qualification de responsable ou de sous-traitant doit être évaluée au regard d'un ensemble spécifique de données ou d'opérations.

Exemple n° 16: Fournisseurs de services Internet proposant des services d'hébergement

Un FSI qui propose des services d'hébergement est, en principe, un sous-traitant des données à caractère personnel publiées en ligne par ses clients, qui recourent à ce FSI pour l'hébergement et la maintenance de leur site web. Si en revanche le FSI traite ultérieurement, à des fins personnelles, les données figurant sur les sites web, il devient alors le responsable du traitement en ce qui concerne cette opération de traitement précise. L'analyse serait différente pour un FSI fournissant des services de courrier électronique ou d'accès à Internet (voir également l'exemple n° 1: opérateurs de télécommunications).

L'aspect le plus important est l'exigence que le sous-traitant agisse «…pour le compte du responsable de traitement…». «Agir pour le compte de» signifie servir les intérêts d'un tiers et renvoie à la notion juridique de délégation. Dans le cas de la législation relative à la protection des données, un sous-traitant est amené à exécuter les instructions données par le responsable du traitement, au moins en ce qui concerne la finalité du traitement et les éléments essentiels des moyens.

Dans cette perspective, la licéité de l'activité de traitement de données du sous-traitant est déterminée par le mandat donné par le responsable du traitement. Un sous-traitant qui outrepasse son mandat et acquiert un rôle important dans la détermination des finalités ou des moyens essentiels du traitement est davantage un (co)responsable qu'un sous-traitant. La question de la licéité de ce traitement sera néanmoins examinée à la lumière d'autres articles (6 à 8). En revanche, la délégation peut impliquer une certaine liberté d'appréciation sur la façon de servir au mieux les intérêts du responsable du traitement, permettant au sous-traitant de choisir les moyens techniques et d'organisation les plus appropriés.

Exemple n° 17: Externalisation de services de courrier

Des organismes privés fournissent des services de courrier pour le compte d'agences (publiques), par exemple l'envoi des allocations familiales et de maternité au nom de la caisse nationale de sécurité sociale. Dans ce cas, une autorité chargée de la protection des données a indiqué que les organismes privés en question devaient être désignés comme sous-traitants car leur tâche, bien qu'exécutée avec un certain degré d'autonomie, se limitait à une partie seulement des opérations de traitement nécessaires aux finalités déterminées par le responsable du traitement des données.

27

Toujours en vue de garantir que l'externalisation et la délégation n'entraînent pas une baisse du niveau de protection des données, la directive contient deux dispositions qui visent précisément le sous-traitant et qui définissent de façon très détaillée ses obligations en matière de confidentialité et de sécurité:

- l'article 16 dispose que le sous-traitant lui-même, ainsi que toute personne agissant sous son autorité qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement;

- l'article 17, qui porte sur la sécurité des traitements, requiert un contrat ou un acte juridique contraignant qui régit les relations entre le responsable du traitement et le sous-traitant. Ce contrat doit revêtir la forme écrite aux fins de preuve et contenir un minimum de clauses, stipulant notamment que le sous-traitant n'agit que sur la seule instruction du responsable du traitement et met en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel. Le contrat doit comporter une description suffisamment détaillée du mandat du sous-traitant.

À cet égard, il convient d'observer que les prestataires de services spécialisés dans certaines opérations de traitement de données (par exemple, le paiement des salaires) établissent fréquemment des prestations et des contrats standards à signer par les responsables du traitement, fixant de facto un certain mode de traitement standardisé des données à caractère personnel[18]. Cependant, le fait que le contrat et ses conditions générales détaillées soient préparés par le prestataire de services plutôt que par le responsable du traitement ne suffit pas *en soi* à conclure que le premier doit être considéré comme un responsable du traitement, pour autant que le responsable du traitement ait librement accepté les clauses contractuelles, assumant de ce fait une totale responsabilité vis-à-vis de ces dernières.

Dans le même ordre d'idée, le faible poids contractuel d'un petit responsable du traitement face à d'importants prestataires de services ne doit pas lui servir de justification pour accepter des clauses et conditions contractuelles contraires à la législation sur la protection des données.

Exemple n° 18: Plateformes de courriel

John Smith recherche une plateforme de courriel qu'il pourrait utiliser avec les cinq employés de sa société. Il découvre qu'une plateforme conviviale conforme à ses besoins (également la seule proposée gratuitement) conserve les données à caractère personnel pendant une durée excessive et qu'elle les transfère à des pays tiers sans aucune garantie appropriée. En outre, les clauses contractuelles sont «à prendre ou à laisser».

Dans cet exemple, M. Smith devrait soit chercher un autre fournisseur soit, en cas de non-respect allégué des règles de protection des données ou d'absence sur le marché d'autres fournisseurs adaptés, en référer aux autorités compétentes, par exemple celles chargées de la protection des données, les associations de protection des consommateurs et les autorités de la concurrence, etc.

[18] La rédaction des clauses contractuelles par le prestataire de services ne remet pas en cause le fait que les aspects essentiels du traitement, décrits au point III.1.b, sont déterminés par le responsable du traitement.

28

Le fait que la directive exige un contrat écrit pour garantir la sécurité du traitement ne signifie pas qu'il ne peut y avoir de relations entre responsables du traitement et sous-traitants sans contrat préalable. Dans ce contexte, le contrat n'est ni constitutif ni déterminant des relations entre les parties, même s'il peut aider à mieux les comprendre[19]. C'est pourquoi, dans ce cas également, il convient d'adopter une approche fonctionnelle, en analysant les éléments de fait de la relation entre les différents sujets et la façon dont les finalités et les moyens du traitement sont déterminés. Lorsqu'une relation entre responsable du traitement/sous-traitant est avérée, ces parties sont obligées de conclure un contrat conformément à la loi (cf. article 17 de la directive).

Pluralité de sous-traitants

Il est de plus en plus fréquent qu'un responsable du traitement confie le traitement de données à caractère personnel à plusieurs sous-traitants. Ceux-ci peuvent entretenir une relation directe avec le responsable du traitement des données, ou être des sous-contractants auxquels les sous-traitants ont délégué une partie des activités de traitement qui leur ont été confiées.

Ces structures complexes (à plusieurs niveaux ou diffuses) de traitement des données à caractère personnel se multiplient avec les nouvelles technologies et certains droits nationaux en font expressément mention. Aucune disposition de la directive n'empêche de désigner, pour des raisons d'organisation, plusieurs entités comme sous-traitants ou (sous-)sous-traitants, notamment en subdivisant les tâches en question. Ces structures sont cependant toutes tenues de se conformer aux instructions données par le responsable du traitement pour procéder au traitement.

Exemple n° 19: Grilles informatiques

Les grandes infrastructures de recherche ont de plus en plus recours à l'informatique répartie, et notamment aux grilles, pour tirer parti de capacités de calcul et de stockage accrues. Des grilles sont installées dans différentes infrastructures de recherche implantées dans divers pays. Une grille européenne peut, par exemple, être composée de grilles nationales qui relèvent elles-mêmes de la responsabilité d'un organisme national. Mais cette grille européenne n'aura peut-être aucun organisme central responsable de son fonctionnement. Les chercheurs qui utilisent ce type de grille ne peuvent généralement pas déterminer l'endroit exact où leurs données sont traitées, et ne peuvent donc pas connaître le responsable du traitement (la situation est encore plus compliquée si les infrastructures de grilles se trouvent dans des pays tiers). Lorsqu'une infrastructure de grilles utilise les données d'une manière non autorisée, elle peut être considérée comme responsable du traitement des données, si elle n'agit pas pour le compte des chercheurs.

Le problème central ici est que, compte tenu de la pluralité d'acteurs qui participent au processus, les obligations et les responsabilités imposées par la législation relative à la protection des données doivent être clairement attribuées et non pas se dispersées tout au

[19] Il peut cependant arriver que l'existence d'un contrat écrit soit une condition nécessaire pour être automatiquement considéré comme un sous-traitant dans certaines conditions. En Espagne, par exemple, le rapport sur les centres d'appel définit comme sous-traitants tous les centres d'appel des pays tiers, pour autant qu'ils respectent les clauses contractuelles. Il en est ainsi même si le contrat a été rédigé par le sous-traitant et si le responsable du traitement se borne à y «adhérer».

29

long de la chaîne d'externalisation/sous-traitance. Autrement dit, il faut proscrire les chaînes de (sous-)sous-traitants qui affaiblissent, voire empêchent un contrôle efficace et une véritable responsabilité des activités de traitement, sauf si les responsabilités des différentes parties de la chaîne sont clairement établies.

Dès lors, dans le même ordre d'idées que ce qui est décrit au paragraphe III.1, point b), s'il n'est pas nécessaire que le responsable du traitement définisse et convienne de tous les détails des moyens utilisés pour poursuivre les finalités envisagées, il faut néanmoins qu'il soit au moins informé des principaux éléments de la structure de traitement (les sujets concernés, les mesures de sécurité, les garanties de traitement dans les pays tiers, etc.), afin d'être toujours en mesure de contrôler les données traitées pour son compte.

Il convient en outre de rappeler que, si la directive fait porter la responsabilité juridique au responsable du traitement, elle n'empêche pas les législations sur la protection des données d'engager également la responsabilité du sous-traitant dans certains cas.

Certains critères peuvent servir à déterminer la qualification des divers sujets participant au traitement:

- le nombre d'instructions préalables données par le responsable du traitement, qui détermine la marge de manœuvre laissée au sous-traitant;

- la surveillance exercée par le responsable du traitement sur l'exécution du service. Un contrôle permanent et rigoureux afin de s'assurer que le sous-traitant se conforme totalement aux instructions et aux clauses contractuelles indique que le responsable du traitement maîtrise totalement et exclusivement les opérations de traitement;

- la visibilité/l'image donnée par le responsable du traitement à la personne concernée, et les attentes que cette visibilité suscite chez les personnes concernées;

Exemple n° 20: Centres d'appel

Un responsable du traitement des données confie à un centre d'appels certaines de ses activités et lui demande de se présenter sous son identité lorsqu'il appelle ses clients. Dans cet exemple, les attentes des clients et la façon dont le responsable du traitement se présente à eux par l'intermédiaire de la société sous-traitante conduisent à conclure que le centre agit en tant que sous-traitant des données pour (le compte de) le responsable du traitement.

- l'expertise des parties: dans certains cas, le rôle traditionnel et l'expertise professionnelle du prestataire de services jouent un rôle prépondérant, pouvant entraîner sa qualification de responsable du traitement.

Exemple n° 21: Avocats

Un avocat représente son client en justice, et dans le cadre de cette mission, il traite des données à caractère personnel qui figurent dans le dossier de l'affaire. Le fondement juridique de l'utilisation des informations nécessaires est le mandat donné par son client.

30

Or ce mandat ne porte pas sur le traitement des données mais sur la représentation en justice, activité pour laquelle ces professions disposent généralement de leur propre fondement juridique. Ces professionnels doivent donc être considérés comme des «responsables du traitement» indépendants lorsqu'ils traitent des données dans le cadre de la représentation de leurs clients.

Dans un autre contexte, une évaluation plus approfondie des moyens mis en place pour parvenir aux finalités escomptées peut également s'avérer déterminante.

Exemple n° 22: Site web d'«objets perdus»

Un site web d'«objets perdus» a été présenté comme un simple sous-traitant, au motif que ce serait les personnes qui publient les annonces d'objets perdus qui déterminent le contenu et donc, au niveau individuel, la finalité (par exemple, retrouver une broche, un perroquet etc.). Une autorité chargée de la protection des données a rejeté cet argument. Le site web a été créé dans le but commercial de tirer profit de la publication d'annonces d'objets perdus et le fait que le site ne décide pas quels objets seront annoncés (contrairement aux catégories d'objets) n'est pas déterminant puisque que la définition de «responsable du traitement» n'inclut pas expressément la détermination d'un contenu. Le site web détermine les conditions de publication des annonces, etc., et il est responsable de la décence du contenu.

Alors qu'il aurait pu y avoir une tendance à généralement considérer l'externalisation comme une activité de sous-traitant, les situations et les évaluations sont aujourd'hui souvent bien plus complexes.

Exemple n° 23: Comptables

La qualification des comptables peut varier en fonction du contexte. Lorsque les comptables fournissent des services au public et aux petits commerçants sur la base d'instructions très générales («préparer ma déclaration de revenus»), le comptable est un responsable du traitement (tout comme les avocats qui interviennent dans des situations analogues et pour des raisons similaires). En revanche, lorsqu'un comptable est engagé par une société et qu'il reçoit des instructions détaillées du comptable de cette dernière, peut-être pour procéder à un audit détaillé, et qu'il n'est pas un employé permanent, il sera considéré comme un sous-traitant, en raison du caractère explicite des instructions et de la marge de manœuvre limitée qui en résulte. Cette analyse connaît cependant une exception majeure, à savoir que lorsqu'ils estiment avoir découvert des irrégularités qu'ils sont obligés de signaler, dans ce cas, en raison des obligations professionnelles auxquelles ils sont tenus, les comptables agissent de manière autonome en tant que responsables du traitement.

Parfois, la complexité des opérations de traitement peut amener à mettre davantage l'accent sur la marge de manœuvre dont disposent les personnes auxquelles le traitement des données à caractère personnel a été confié, par exemple lorsque le traitement comporte un risque pour la protection des données. L'introduction de nouveaux moyens de traitement pourrait favoriser la qualification de responsable du traitement plutôt que de sous-traitant. Ces exemples peuvent également conduire à une clarification (et une désignation du responsable du traitement) expressément prévue par le droit.

31

Exemple n° 24: Traitement à des fins historiques, scientifiques et statistiques

S'agissant du traitement de données à caractère personnel à des fins historiques, scientifiques et statistiques, le droit national peut introduire la notion d'organisation intermédiaire pour désigner l'organisme chargé de transformer les données non codées en données codées, afin que le responsable du traitement à des fins historiques, scientifiques et statistiques ne soit pas en mesure d'identifier à nouveau les personnes concernées.

Si plusieurs responsables d'opérations de traitement initial transmettent les données à un ou plusieurs tiers pour un traitement ultérieur à des fins historiques, scientifiques et statistiques, les données sont tout d'abord codées par une organisation intermédiaire. Dans ce cas, celle-ci peut être considérée comme responsable du traitement en application de règlements nationaux, et elle est tenue au respect de toutes les obligations qui en découlent (pertinence des données, information de la personne concernée, notification etc.). En effet, lorsque des données provenant de différentes sources sont rassemblées, leur protection est particulièrement menacée, ce qui justifie la responsabilité propre de l'organisation intermédiaire. Par conséquent, cette dernière n'est pas seulement considérée comme un sous-traitant, mais également comme un responsable du traitement en vertu du droit national.

Dans le même ordre d'idée, le pouvoir de décision autonome conféré aux différentes parties participant au traitement est un élément à prendre en considération. L'exemple des essais cliniques de médicaments montre que la relation entre les bailleurs de fonds et les sociétés externes chargées de procéder aux essais dépend de la marge de manœuvre laissée à ces dernières pour le traitement des données. Il peut donc y avoir plus d'un responsable du traitement, mais également plus d'un sous-traitant ou plus d'une personne chargée du traitement.

Exemple n° 25: Essais cliniques de médicaments

La société pharmaceutique XYZ finance certains essais de médicaments et sélectionne les centres d'essai candidats en analysant leur admissibilité et leurs intérêts respectifs; elle élabore le protocole d'essai, fournit les indications nécessaires aux centres en ce qui concerne le traitement des données, et vérifie que les centres se conforment au protocole et aux procédures internes.

Bien que le bailleur de fonds ne collecte aucune donnée directement, il acquiert les données des patients rassemblées par les centres d'essai et les traite de diverses façons (en évaluant les informations que contiennent les documents médicaux; en recevant les données relatives aux effets indésirables; en saisissant ces données dans la base de données correspondante; en procédant à des analyses statistiques pour parvenir aux résultats de l'essai). Le centre d'essai réalise les essais de façon autonome, mais conformément aux indications du bailleur de fonds; il fournit les notes d'information aux patients et obtient leur consentement pour le traitement des données les concernant; il permet aux collaborateurs du bailleur de fonds d'accéder aux documents médicaux originaux des patients dans le cadre des activités de suivi; il gère ces documents et est responsable de leur conservation. Il apparaît donc que les responsabilités sont confiées aux acteurs individuels.

Dans ce contexte, tant les centres d'essai que les bailleurs de fonds prennent des décisions importantes en ce qui concerne la façon dont les données à caractère

32

personnel relatives aux essais cliniques sont traitées. Ils peuvent de ce fait être considérés comme coresponsables du traitement. La relation entre le bailleur de fonds et les centres d'essai pourrait être interprétée différemment si le bailleur de fonds déterminait les finalités et les éléments essentiels des moyens et si le chercheur ne disposait que d'une marge de manœuvre très réduite.

III.3. Définition des tiers

La notion de «tiers» n'était pas définie dans la convention 108; elle a été introduite par la proposition modifiée de la Commission, à la suite d'un amendement proposé par le Parlement européen. Selon l'exposé des motifs, l'amendement a été reformulé de manière à préciser que les tiers ne comprennent pas la personne concernée, le responsable du traitement et toute personne autorisée à traiter les données sous l'autorité directe du responsable du traitement ou du sous-traitant ou pour leur compte, comme c'est le cas du sous-traitant. Ce qui signifie que «*les personnes travaillant pour une autre organisation, même si celle-ci appartient au même groupe ou à la même holding, seront généralement des tiers*» tandis que «*les agences d'une banque traitant les comptes de clients sous l'autorité directe de leur siège ne seraient pas des tiers*».

La directive emploie le terme «tiers» d'une façon qui n'est pas sans rappeler celle dont cette notion est normalement utilisée dans le droit civil, le tiers étant généralement un sujet qui ne fait pas partie d'une entité ou d'un accord. Dans le cadre de la protection des données, cette notion doit être interprétée comme désignant tout sujet qui n'a aucune légitimité ni autorisation (qui pourrait découler, par exemple, de son rôle de responsable du traitement, de sous-traitant, ou d'employé de ceux-ci) pour traiter des données à caractère personnel.

La directive mentionne cette notion dans nombre de ses dispositions, généralement pour établir des interdictions, des limitations et des obligations dans l'éventualité où les données à caractère personnel pourraient être traitées par d'autres personnes qui, au départ, n'étaient pas censées traiter certaines de ces données.

On peut ainsi conclure qu'un tiers recevant des données à caractère personnel, de manière licite ou non, serait en principe un nouveau responsable du traitement, pour autant que les autres conditions nécessaires à sa qualification en tant que tel et à l'application de la législation relative à la protection des données soient réunies.

Exemple n° 26: Accès non autorisé par un employé

Un employé d'une société, dans l'exercice de ses fonctions, prend connaissance de données à caractère personnel auxquelles il n'a pas le droit d'accéder. Dans ce cas, cet employé doit être considéré comme un «tiers» vis-à-vis de son employeur, avec toutes les conséquences et responsabilités en termes de licéité de communication et de traitement des données que cela entraîne.

IV. Conclusions

La notion de responsable du traitement des données et son interaction avec la notion de sous-traitant des données jouent un rôle central dans l'application de la directive 95/46/CE, car elles déterminent la ou les personnes chargées de faire respecter

des règles de protection des données, la manière dont les personnes concernées peuvent exercer leurs droits, le droit national applicable et le degré d'efficacité des autorités chargées de la protection des données.

Les modes d'organisation différenciés dans les secteurs public et privé, le développement des TIC ainsi que la mondialisation du traitement des données rendent plus complexe le traitement des données à caractère personnel et appellent à préciser ces notions, pour garantir la bonne application efficace et le respect de la directive dans la pratique.

La notion de responsable du traitement est autonome, en ce sens que son interprétation relève principalement de la législation européenne sur la protection des données, et fonctionnelle, car elle vise à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle repose par conséquent sur une analyse factuelle plutôt que formelle.

La définition énoncée dans la directive s'articule en trois volets: l'aspect individuel («*la personne physique ou morale, l'autorité publique, le service ou tout autre organisme*»); la possibilité d'une responsabilité pluraliste («*qui seul ou conjointement avec d'autres*»); et les éléments essentiels qui permettent de distinguer le responsable du traitement d'autres acteurs («*détermine les finalités et les moyens du traitement de données à caractère personnel*»).

L'analyse de ces volets conduit aux principales conclusions suivantes:

- Le pouvoir de «*déterminer* les finalités et les moyens ....» peut procéder de différents éléments de droit et/ou de fait: une compétence explicitement donnée par la loi, lorsqu'elle désigne le responsable du traitement ou qu'elle charge une personne, ou lui impose, de collecter et traiter certaines données; des règles juridiques générales ou des rôles traditionnels qui impliquent normalement une certaine responsabilité dans certaines organisations (par exemple, l'employeur vis-à-vis des données de ses employés); des circonstances factuelles et d'autres éléments (relations contractuelles, contrôle effectif exercé par une partie, visibilité envers les personnes concernées, etc.).

  Lorsqu'aucune de ces catégories ne peut être appliquée, la désignation d'un responsable du traitement doit être considérée comme «nulle». En effet, un organisme qui n'exerce ni influence de droit ni influence de fait pour déterminer la manière dont les données à caractère personnel seront traitées ne saurait être considéré comme un responsable du traitement.

  La détermination de la «finalité» du traitement entraîne la qualification de responsable du traitement (de fait). En revanche, la détermination des «moyens» du traitement peut être déléguée par le responsable du traitement, pour autant qu'elle concerne des questions techniques ou d'organisation. Mais les questions sensibles qui sont fondamentales pour la licéité du traitement, comme les données à traiter, la durée de conservation, l'accès, etc., doivent être déterminées par le responsable du traitement.

- L'aspect *personnel* de la définition renvoie à un vaste éventail de sujets susceptibles de jouer le rôle de responsable du traitement. Toutefois, dans la perspective stratégique d'attribution des responsabilités, il serait préférable de considérer comme responsable du traitement la société ou l'organisme en tant que tel, plutôt qu'une

personne en son sein. C'est en effet la société ou l'organisme qu'il convient de considérer, en dernier ressort, comme responsable du traitement des données et des obligations énoncées par la législation relative à la protection des données, à moins que certains éléments précis n'indiquent qu'une personne physique doit être responsable, par exemple lorsqu'une telle personne travaillant dans une société ou un organisme public utilise des données à des fins personnelles, en dehors des activités de la société.

- La possibilité d'une *responsabilité pluraliste* tient compte du nombre croissant de situations dans lesquelles différentes parties agissent en tant que responsables du traitement. L'évaluation de cette coresponsabilité doit être calquée sur celle de la responsabilité «unique», en adoptant une approche concrète et pratique, pour établir si les finalités et les éléments essentiels des moyens sont déterminés par plus d'une partie.

  La participation des parties à la détermination des finalités et des moyens de traitement dans le cadre d'une coresponsabilité peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale. Le présent avis présente maints exemples de différents types et degrés de coresponsabilité. Des degrés différents de contrôle peuvent donner lieu à divers degrés de responsabilité, et la responsabilité «solidaire» ne peut certainement pas être présumée dans tous les cas. De plus, il est tout à fait possible que, dans des systèmes complexes qui font intervenir de multiples acteurs, l'accès aux données à caractère personnel et l'exercice des autres droits des personnes concernées puissent aussi être garantis à différents niveaux par différents acteurs.

Le présent avis analyse également la notion de sous-traitant, dont l'existence dépend du responsable du traitement, qui peut décider soit de traiter les données au sein de son organisation soit de déléguer tout ou partie des activités de traitement à une organisation extérieure. Par conséquent, les deux conditions fondamentales pour agir en qualité de sous-traitant sont, d'une part, d'être une entité juridique distincte du responsable du traitement et, d'autre part, de traiter les données à caractère personnel pour le compte de ce dernier. L'activité de traitement peut se limiter à une tâche ou un contexte bien précis ou laisser une certaine marge d'appréciation sur la façon de servir les intérêts du responsable du traitement, permettant au sous-traitant de choisir les moyens techniques et d'organisation les plus appropriés.

En outre, le rôle de sous-traitant ne résulte pas de sa nature d'acteur traitant des données à caractère personnel mais de ses activités concrètes dans un cadre précis, par rapport à des ensembles spécifiques de données ou d'opérations. Certains critères peuvent aider à déterminer la qualification des divers acteurs participant au traitement: le nombre d'instructions préalables données par le responsable du traitement; la surveillance qu'il exerce sur le niveau du service; la visibilité vis-à-vis des personnes concernées; l'expertise des parties; le pouvoir de décision autonome laissé aux différentes parties.

Enfin, la catégorie des «tiers» comprend tout acteur qui n'a aucune légitimité ni autorisation (qui pourrait découler, par exemple, de son rôle de responsable du traitement, de sous-traitant, ou d'employé de ceux-ci) pour traiter des données à caractère personnel.

* * *

35

Le groupe de travail reconnaît la difficulté d'appliquer les définitions de la directive dans un environnement complexe qui permet d'envisager maints scénarios faisant intervenir des responsables du traitement et des sous-traitants, seuls ou conjointement avec d'autres, avec différents degrés d'autonomie et de responsabilité.

Dans son analyse, il a souligné la nécessité d'attribuer les responsabilités de sorte à garantir comme il se doit le respect des règles de protection des données dans la pratique. Il estime cependant n'avoir aucune raison de penser que la distinction actuelle entre responsables du traitement et sous-traitants n'est plus pertinente ni réaliste dans cette perspective.

Par conséquent, le groupe de travail espère que les explications figurant dans le présent avis, illustrées par des exemples concrets tirés de l'expérience quotidienne des autorités chargées de la protection des données, donneront des indications utiles pour l'interprétation de ces définitions fondamentales de la directive.

Fait à Bruxelles, le 16 février 2010

Pour le groupe de travail
Le président
Jacob KOHNSTAMM

36

Avis sur les techniques d'anonymisation (WP216)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

0829/14/FR
WP216

Avis 05/2014 sur les Techniques d'anonymisation

Adopté le 10 avril 2014

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Son secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale «Justice» de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

2

RÉSUMÉ

Dans le présent avis, le groupe de travail «Article 29» analyse l'efficacité et les limites des techniques d'anonymisation existantes dans le contexte juridique de la protection des données dans l'Union et formule des recommandations pour l'utilisation de ces techniques en tenant compte du risque résiduel d'identification inhérent à chacune d'elles.

Le groupe de travail «Article 29» convient de l'intérêt potentiel de l'anonymisation, notamment comme stratégie permettant aux citoyens et à la société en général de bénéficier des avantages des «données ouvertes», tout en atténuant les risques pour les personnes concernées. Cependant, les études de cas et les recherches publiées ont montré combien il est difficile de créer un ensemble de données vraiment anonymes en conservant suffisamment d'informations sous-jacentes pour les besoins de la tâche concernée.

Au regard de la directive 95/46/CE et d'autres instruments juridiques pertinents de l'Union, l'anonymisation est le résultat du traitement des données personnelles afin d'empêcher, de façon irréversible, toute identification. Ce faisant, les responsables du traitement des données doivent tenir compte de plusieurs éléments, en prenant en considération l'ensemble des moyens «susceptibles d'être raisonnablement mis en œuvre» à des fins d'identification (soit par le responsable du traitement, soit par un tiers).

L'anonymisation constitue un traitement ultérieur des données à caractère personnel; à ce titre, elle doit satisfaire à l'exigence de compatibilité au regard des motifs juridiques et des circonstances du traitement ultérieur. De plus, si les données anonymisées sortent du champ d'application de la législation sur la protection des données, les personnes concernées peuvent néanmoins avoir droit à une protection au titre d'autres dispositions (comme celles qui protègent la confidentialité des communications).

Les principales techniques d'anonymisation, à savoir la randomisation et la généralisation, sont décrites dans le présent avis. Il y est notamment question d'ajout de bruit, de permutation, de confidentialité différentielle, d'agrégation, de k-anonymat, de l-diversité et de t-proximité. Les principes, les points forts et les points faibles de ces techniques sont expliqués, de même que les erreurs courantes et les échecs qui se rapportent à l'utilisation de chaque technique.

L'avis examine la fiabilité de chaque technique sur la base de trois critères:

i) est-il toujours possible d'isoler un individu?

ii) est-il toujours possible de relier entre eux les enregistrements relatifs à un individu? et

iii) peut-on déduire des informations concernant un individu?

La connaissance des principales forces et faiblesses de chaque technique peut être utile pour décider comment concevoir un processus d'anonymisation adéquat dans un contexte donné.

Il est aussi question de la pseudonymisation, afin d'éviter certains écueils et idées fausses: la pseudonymisation n'est pas une méthode d'anonymisation. Elle réduit simplement la corrélation d'un ensemble de données avec l'identité originale d'une personne concernée et constitue par conséquent une mesure de sécurité utile.

La conclusion du présent avis est que les techniques d'anonymisation peuvent apporter des garanties en matière de respect de la vie privée et peuvent servir à créer des procédés d'anonymisation efficaces, mais uniquement si leur application est correctement conçue – ce qui suppose que les conditions préalables (le contexte) et les objectif(s) du processus d'anonymisation soient clairement définis de façon à parvenir à l'anonymisation visée, tout en produisant des données utiles. Le choix de la solution optimale devrait s'opérer au cas par cas, en utilisant éventuellement une combinaison de techniques différentes, sans perdre de vue les recommandations pratiques formulées dans cet avis.

Enfin, les responsables du traitement des données devraient être conscients qu'un ensemble de données anonymisées peut encore présenter des risques résiduels pour les personnes concernées. En effet, d'une part, l'anonymisation et la ré-identification sont des domaines de recherche très actifs où de nouvelles découvertes sont régulièrement publiées et, d'autre part, même des données anonymisées, comme les statistiques, peuvent servir à étoffer des profils existants, créant ainsi de nouveaux problèmes en termes de protection des données. C'est pourquoi l'anonymisation ne doit pas être considérée comme un exercice ponctuel: il appartient aux responsables du traitement des données de réévaluer régulièrement les risques associés.

4

1 Introduction

Alors que les appareils, les capteurs et les réseaux engendrent des volumes considérables et de nouveaux types de données et que le coût de leur stockage devient négligeable, les perspectives de réutilisation de ces données suscitent dans le public un intérêt et une demande qui ne cessent de croître. Les «données ouvertes» peuvent apporter des avantages évidents à la société, aux citoyens et aux organisations, à condition cependant que soit respecté le droit de chacun à la protection de ses données à caractère personnel et de sa vie privée.

L'anonymisation peut constituer une bonne stratégie afin de préserver ces avantages tout en atténuant les risques. Dès lors qu'un ensemble de données est vraiment anonymisé et que les individus ne sont plus identifiables, la législation européenne sur la protection des données ne s'applique plus. Toutefois, les études de cas et les travaux de recherche publiés font clairement ressortir toute la difficulté de créer un ensemble de données vraiment anonymes à partir d'une profusion de données à caractère personnel, en conservant suffisamment d'informations sous-jacentes pour les besoins de la tâche concernée. Par exemple, un ensemble de données considérées comme anonymes peut être combiné avec un autre ensemble de données de telle façon qu'un ou plusieurs individus deviennent identifiables.

Dans le présent avis, le groupe de travail «Article 29» analyse l'efficacité et les limites des techniques d'anonymisation existantes dans le contexte juridique de la protection des données dans l'Union et formule des recommandations pour une utilisation prudente et responsable de ces techniques afin de mettre en place un processus d'anonymisation.

2 Définitions et analyse juridique

2.1. Définitions dans le contexte législatif de l'Union

La directive 95/46/CE mentionne l'anonymisation au considérant 26 pour exclure les données anonymisées du champ d'application de la législation sur la protection des données:

> *«considérant que les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable; que, pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne; que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable; que les codes de conduite au sens de l'article 27 peuvent être un instrument utile pour fournir des indications sur les moyens par lesquels les données peuvent être rendues anonymes et conservées sous une forme ne permettant plus l'identification de la personne concernée»*[1].

[1] Il est à noter, de surcroît, que c'est aussi l'approche suivie dans le projet de règlement de l'Union sur la protection des données, au considérant 23: «Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne.»

Une lecture attentive du considérant 26 permet d'en tirer une définition conceptuelle de l'anonymisation. Le considérant 26 signifie que, pour rendre des données anonymes, il faut en retirer suffisamment d'éléments pour que la personne concernée ne puisse plus être identifiée. Plus précisément, les données doivent être traitées de façon à ne plus pouvoir être utilisées pour identifier une personne physique en recourant à «l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre», soit par le responsable du traitement, soit par un tiers. Un facteur important est que le traitement doit être irréversible. La directive ne précise pas comment un tel processus d'anonymisation devrait ou pourrait être exécuté[2]. L'accent est mis sur le résultat: il faut faire en sorte que les données ne permettent pas d'identifier la personne concernée par «l'ensemble» des moyens «susceptibles» d'être «raisonnablement» employés. Il est fait référence aux codes de conduite en tant qu'instrument utile pour envisager des mécanismes possibles d'anonymisation et de conservation des données sous une forme «ne permettant plus» l'identification de la personne concernée. La directive place donc manifestement la barre très haut.

La directive «vie privée et communications électroniques» (directive 2002/58/CE) évoque aussi l'anonymisation et les données anonymes dans une optique très similaire. Le considérant 26 indique:

> *«Il convient également d'effacer ou de rendre anonymes les données relatives au trafic utilisées pour la commercialisation de services de communications ou pour la fourniture de services à valeur ajoutée, lorsque les services en question ont été fournis.»*

En conséquence de quoi, l'article 6, paragraphe 1, dispose:

> *«Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.»*

De plus, conformément à l'article 9, paragraphe 1:

> *«Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée.»*

Le raisonnement qui sous-tend ces dispositions est que le résultat de l'anonymisation, en tant que technique appliquée aux données à caractère personnel, devrait être, dans l'état actuel de la technologie, aussi permanent qu'un effacement, c'est-à-dire qu'il devrait rendre impossible tout traitement de données à caractère personnel[3].

[2] Cette notion est approfondie en p. 9 du présent avis.

[3] Il convient de rappeler ici que l'anonymisation est aussi définie dans des normes internationales – notamment la norme ISO 29100 – comme étant le «processus par lequel des informations personnellement identifiables (IPI) sont irréversiblement altérées de telle façon que le sujet des IPI ne puisse plus être identifié directement ou indirectement, que ce soit par le responsable du traitement des IPI seul ou en collaboration avec une quelconque autre partie» (ISO 29100:2011). L'irréversibilité de l'altération subie par les données personnelles pour ne plus permettre l'identification directe ou indirecte est donc aussi un élément déterminant pour l'ISO. De ce point de vue, la norme présente une convergence considérable avec les principes et les notions qui sous-tendent la

2.2. Analyse juridique

L'analyse du libellé des dispositions relatives à l'anonymisation dans les principaux instruments de protection des données de l'Union permet de retenir quatre aspects essentiels:

- L'anonymisation peut être le résultat du traitement de données à caractère personnel dans le but d'empêcher irréversiblement l'identification de la personne concernée.

- Plusieurs techniques d'anonymisation peuvent être envisagées; il n'y a pas de normes prescriptives dans la législation de l'Union.

- Les éléments contextuels ont leur importance: il faut prendre en considération «l'ensemble» des moyens «susceptibles» d'être «raisonnablement» utilisés à des fins d'identification par le responsable du traitement ou par des tiers, en prêtant une attention particulière aux moyens que l'état actuel de la technologie a rendu récemment «susceptibles» d'être «raisonnablement» mis en œuvre (compte tenu de l'évolution de la puissance de calcul et des outils disponibles).

- Pour apprécier la validité d'une technique d'anonymisation, il faut tenir compte du facteur de risque qui lui est inhérent – et notamment des utilisations possibles des données «anonymisées» au moyen de cette technique – et évaluer la gravité et la probabilité de ce risque.

L'expression «technique d'anonymisation» est employée dans le présent avis, plutôt que les termes «anonymat» ou «données anonymes», afin d'insister sur le risque résiduel de ré-identification inhérent à toute mesure technique ou organisationnelle visant à rendre des données «anonymes».

2.2.1. Licéité du processus d'anonymisation

Premièrement, l'anonymisation est une technique appliquée aux données à caractère personnel afin d'empêcher irréversiblement leur identification. L'hypothèse de départ est donc que les données à caractère personnel doivent avoir été collectées et traitées dans le respect de la législation applicable en matière de conservation des données sous une forme identifiable.

Dans ce contexte, le processus d'anonymisation, désignant le traitement de telles données à caractère personnel en vue de les rendre anonymes, constitue un «traitement ultérieur». À ce titre, ce traitement doit satisfaire au critère de compatibilité conformément aux lignes directrices proposées par le groupe de travail «Article 29» dans son avis 03/2013 sur la limitation des finalités[4].

Il s'ensuit que la base juridique de l'anonymisation peut, en principe, résider dans l'un des motifs mentionnés à l'article 7 (notamment l'intérêt légitime poursuivi par le responsable du

directive 95/46/CE. Cela s'applique aussi aux définitions que l'on peut trouver dans certaines législations nationales (par exemple, en Italie, en Allemagne et en Slovénie), qui insistent sur le caractère non identifiable et qui font référence à l'«effort disproportionné» qu'exigerait une ré-identification (D, SI). La loi française relative à la protection des données prévoit néanmoins que les données conservent un caractère personnel même si la ré-identification de la personne concernée est rendue très difficile et improbable – c'est-à-dire qu'il n'y a pas de disposition renvoyant au critère du «caractère raisonnable».

[4] Avis 03/2013 du groupe de travail «Article 29», disponible à l'adresse: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

traitement des données) pour autant que les exigences de qualité des données visées à l'article 6 de la directive soient également satisfaites, en tenant dûment compte des circonstances spécifiques et de tous les facteurs mentionnés dans l'avis du groupe de travail «Article 29» sur la limitation des finalités[5].

D'un autre côté, il faut mentionner les dispositions énoncées à l'article 6, paragraphe 1, point e), de la directive 95/46/CE (mais aussi à l'article 6, paragraphe 1, et à l'article 9, paragraphe 1, de la directive «vie privée et communications électroniques»), qui soulignent la nécessité de conserver des données à caractère personnel «sous une forme permettant l'identification» pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.

En soi, cette exigence insiste sur le fait que les données à caractère personnel devraient, à tout le moins, être anonymisées «par défaut» (sous réserve de dispositions juridiques différentes, comme celles mentionnées dans la directive «vie privée et communications électroniques» à propos des données relatives au trafic). Si le responsable du traitement des données souhaite conserver ces données à caractère personnel après que les finalités du traitement original ou ultérieur ont été réalisées, des techniques d'anonymisation devraient être appliquées de façon à empêcher irréversiblement l'identification.

Par conséquent, le groupe de travail «Article 29» considère que l'anonymisation, en tant que traitement ultérieur de données à caractère personnel, peut être jugée compatible avec les finalités originales du traitement, à condition que le processus d'anonymisation soit de nature à produire des informations anonymisées au sens décrit dans le présent document.

Il faut ajouter que l'anonymisation doit demeurer conforme aux contraintes juridiques rappelées par la Cour de justice dans son arrêt C-553/07 (College van burgemeester en wethouders van Rotterdam/M.E.E. Rijkeboer), concernant la nécessité de conserver les données sous une forme identifiable pour permettre, par exemple, l'exercice des droits d'accès des personnes concernées. La Cour a jugé que *«[l]'article 12, sous a), de la directive [95/46/CE] impose aux États membres de prévoir un droit d'accès à l'information sur les destinataires ou les catégories de destinataires des données ainsi qu'au contenu de l'information communiquée non seulement pour le présent, mais aussi pour le passé. Il appartient aux États membres de fixer un délai de conservation de cette information ainsi qu'un accès corrélatif à celle-ci qui constituent un juste équilibre entre, d'une part, l'intérêt de la personne concernée à protéger sa vie privée, notamment au moyen des voies d'intervention et de recours prévus par la directive et, d'autre part, la charge que l'obligation de conserver cette information représente pour le responsable du traitement.»*

Cela vaut en particulier dans le cas où un responsable du traitement des données s'appuie sur l'article 7, point f), de la directive 95/46/CE, en ce qui concerne l'anonymisation: l'intérêt légitime poursuivi par le responsable du traitement des données doit toujours être mis en balance avec les droits et les libertés fondamentales des personnes concernées.

[5] Cela signifie notamment qu'il faut procéder à une appréciation matérielle à la lumière de toutes les circonstances pertinentes, en prêtant une attention particulière aux facteurs-clés suivants:
a) la relation entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur;
b) le contexte dans lequel les données à caractère personnel ont été collectées et les attentes raisonnables des personnes concernées à propos de leur utilisation ultérieure;
c) la nature des données à caractère personnel et l'impact du traitement ultérieur sur les personnes concernées;
d) les garanties appliquées par le responsable du traitement pour assurer un traitement équitable et éviter tout impact excessif sur les personnes concernées.

Par exemple, une enquête des autorités néerlandaises chargées de la protection des données DPA en 2012-2013 sur le recours à des technologies d'inspection approfondie des paquets par quatre opérateurs de téléphonie mobile a mis en évidence un fondement juridique, au titre de l'article 7, point f) de la directive 95/46/CE, justifiant l'anonymisation des contenus des données relatives au trafic dès que possible après la collecte de ces données. En effet, l'article 6 de la directive «vie privée et communications électroniques» stipule que les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes aussi rapidement que possible. Dans ce cas, dès lors que l'article 6 de la directive «vie privée et communications électroniques» le permet, il existe un fondement juridique correspondant dans l'article 7 de la directive sur la protection des données. L'inverse est vrai également: si un type de traitement de données n'est pas autorisé au titre de l'article 6 de la directive «vie privée et communications électroniques», l'article 7 de la directive sur la protection des données ne peut constituer un fondement juridique.

2.2.2. Caractère potentiellement identifiable des données anonymisées

Le groupe de travail «Article 29» a examiné en détail le concept de données à caractère personnel dans son avis 4/2007 sur les données à caractère personnel, en concentrant son attention sur les éléments constitutifs de la définition figurant à l'article 2, point a), de la directive 95/46/CE, et notamment la mention «identifiée ou identifiable» qui fait partie de cette définition. Dans ce contexte, le groupe de travail «Article 29» a aussi conclu que les «"données anonymisées" sont donc des données anonymes qui concernaient auparavant une personne identifiable, mais ne permettent plus cette identification».

De ce fait, le groupe de travail «Article 29» a déjà fait ressortir que le critère des «moyens susceptibles d'être raisonnablement mis en œuvre» évoqué par la directive doit être appliqué pour apprécier si le procédé d'anonymisation est suffisamment fiable, c'est-à-dire si l'identification est devenue «raisonnablement» impossible. Le contexte et les circonstances propres à chaque cas spécifique ont un impact direct sur le caractère identifiable. Dans l'annexe technique jointe au présent avis, les conséquences du choix de la technique la plus appropriée sont analysées.

Ainsi qu'il a déjà été signalé, les recherches, les outils et la puissance de calcul évoluent. Il n'est par conséquent ni réaliste ni utile de dresser une liste exhaustive des circonstances dans lesquelles l'identification n'est plus possible. Cependant, certains facteurs-clés méritent d'être pris en considération et illustrés.

Premièrement, il peut être avancé que les responsables du traitement des données devraient concentrer leur attention sur les moyens concrets qui seraient nécessaires pour inverser la technique d'anonymisation, notamment en termes de coût et de savoir-faire requis pour mettre en œuvre ces moyens, et sur l'appréciation de leur probabilité et de leur gravité. Par exemple, les responsables du traitement des données devraient mettre en balance leurs efforts d'anonymisation et les coûts résultants (en termes de temps et de ressources) avec la disponibilité croissante, à peu de frais, des moyens techniques permettant d'identifier des individus dans des ensembles de données, l'accessibilité publique croissante d'autres ensembles de données (comme ceux mis à disposition dans le cadre de politique de «données ouvertes»), et les nombreux exemples d'anonymisation incomplète entraînant par la suite des

effets négatifs, parfois irréparables, pour les personnes concernées[6]. Il est à noter que le risque d'identification peut augmenter avec le temps et dépend aussi des progrès des technologies de l'information et des communications. Les règles juridiques doivent donc, le cas échéant, être formulées d'une manière technologiquement neutre et tenir compte, dans l'idéal, des capacités d'évolution des technologies de l'information[7].

Deuxièmement, «les moyens» qu'il convient de considérer «pour déterminer si une personne est identifiable» sont ceux «susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne». Il est donc crucial de comprendre que, dans le cas où un responsable du traitement des données n'efface pas les données originales (identifiables) au niveau des événements individuels et transmet une partie de cet ensemble de données (par exemple après avoir supprimé ou masqué les données identifiables), l'ensemble de données résultant constitue encore des données à caractère personnel. Ce n'est que si les données sont agrégées par le responsable de leur traitement à un niveau où les événements individuels ne sont plus identifiables que l'ensemble de données résultant peut être qualifié d'anonyme. Par exemple: si une organisation collecte des données sur des déplacements individuels, les habitudes de voyage au niveau des événements individuels pourraient encore être considérées comme des données à caractère personnel pour toute partie intéressée, tant que le responsable du traitement des données (ou un tiers) continue à avoir accès aux données brutes originales, même si les identifiants directs ont été supprimés de l'ensemble de données transmis à des tiers. Mais si le responsable du traitement des données efface les données brutes et ne transmet à des tiers que des statistiques agrégées à un niveau supérieur, par exemple «le lundi, sur le trajet X, le nombre de passagers est supérieur de 160 % à celui du mardi», ces données pourraient être qualifiées d'anonymes.

Une solution d'anonymisation efficace doit empêcher toutes les parties d'isoler un individu dans un ensemble de données, de relier entre eux deux enregistrements dans un ensemble de données (ou dans deux ensembles de données séparés) et de déduire des informations de cet ensemble de données. D'une manière générale, il ne suffit donc pas de supprimer directement des éléments qui sont, en eux-mêmes, identifiants pour garantir que toute identification de la personne n'est plus possible. Il sera souvent nécessaire de prendre des mesures supplémentaires pour empêcher l'identification, toujours en fonction du contexte et des finalités du traitement auquel sont destinées les données anonymisées.

EXEMPLE:
Les profils génétiques constituent un exemple de données à caractère personnel qui, en raison du caractère unique de certains profils, peuvent présenter un risque d'identification si la seule technique utilisée est la suppression de l'identité du donneur. Il a déjà été démontré dans la littérature[8] que la combinaison de ressources génétiques publiquement disponibles (par exemple, des registres généalogiques, des notices nécrologiques, les résultats obtenus en interrogeant des moteurs de recherche) et des métadonnées concernant les données d'ADN (date du prélèvement, âge, lieu de résidence) peut révéler l'identité de certains individus même si cet ADN a été donné «anonymement».

[6] Il est intéressant de relever que les amendements du Parlement européen au projet de règlement général sur la protection des données récemment proposé (21 octobre 2013) mentionnent spécifiquement au considérant 23: «Pour établir si des moyens sont raisonnablement susceptibles d'être mis en œuvre afin d'identifier une personne physique, il convient de considérer l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte à la fois des technologies disponibles au moment du traitement et de l'évolution de celles-ci.».

[7] Voir l'avis 4/2007 du groupe de travail «Article 29», p. 16.

[8] Voir John Bohannon, «Genealogy Databases Enable Naming of Anonymous DNA Donors», *Science*, vol. 339, n° 6117 (18 janvier 2013), p. 262.

Les deux grandes familles de techniques d'anonymisation – la randomisation et la généralisation des données[9] – ont leurs lacunes; cependant, chacune d'elles peut être appropriée, selon les circonstances et le contexte, pour atteindre la finalité souhaitée sans compromettre le droit des personnes concernées au respect de leur vie privée. Il faut insister sur le fait que l'«identification» ne désigne pas simplement la possibilité de retrouver le nom et/ou l'adresse d'une personne, mais inclut aussi la possibilité de l'identifier par un procédé d'individualisation, de corrélation ou d'inférence. De surcroît, pour que la législation sur la protection des données s'applique, peu importe que les intentions soient celles du responsable du traitement des données ou de celui à qui elles sont destinées. Du moment que les données sont identifiables, les règles en matière de protection des données s'appliquent.

Quand des tiers traitent un ensemble de données auquel une technique d'anonymisation a été appliquée (données anonymisées et communiquées par le responsable de leur traitement à l'origine), ils ne sont pas tenus d'observer les exigences de protection des données pour autant qu'ils ne puissent pas identifier (directement ou indirectement) les personnes concernées dans l'ensemble de données original. Cependant, les tiers doivent prendre en compte les facteurs contextuels et circonstanciels mentionnés précédemment (y compris les spécificités des techniques d'anonymisation appliquées par le responsable du traitement des données à l'origine) pour décider comment ils comptent exploiter et, en particulier, combiner ces données anonymisées pour leur propre usage – car les conséquences résultantes peuvent entraîner différents types de responsabilité de leur part. Dans le cas où ces facteurs et ces caractéristiques sont de nature à comporter un risque inacceptable d'identification des personnes concernées, le traitement entre de nouveau dans le champ d'application de la législation en matière de protection des données.

La liste présentée plus haut ne se veut en aucune façon exhaustive, mais vise plutôt à donner une orientation générale pour l'appréciation du caractère potentiellement identifiable d'un ensemble de données selon les différentes techniques d'anonymisation disponibles qui lui sont appliquées. Tous les aspects mentionnés ci-dessus peuvent être considérés comme autant de facteurs de risque que doivent peser aussi bien les responsables du traitement qui anonymisent les ensembles de données que les tiers qui exploitent ces ensembles de données «anonymisés» pour leur propre usage.

2.2.3. Risques de l'utilisation de données anonymisées

Quand ils envisagent de recourir à des techniques d'anonymisation, les responsables du traitement des données doivent tenir compte des risques suivants.

- Un piège à éviter en particulier est de considérer les données pseudonymisées comme équivalentes à des données anonymisées. La section consacrée à l'analyse technique expliquera que les données pseudonymisées ne peuvent être assimilées à des informations anonymisées puisqu'elles continuent à permettre l'individualisation d'une personne concernée et la corrélation entre différents ensembles de données. Le pseudonymat n'est pas de nature à empêcher qu'une personne concernée soit identifiable et reste donc dans le champ d'application du régime juridique de la protection des données. Cela vaut en particulier dans le contexte des recherches scientifiques, statistiques ou historiques[10].

[9] Les principales caractéristiques de ces deux techniques d'anonymisation et leurs différences sont décrites à la section 3 ci-après («Analyse technique»).
[10] Voir aussi l'avis 4/2007 du groupe de travail «Article 29», p. 19 à 21.

EXEMPLE:
L'«affaire AOL (America On Line)» illustre de manière typique les idées fausses qui entourent la pseudonymisation. En 2006, une base de données contenant vingt millions de mots-clés figurant dans les recherches effectuées par plus de 650 000 utilisateurs au cours d'une période de 3 mois a été diffusée publiquement, sans autre mesure destinée à préserver la vie privée que le remplacement de l'identifiant d'utilisateur AOL par un attribut numérique. À la suite de quoi, l'identité et la localisation de certains utilisateurs ont été rendues publiques. Les requêtes transmises à un moteur de recherches, surtout si elles peuvent être couplées avec d'autres attributs, comme les adresses IP ou d'autres paramètres de configuration, ont un potentiel d'identification très élevé.

- Une deuxième erreur serait de considérer que les individus n'ont plus aucune garantie dès lors que les données ont été correctement anonymisées (ayant satisfait à l'ensemble des conditions et critères mentionnés ci-dessus et sortant, par définition, du champ d'application de la directive sur la protection des données) – d'abord et avant tout parce que d'autres actes législatifs peuvent s'appliquer à l'utilisation de ces données. Par exemple, l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» interdit le stockage d'«informations» de quelque type que ce soit (y compris les informations non personnelles) et l'accès à ces informations sur l'équipement terminal d'un abonné ou d'un utilisateur sans son accord, dans le cadre du principe plus large de la confidentialité des communications.

- Une troisième négligence résulterait aussi de ne pas envisager l'impact que des données correctement anonymisées peuvent avoir sur les individus dans certaines circonstances, en particulier dans le cas du profilage. La vie privée des personnes est protégée par l'article 8 de la CEDH et par l'article 7 de la Charte des droits fondamentaux de l'Union européenne; de ce fait, même si la législation sur la protection des données ne s'applique plus à ce type de données, l'usage qui est fait des ensembles de données anonymisées et mises à la disposition de tiers peut entraîner une atteinte à la vie privé. Une prudence particulière s'impose dans la manipulation d'informations anonymisées, surtout lorsque ces informations servent (souvent en combinaison avec d'autres données) à prendre des décisions qui produisent des effets (même indirectement) sur les individus. Ainsi qu'il a déjà été signalé dans le présent avis et comme l'a clairement précisé le groupe de travail «Article 29» notamment dans son avis sur la notion de «limitation des finalités» (avis 03/2013)[11], les attentes légitimes des personnes concernées quant au traitement ultérieur de leurs données doivent être appréciées à la lumière des facteurs contextuels pertinents – comme la nature de la relation entre les personnes concernées et les responsables du traitement des données, les obligations juridiques applicables, la transparence des opérations de traitement.

3 Analyse technique, fiabilité des technologies et erreurs typiques

Il existe différentes pratiques et techniques d'anonymisation, avec des degrés de fiabilité variables. Cette section portera sur les principaux points que les responsables du traitement des données doivent prendre en considération quand ils choisissent d'appliquer une technique donnée, au regard notamment des garanties offertes par cette technique, en tenant compte de l'état actuel de la technologie et en envisageant trois risques essentiels en matière d'anonymisation:

[11] Disponible à l'adresse http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

- *l'individualisation*, qui correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données;
- *la corrélation,* qui consiste dans la capacité de relier entre elles, au moins, deux enregistrements se rapportant à la même personne concernée ou à un groupe de personnes concernées (soit dans la même base de données, soit dans deux bases de données différentes). Si une attaque permet d'établir (par exemple, au moyen d'une analyse de corrélation) que deux enregistrements correspondent à un même groupe d'individus, mais ne permet pas d'isoler des individus au sein de ce groupe, la technique résiste à l'«individualisation», mais non à la corrélation;
- *l'inférence*, qui est la possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs.

Une solution résistant à ces trois risques offrirait par conséquent une protection fiable contre les tentatives de ré-identification utilisant les moyens les plus susceptibles d'être raisonnablement mis en œuvre par le responsable du traitement des données ou par des tiers. Le groupe de travail «Article 29» souligne, à cet égard, que les recherches en matière de techniques d'anonymisation se poursuivent et font apparaître invariablement qu'aucune technique n'est, en soi, infaillible. En termes généraux, on distingue deux grandes approches de l'anonymisation: la première repose sur la ***randomisation*** tandis que la seconde se fonde sur la ***généralisation***. D'autres notions sont aussi abordées dans le présent avis, comme la *pseudonymisation*, la *confidentialité différentielle*, la *l-diversité* et la *t-proximité*.

Le vocabulaire suivant est employé dans cette section: un ensemble de données se compose des différents enregistrements relatifs à des individus (les personnes concernées). Chaque enregistrement se rapporte à une personne concernée et comporte une série de valeurs (ou «entrées», par exemple: 2013) pour chaque attribut (par exemple, l'année). Un ensemble de données est donc un groupe d'enregistrements qui peuvent être présentés tantôt sous la forme d'un tableau (ou de plusieurs tableaux), tantôt sous la forme d'un graphique annoté/pondéré, ce qui est de plus en plus souvent le cas aujourd'hui. Les exemples donnés dans le présent avis porteront sur des tableaux, mais ils s'appliquent aussi à d'autres représentations graphiques des enregistrements. Les combinaisons d'attributs qui se rapportent à une personne concernée ou à un groupe de personnes concernées peuvent être désignées par le terme de «quasi-identifiants». Dans certains cas, un ensemble de données peut comporter des enregistrements multiples pour un même individu. Un «attaquant» est un tiers (c'est-à-dire ni le responsable du traitement des données ni un sous-traitant) qui accède aux enregistrements originaux par accident ou de manière intentionnelle.

3.1. Randomisation

La randomisation est une famille de techniques qui altèrent la véracité des données afin d'affaiblir le lien entre les données et l'individu. Si les données sont suffisamment incertaines, elles ne peuvent plus être rattachées à un individu en particulier. En elle-même, la randomisation ne réduira pas la singularité de chaque enregistrement, qui sera toujours dérivé d'une seule personne concernée, mais elle peut apporter une protection contre les attaques/risques relevant de l'inférence et peut être combinée avec des techniques de généralisation pour offrir de meilleures garanties de respect de la vie privée. Des techniques supplémentaires peuvent se révéler nécessaires pour empêcher qu'un enregistrement permette d'identifier un individu.

3.1.1. Ajout de bruit

La technique d'ajout de bruit est particulièrement utile quand des attributs peuvent avoir un effet négatif important sur des individus et consiste à modifier des attributs dans l'ensemble de données pour les rendre moins précis, tout en conservant la distribution générale. Pour traiter un ensemble de données, un observateur supposera que les valeurs sont exactes, mais ce ne sera vrai qu'à un certain degré. Par exemple, si la taille d'un individu a été mesurée à l'origine au centimètre près, l'ensemble de données anonymisées peut présenter une précision de ± 10 cm seulement. Si cette technique est appliquée efficacement, un tiers ne sera pas en mesure d'identifier un individu ni ne pourra restaurer les données ou discerner de quelque autre façon comment les données ont été modifiées.

L'ajout de bruit devra ordinairement être combiné avec d'autres techniques d'anonymisation comme la suppression des attributs évidents et des quasi-identifiants. Le niveau de bruit devrait dépendre du niveau d'information requis et de l'impact que la divulgation des attributs protégés aurait sur le respect de la vie privée des individus.

3.1.1.1. Garanties

- *Individualisation:* Il reste possible d'isoler les enregistrements correspondant à un individu (peut-être de manière non identifiable), même si les enregistrements sont moins fiables.
- *Corrélation:* Il reste possible relier entre eux les enregistrements correspondant au même individu, mais ces enregistrements sont moins fiables et il peut donc arriver qu'un enregistrement réel soit relié à un enregistrement ajouté artificiellement (c'est-à-dire à un «bruit»). Dans certains cas, une attribution erronée pourrait exposer une personne concernée à un niveau de risque considérable, voire plus élevé que celui résultant d'une attribution correcte.
- *Inférence:* Une attaque par inférence est peut-être possible, mais le taux de succès sera moins élevé et certains faux positifs (et faux négatifs) sont plausibles.

3.1.1.2. Erreurs courantes

- Ajout de bruit incohérent: Si le bruit n'est pas sémantiquement viable (c'est-à-dire s'il est disproportionné et ne respecte pas la logique entre les attributs d'un ensemble), un attaquant ayant accès à la base de données sera en mesure de le filtrer et, dans certains cas, de recréer les entrées manquantes. De plus, si l'ensemble de données est trop clairsemé[12], il peut arriver qu'il reste possible de relier les entrées de données bruitées avec une source extérieure.
- Supposer que l'ajout de bruit est suffisant: l'ajout de bruit est une mesure complémentaire qui rend plus difficile la récupération des données à caractère personnel par un attaquant. À moins que le bruit ne soit plus élevé que le niveau d'information contenu dans l'ensemble de données, il ne faut pas supposer que l'ajout de bruit représente une solution d'anonymisation qui se suffit à elle-même.

3.1.1.3. Échecs de l'ajout de bruit

Une expérience de ré-identification très connue est celle réalisée sur la base de données des clients du fournisseur de contenu vidéo Netflix. Des chercheurs ont analysé les

[12] Cette notion est examinée plus en détail dans l'annexe, en p. 33.

propriétés géométriques de cette base de données composée de plus de 100 millions d'évaluations, sur une échelle de 1 à 5, attribuées à plus de 18 000 films par près de 500 000 utilisateurs, qui avait été rendue publique par la société, après avoir été «anonymisée» conformément à la politique interne de l'entreprise en matière de confidentialité, en supprimant toutes les informations d'identification des utilisateurs hormis les évaluations et les dates. Un bruit avait été ajouté dans la mesure où les évaluations avaient été légèrement augmentées ou diminuées.

Malgré ces précautions, il est apparu que 99 % des enregistrements des utilisateurs pouvaient être identifiés de manière unique dans l'ensemble de données en prenant comme critères de sélection 8 évaluations et des dates comportant une marge d'erreur de 14 jours, tandis qu'un abaissement des critères de sélection (2 évaluations, avec une marge d'erreur de 3 jours dans les dates) permettait encore d'identifier 68 % des utilisateurs[13].

3.1.2. Permutation

Cette technique, qui consiste à mélanger les valeurs des attributs dans un tableau de telle sorte que certaines d'entre elles sont artificiellement liées à des personnes concernées différentes, est utile quand il est important de conserver la distribution exacte de chaque attribut dans l'ensemble de données.

La permutation peut être considérée comme une forme spéciale d'ajout de bruit. Dans une technique de bruit classique, les attributs sont modifiés au moyen de valeurs aléatoires. La production d'un bruit cohérent peut se révéler une tâche difficile et le simple fait de modifier légèrement les valeurs des attributs risque de ne pas garantir la confidentialité adéquate. Au lieu de quoi, les techniques de permutation altèrent les valeurs au sein de l'ensemble de données en les échangeant simplement d'un enregistrement à un autre. Cet échange garantira que la fourchette et la distribution des valeurs resteront les mêmes, mais non les corrélations entre les valeurs et les individus. Si deux ou plusieurs attributs sont liés par une relation logique ou une corrélation statistique et sont permutés indépendamment l'un de l'autre, ce lien sera détruit. Il peut donc être important de permuter un ensemble d'attributs de façon à ne pas briser la relation logique, faute de quoi un attaquant pourrait identifier les attributs permutés et inverser la permutation.

Par exemple, si l'on examine un sous-ensemble d'attributs dans un ensemble de données médicales, comme les «motifs d'hospitalisation/symptômes/service concerné», les valeurs seront dans la plupart des cas liées par une forte relation logique et la permutation d'une seule des valeurs serait par conséquent détectée et pourrait même être inversée.

À l'instar de l'ajout de bruit, la permutation risque de ne pas garantir en soi l'anonymisation et devrait toujours être combinée à la suppression des attributs évidents/quasi-identifiants.

3.1.2.1. Garanties

- *Individualisation:* Comme dans le cas de l'ajout de bruit, il reste possible d'isoler les enregistrements correspondant à un individu, mais ces enregistrements sont moins fiables.

[13] Narayanan, A., et Shmatikov, V. (mai 2008), «Robust de-anonymization of large sparse datasets», in *Security and Privacy, 2008, SP 2008, IEEE Symposium on* (p. 111 à 125), IEEE.

- *Corrélation:* Si la permutation affecte des attributs et des quasi-identifiants, elle peut empêcher de relier «correctement» des attributs entre eux tant à l'intérieur qu'à l'extérieur d'un ensemble de données, mais elle autorise toujours une corrélation «incorrecte», puisqu'une entrée réelle peut se trouver associée à une personne concernée différente.
- *Inférence:* Des déductions peuvent encore être tirées de l'ensemble de données, en particulier si les attributs sont corrélés entre eux ou ont des relations logiques fortes; toutefois, sans savoir quels attributs ont été permutés, l'attaquant doit envisager la possibilité que son inférence se fonde sur une hypothèse et seule une inférence probabiliste demeure possible.

3.1.2.2. Erreurs courantes

- Sélection du mauvais attribut: La permutation des attributs non sensibles ou ne comportant pas de risques n'apporterait pas de gain significatif en termes de protection des données à caractère personnel. En effet, si les attributs sensibles/à risque restent associés à la valeur originale, un attaquant aura toujours la possibilité d'extraire des informations sensibles à propos des individus.
- Permutation aléatoire des attributs: Si deux attributs sont fortement corrélés, le fait de permuter les attributs au hasard n'offrira pas de garanties solides. Cette erreur courante est illustrée dans le tableau 1.
- Supposer que la permutation est suffisante: À l'instar de l'ajout de bruit, la permutation ne garantit pas en elle-même l'anonymat et devrait être combinée avec d'autres techniques comme la suppression des attributs évidents.

3.1.2.3. Échecs de la permutation

L'exemple qui suit montre que la permutation aléatoire des attributs offre de piètres garanties de confidentialité quand il existe des liens logiques entre différents attributs. Après la tentative d'anonymisation, il est facile de déduire le revenu de chaque individu selon sa situation professionnelle (et l'année de sa naissance). Par exemple, un examen direct des données permet de soutenir que le PDG est très probablement né en 1957 et perçoit la rémunération la plus élevée, tandis que le chômeur est né en 1964 et a le revenu le moins élevé.

Année	Sexe	Situation professionnelle	Revenu (permuté)
1957	M	Ingénieur	70 000
1957	M	PDG	5 000
1957	M	Sans emploi	43 000
1964	M	Ingénieur	100 000
1964	M	Directeur	45 000

Tableau 1. Un exemple d'anonymisation inefficace par permutation d'attributs corrélés

3.1.3. Confidentialité différentielle

La confidentialité différentielle[14] fait partie de la famille des techniques de randomisation, avec une approche différente: si, dans les faits, l'insertion de bruit intervient à l'avance, quand

[14] Dwork, C. (2006), «Differential privacy», in *Automata, languages and programming* (p. 1 à 12), Springer Berlin Heidelberg.

l'ensemble de données est censé être publié, la confidentialité différentielle peut être utilisée quand le responsable du traitement des données produit des aperçus anonymisés d'un ensemble de données tout en conservant une copie des données originales. Ces aperçus anonymisés sont ordinairement produits au moyen d'un sous-ensemble de requêtes à l'intention d'un tiers en particulier. Le sous-ensemble comprend un bruit aléatoire délibérément ajouté a posteriori. La confidentialité différentielle indique au responsable du traitement des données quel niveau de bruit il doit ajouter, et sous quelle forme, pour obtenir les garanties nécessaires[15]. Dans ce contexte, il sera particulièrement important d'assurer un contrôle permanent (au moins pour chaque nouvelle requête), afin de repérer toute possibilité d'identifier un individu dans l'ensemble des résultats de la requête. Il faut cependant préciser que les techniques de confidentialité différentielle ne modifient pas les données originales et que, par conséquent, tant que les données originales sont conservées, le responsable du traitement des données reste en mesure d'identifier des individus dans les résultats des requêtes de confidentialité différentielle, compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre. Ces résultats doivent donc aussi être considérés comme des données à caractère personnel.

L'un des avantages d'une approche reposant sur la confidentialité différentielle tient au fait que des ensembles de données sont communiqués à des tiers autorisés en réponse à une demande spécifique, plutôt que d'être publiés sous la forme d'un unique ensemble de données. Pour faciliter le contrôle, le responsable du traitement des données peut conserver une liste de toutes les demandes et requêtes afin de vérifier que les tiers n'ont pas accès à des données pour lesquelles ils ne disposent pas d'autorisation. Une requête peut aussi être soumise à des techniques d'anonymisation, incluant l'ajout de bruit ou la substitution, pour mieux garantir la confidentialité. Les recherches se poursuivent en vue de trouver un bon mécanisme interactif de question-réponse, qui soit capable tout à la fois de répondre assez précisément à n'importe quelle question (c'est-à-dire en ajoutant le moins de bruit possible) et de préserver la confidentialité.

Pour limiter les attaques par inférence et par corrélation, il est nécessaire de garder une trace des requêtes soumises par une entité et de surveiller les informations obtenues à propos des personnes concernées; par conséquent, les bases de données à «confidentialité différentielle» ne devraient pas être déployées sur des moteurs de recherche ouverts qui n'offrent aucune traçabilité des entités requérantes.

3.1.3.1 Garanties

- *Individualisation:* Si les résultats se limitent à la production de statistiques et si les règles appliquées à l'ensemble de données sont bien choisies, il ne devrait pas être possible d'utiliser les réponses pour isoler un individu.
- *Corrélation:* En recourant à des requêtes multiples, il pourrait être possible de relier entre elles les entrées relatives à un individu spécifique d'une réponse à l'autre.
- *Inférence:* Il est possible de déduire des informations concernant des individus ou des groupes au moyen de requêtes multiples.

[15] Cf. Ed Felten (2012), «Protecting privacy by adding noise». Internet: https://techatftc.wordpress.com/2012/06/21/protecting-privacy-by-adding-noise/.

3.1.3.2. Erreurs courantes

- Ne pas injecter suffisamment de bruit: Afin d'empêcher que des liens puissent être établis avec des connaissances tirées du contexte, la difficulté consiste à fournir le moins d'éléments possibles indiquant si une personne concernée ou un groupe de personnes concernées en particulier a contribué ou non à l'ensemble de données. Le plus difficile, du point de vue de la protection des données, est de parvenir à générer le niveau de bruit approprié à ajouter aux réponses réelles, de façon à protéger la vie privée des individus sans nuire à l'utilité des réponses fournies.

3.1.3.3 Échecs de la confidentialité différentielle

Traitement indépendant de chaque requête: Une combinaison de résultats de requêtes risque de permettre la divulgation d'informations censées rester confidentielles. Si un historique des requêtes n'est pas conservé, un attaquant peut concevoir des questions multiples destinées à interroger une base de données à «confidentialité différentielle» qui réduisent progressivement l'amplitude de l'échantillon résultant jusqu'à ce qu'un caractère spécifique à une seule personne concernée ou à un groupe de personnes concernées finisse par émerger, de façon certaine ou avec un taux de probabilité très élevé. Il faut, en outre, veiller à ne pas commettre l'erreur de penser que les données sont anonymes pour les tiers, alors que le responsable du traitement des données reste en mesure d'identifier la personne concernée dans la base de données originale, compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre.

3.2. Généralisation

La généralisation constitue la seconde famille de techniques d'anonymisation. Cette approche consiste à généraliser, ou diluer, les attributs des personnes concernées en modifiant leur échelle ou leur ordre de grandeur respectif (par exemple, une région plutôt qu'une ville, un mois plutôt qu'une semaine). Si la généralisation peut être efficace pour empêcher l'individualisation, elle ne garantit pas une anonymisation effective dans tous les cas; en particulier, elle requiert des approches quantitatives spécifiques et sophistiquées afin de prévenir la corrélation et l'inférence.

3.2.1. Agrégation et k-anonymat

Les techniques de l'agrégation et du k-anonymat visent à empêcher qu'une personne concernée puisse être isolée en la regroupant avec, au moins, *k* autres individus. Pour ce faire, les valeurs des attributs sont généralisées dans une mesure telle que tous les individus partagent la même valeur. Par exemple, en abaissant la granularité géographique d'une ville à un pays, on inclut un nombre plus élevé de personnes concernées. Les dates de naissance individuelles peuvent être généralisées en une fourchette de dates, ou regroupées par mois ou par année. D'autres attributs numériques (par exemple, les salaires, le poids, la taille ou la dose d'un médicament administrée) peuvent être généralisés au moyen de valeurs d'intervalle (par exemple, salaire de 20 000 à 30 000 EUR). Ces méthodes peuvent être utilisées quand la corrélation de valeurs d'attributs ponctuelles risque de créer des quasi-identifiants.

3.2.1.1. Garanties

- *Individualisation:* Dès lors que les mêmes attributs sont désormais partagés par *k* utilisateurs, il ne devrait plus être possible d'isoler un individu au sein d'un groupe de *k* utilisateurs.

- *Corrélation:* Si la corrélation est limitée, il reste possible de relier les enregistrements par groupe de *k* utilisateurs. Ensuite, au sein de ce groupe, la probabilité que deux enregistrements correspondent aux mêmes pseudo-identifiants est de 1/*k* (ce qui pourrait être nettement plus que la probabilité que ces entrées ne puissent pas être reliées entre elles).
- *Inférence:* Le principal défaut du modèle du k-anonymat est qu'il n'empêche pas un quelconque type d'attaque par inférence. En effet, si tous les *k* individus font partie du même groupe, pour peu que l'on sache à quel groupe appartient un individu, il est facile d'obtenir la valeur de cette propriété.

3.2.1.2. Erreurs courantes

- Négliger certains quasi-identifiants: Le seuil de *k* constitue un paramètre critique dans la technique du k-anonymat. Plus la valeur de *k* est élevée, plus les garanties de confidentialité sont fortes. Une erreur courante consiste à augmenter artificiellement la valeur de *k* en réduisant l'ensemble des quasi-identifiants pris en considération. Un nombre réduit de quasi-identifiants facilite la constitution de groupes de *k* utilisateurs du fait de la capacité d'identification inhérente associée aux autres attributs (surtout si certains d'entre eux sont sensibles ou ont une entropie très élevée, comme dans le cas d'attributs très rares). Le fait de ne pas prendre en considération tous les quasi-identifiants lors de la sélection de l'attribut à généraliser est une erreur critique; si certains attributs peuvent servir à isoler un individu dans un groupe de *k*, la généralisation ne permet pas de protéger certains individus (voir l'exemple du tableau 2).
- Faible valeur de *k*: La recherche d'une faible valeur de *k* se révèle, elle aussi, problématique. Si *k* est trop petit, le coefficient de pondération d'un individu au sein d'un groupe est trop important et les attaques par inférence ont de meilleures chances de succès. Par exemple, si $k=2$ la probabilité que les deux individus partagent la même propriété est plus grande que dans le cas où $k>10$.
- Ne pas regrouper des individus dont le coefficient de pondération est similaire: Le fait de constituer un ensemble d'individus présentant une distribution inégale d'attributs peut aussi créer des problèmes. L'impact des enregistrements correspondant à un individu sur un ensemble de données variera: certains représenteront une fraction considérable des entrées tandis les contributions d'autres resteront assez insignifiantes. Il est donc important de veiller à ce que *k* soit suffisamment élevé pour qu'aucun individu ne représente une fraction trop grande des entrées dans un groupe.

3.1.3.3. Échecs du k-anonymat

Le principal problème lié au k-anonymat est qu'il n'empêche pas les attaques par inférence. Dans l'exemple qui suit, si l'attaquant sait qu'un individu figure dans l'ensemble de données et est né en 1964, il sait aussi que cet individu a fait une crise cardiaque. De plus, si l'on sait que cet ensemble de données a été obtenu auprès d'une organisation française, on peut en déduire que chacun des individus réside à Paris puisque les trois premiers chiffres des codes postaux sont 750*).

Année	Sexe	Code postal	Diagnostic
1957	M	750*	Crise cardiaque
1957	M	750*	Cholestérol
1957	M	750*	Cholestérol
1964	M	750*	Crise cardiaque
1964	M	750*	Crise cardiaque

Tableau 2. Un exemple de k-anonymisation mal conçue

3.2.2. l-diversité/t-proximité

La l-diversité étend le k-anonymat pour faire en sorte qu'il ne soit plus possible d'obtenir des résultats certains au moyen d'attaques par inférence en veillant à ce que, dans chaque classe d'équivalence, chaque attribut ait au moins *l* valeurs différentes.

Un objectif fondamental à atteindre est d'éviter autant que possible les classes d'équivalence caractérisées par une faible variabilité des attributs, de telle sorte qu'un attaquant reste toujours confronté à un degré d'incertitude considérable, malgré les connaissances tirées du contexte dont il pourrait disposer à propos d'une personne concernée.

La l-diversité est utile pour protéger les données contre les attaques par inférence, quand les valeurs des attributs sont bien distribuées. Il faut cependant souligner que cette technique n'empêche pas les fuites d'informations si les attributs au sein d'un segment sont distribués de manière inégale ou ne présentent qu'un faible écart de valeurs ou de contenus sémantiques. En définitive, la l-diversité se prête à des attaques par inférence probabilistes.

La t-proximité constitue un affinement de la l-diversité, en ce sens qu'elle vise à créer des classes d'équivalence qui ressemblent à la distribution initiale des attributs dans le tableau. Cette technique est utile quand il est important de conserver des données aussi proches que possible des données originales; à cet effet, une contrainte supplémentaire est ajoutée à la classe d'équivalence, à savoir que non seulement chaque classe d'équivalence doit comporter au moins *l* valeurs différentes, mais aussi que chaque valeur est représentée autant de fois que nécessaire pour refléter la distribution initiale de chaque attribut.

3.2.2.1. Garanties

- *Individualisation:* À l'instar du k-anonymat, la l-diversité et la t-proximité permettent d'empêcher que les enregistrements relatifs à un individu soient isolés dans la base de données.
- *Corrélation:* La l-diversité et la t-proximité n'apportent pas d'amélioration par rapport au k-anonymat pour ce qui est d'empêcher la corrélation. Le problème reste le même pour n'importe quel regroupement: la probabilité que les mêmes entrées se rapportent à la même personne concernée est plus élevée que $1/N$ (où N est le nombre de personnes concernées dans la base de données).
- *Inférence:* la principale amélioration de la l-diversité et de la t-proximité par rapport au k-anonymat est qu'il n'est plus possible de lancer des attaques par inférence contre une base de données à «l-diversité» ou «t-proximité» avec un degré de certitude de 100 %.

3.2.2.2. Erreurs courantes

- Protéger les valeurs des attributs sensibles en les mélangeant avec d'autres attributs sensibles: Le fait d'avoir deux valeurs pour un attribut dans un groupe ne suffit pas à apporter des garanties de confidentialité. En fait, la distribution des valeurs sensibles dans chaque groupe devrait être semblable à la distribution de ces valeurs dans la population totale ou, du moins, elle devrait être uniforme dans l'ensemble du groupe.

3.2.2.3. Échecs de la l-diversité

Dans le tableau présenté ci-dessous, la l-diversité est assurée pour l'attribut «Diagnostic»; cependant, pour peu que l'on connaisse un individu né en 1964 qui figure dans ce tableau, il reste possible de supposer avec une probabilité très élevée qu'il a fait une crise cardiaque.

Année	Sexe	Code postal	Diagnostic
1957	M	750*	**Crise cardiaque**
1957	M	750*	**Cholestérol**
1957	M	750*	**Cholestérol**
1957	M	750*	**Cholestérol**
1964	M	750*	**Crise cardiaque**
1964	M	750*	**Crise cardiaque**
1964	M	750*	**Crise cardiaque**
1964	M	750*	**Cholestérol**
1964	M	750*	**Crise cardiaque**
1964	M	750*	**Crise cardiaque**
1964	M	750*	**Crise cardiaque**
1964	M	750*	**Crise cardiaque**
1964	M	750*	**Crise cardiaque**
1964	M	750*	**Crise cardiaque**

Tableau 3. Un exemple de l-diversité où les valeurs de «Diagnostic» ne sont pas uniformément distribuées

Nom	Date de naissance	Sexe
Smith	1964	M
Rossi	1964	M
Dupont	1964	M
Jansen	1964	M
Garcia	1964	M

Tableau 4. En sachant que ces individus figurent dans le tableau 3, un attaquant pourrait en déduire qu'ils ont fait une crise cardiaque

4. Pseudonymisation

La pseudonymisation consiste à remplacer un attribut (généralement un attribut unique) par un autre dans un enregistrement. La personne physique est donc toujours susceptible d'être identifiée indirectement; par conséquent, la pseudonymisation ne permet pas, à elle seule, de produire un ensemble de données anonymes. Elle est néanmoins examinée dans le présent avis en raison de nombreuses idées fausses et erreurs qui entourent son utilisation.

La pseudonymisation réduit le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée; à ce titre, c'est une mesure de sécurité utile, mais non une méthode d'anonymisation.

Le résultat de la pseudonymisation peut être indépendant de la valeur initiale (comme dans le cas d'un numéro aléatoire généré par le responsable du traitement ou d'un nom choisi par la personne concernée) ou il peut être dérivé des valeurs originales d'un attribut ou d'un ensemble d'attributs, par exemple au moyen d'une fonction de hachage ou d'un système de chiffrement.

Les techniques de pseudonymisation les plus utilisées sont les suivantes:

- Système cryptographique à clé secrète: dans ce cas, le détenteur de la clé peut aisément ré-identifier chaque personne concernée en décryptant l'ensemble de données, puisque les données à caractère personnel y figurent toujours, quoique sous une forme cryptée. En supposant qu'un système cryptographique conforme à l'état de la technique a été appliqué, le décryptage ne serait possible qu'à condition de connaître la clé.
- Fonction de hachage: il s'agit d'une fonction qui renvoie un résultat de taille fixe, quelle que soit la taille de l'entrée encodée (l'entrée peut être un attribut unique ou un ensemble d'attributs) et qui ne peut être inversée; c'est-à-dire que le risque de récupération des données observé dans le cas du chiffrement n'existe plus. Cependant, si la fourchette dans laquelle se situent les valeurs d'entrée de la fonction de hachage est connue, il est possible de réintroduire ces valeurs dans la fonction de hachage afin d'obtenir la valeur correcte correspondant à un enregistrement en particulier. Par exemple, si un ensemble de données a été pseudonymisé en procédant au hachage du numéro d'identification national, il peut être reconstitué simplement en appliquant la fonction de hachage à toutes les valeurs possibles et en comparant les résultats avec les valeurs figurant dans l'ensemble de données. Les fonctions de hachage sont ordinairement conçues pour être calculées relativement vite et se prêtent donc à des

attaques par force brute[16]. Des tables pré-calculées peuvent aussi être créées pour permettre la reconstitution en masse d'un ensemble volumineux de valeurs de hachage.

L'utilisation d'une fonction de hachage avec salage (où une valeur aléatoire, appelée «sel», est ajoutée à l'attribut qui fait l'objet du hachage) permet de réduire la probabilité de reconstituer la valeur d'entrée. Il reste néanmoins possible, avec des moyens raisonnables, de calculer la valeur originale de l'attribut qui se cache derrière le résultat d'une fonction de hachage avec salage[17].

- Fonction de hachage par clé avec clé enregistrée: il s'agit d'une fonction de hachage particulière qui utilise une clé secrète comme entrée supplémentaire (à la différence d'une fonction de hachage avec salage, où le «sel» n'est généralement pas secret). Un responsable du traitement des données peut ré-exécuter la fonction sur l'attribut en se servant de la clé secrète, mais il est beaucoup plus difficile pour un attaquant de ré-exécuter la fonction sans connaître la clé car le nombre de possibilités à tester est suffisamment grand pour rendre la tâche impraticable.
- Chiffrement déterministe ou fonction de hachage par clé avec suppression de la clé: cette technique équivaut à sélectionner un nombre aléatoire comme pseudonyme pour chaque attribut de la base de données et à supprimer ensuite la table de correspondance. Cette solution permet[18] de réduire le risque de corrélation entre les données à caractère personnel figurant dans l'ensemble de données et celles qui se rapportent au même individu dans un autre ensemble de données, où un pseudonyme différent est utilisé. En supposant qu'un algorithme conforme à l'état de la technique soit appliqué, il sera difficile pour un attaquant, en termes de puissance de calcul requise, de décrypter ou de ré-exécuter la fonction, car cela supposerait d'essayer chaque clé possible, puisque la clé n'est pas disponible.
- Tokenization: cette technique est généralement appliquée dans le secteur financier (même si elle n'y est pas confinée) pour remplacer les numéros d'identification de cartes par des valeurs sans grande utilité pour un attaquant. Elle dérive des techniques précédentes, dans la mesure où elle repose normalement sur l'application de mécanismes de chiffrement à sens unique ou sur l'assignation, au moyen d'une fonction d'index, d'un numéro séquentiel ou d'un nombre produit de manière aléatoire qui n'est pas mathématiquement dérivé des données originales.

4.1. Garanties

- *Individualisation:* Il reste possible d'isoler les enregistrements d'un individu, puisque celui-ci est toujours identifié par un attribut unique qui est le résultat de la fonction de pseudonymisation (= l'attribut pseudonymisé).
- *Corrélation:* La corrélation restera facile entre les enregistrements qui utilisent le même attribut pseudonymisé en référence au même individu. Même si des attributs pseudonymisés différents sont utilisés pour la même personne concernée, la corrélation est encore possible au moyen d'autres attributs. Ce n'est que dans le cas où

[16] Ces attaques consistent à essayer toutes les entrées plausibles afin de constituer des tableaux de correspondance.
[17] Surtout si le type d'attribut est connu (nom, numéro de sécurité sociale, date de naissance, etc.). Pour augmenter la puissance de calcul requise, on pourrait recourir à une fonction de hachage à dérivation de clé, où la valeur calculée est hachée plusieurs fois avec une courte chaîne de «sel».
[18] Tout dépend des autres attributs figurant dans l'ensemble de données et de la suppression des données originales.

aucun autre attribut dans l'ensemble de données ne peut servir à identifier la personne concernée et où tout lien entre l'attribut original et l'attribut pseudonymisé a été éliminé (notamment par la suppression des données originales) qu'aucun recoupement évident ne pourra être fait entre deux ensembles de données qui utilisent des attributs pseudonymisés différents.

- *Inférence:* Les attaques par inférence sur l'identité réelle d'une personne concernée sont possibles au sein de l'ensemble de données ou entre différentes bases de données qui utilisent le même attribut pseudonymisé pour un individu, ou encore dans le cas où les pseudonymes sont transparents et ne masquent pas correctement l'identité originale de la personne concernée.

4.2. Erreurs courantes

- Croire qu'un ensemble de données pseudonymisé est anonymisé: Les responsables du traitement des données supposent souvent qu'il suffit de supprimer ou de remplacer un ou plusieurs attributs pour rendre l'ensemble de données anonyme. De nombreux exemples ont montré que ce n'est pas le cas; le simple fait de modifier l'identité n'empêche pas quelqu'un d'identifier une personne concernée s'il subsiste des quasi-identifiants dans l'ensemble de données, ou si les valeurs d'autres attributs permettent encore d'identifier un individu. Dans bien des cas, il peut se révéler aussi facile d'identifier un individu dans un ensemble de données pseudonymisé qu'à partir des données originales. Des mesures supplémentaires devraient être prises pour pouvoir considérer l'ensemble de données comme anonymisé, notamment la suppression et la généralisation d'attributs, l'effacement des données originales ou du moins leur conservation à un niveau hautement agrégé.
- Erreurs courantes lors de l'utilisation de la pseudonymisation comme technique destinée à réduire la corrélation:

  - Utiliser la même clé dans des bases de données différentes: l'élimination du risque de corrélation entre différents ensembles de données dépend beaucoup de l'utilisation d'un algorithme à clé et du fait qu'un même individu correspondra à différents attributs pseudonymisés dans des contextes différents. Il est donc important d'éviter d'utiliser la même clé dans des bases de données différentes pour pouvoir réduire la corrélation.
  - Utiliser des clés différentes («clés alternées») pour des utilisateurs différents: il pourrait être tentant d'employer des clés différentes pour différents ensembles d'utilisateurs et de changer la clé en fonction de son utilisation (par exemple, se servir de la même clé pour 10 entrées d'enregistrement relatives au même utilisateur). Cependant, si elle n'est pas correctement conçue, cette opération pourrait faire apparaître des motifs, réduisant partiellement les avantages escomptés. Par exemple, l'utilisation alternée d'une clé selon des règles spécifiques pour des individus spécifiques faciliterait la mise en corrélation des entrées correspondant à des individus donnés. De plus, la disparition de données pseudonymisées récurrentes dans la base de données au moment où de nouvelles données apparaissent peut indiquer que les enregistrements se rapportent à la même personne physique.
  - Conserver la clé: si la clé secrète est conservée avec les données pseudonymisées, et si les données sont compromises, l'attaquant peut être en mesure de relier facilement les données pseudonymisées avec leur attribut

original. Il en va de même si la clé est conservée séparément, mais de façon peu sûre.

4.3. Lacunes de la pseudonymisation

- *Soins de santé*

1. Nom, adresse, date de naissance	2. Période de perception d'une prestation d'assistance spéciale	3. Indice de masse corporelle	6. N° de référence dans la cohorte de recherche
[redacted]	< 2 ans	15	QA5FRD4
	> 5 ans	14	2B48HFG
	< 2 ans	16	RC3URPQ
	> 5 ans	18	SD289K9
	< 2 ans	20	5E1FL7Q

Tableau 5. Un exemple de pseudonymisation par hachage (nom, adresse, date de naissance) qui peut être aisément inversée

Un ensemble de données a été créé pour examiner la relation entre le poids d'une personne et la perception d'une prestation d'assistance spéciale. L'ensemble de données original comprenait le nom, l'adresse et la date de naissance des personnes concernées, qui ont été effacés. Le numéro de référence dans la cohorte de recherche a été généré à partir des données supprimées en utilisant une fonction de hachage. Bien que le nom, l'adresse et la date de naissance aient été supprimés du tableau, si l'on connaît le nom, l'adresse et la date de naissance d'une personne concernée, en plus de la fonction de hachage utilisée, il est facile de calculer les numéros de référence dans la cohorte de recherche.

- *Réseaux sociaux*

Il a été démontré[19] que des informations sensibles à propos d'individus spécifiques peuvent être extraites des graphes de réseaux sociaux, malgré les techniques de «pseudonymisation» appliquées à ces données. L'exploitant d'un réseau social a supposé à tort que la pseudonymisation suffisait à empêcher l'identification après la vente des données à d'autres sociétés à des fins de marketing et de publicité. À la place des noms réels, l'exploitant utilisait des pseudonymes, mais ce n'est manifestement pas assez pour anonymiser les profils d'utilisateurs, étant donné que les relations entre les différents individus sont uniques et peuvent servir d'identifiants.

- *Localisation*

Les chercheurs du MIT[20] ont récemment analysé un ensemble de données pseudonymisé couvrant 15 mois de coordonnées mobiles spatiales et temporelles de 1,5 million de personnes sur un territoire d'un rayon de 100 km. Ils ont démontré que quatre points de localisation permettaient d'isoler 95 % de cette population et que deux points seulement suffisaient pour isoler plus de 50 % des personnes concernées (un seul point étant supposé être très probablement le domicile ou le lieu de travail), ce qui laissait très peu de place à la

[19] A. Narayanan et V. Shmatikov, «De-anonymizing social networks», in *30th IEEE Symposium on Security and Privacy*, 2009.
[20] Y.-A. de Montjoye, C. Hidalgo, M. Verleysen et V. Blondel, «Unique in the Crowd: The privacy bounds of human mobility», *Nature*, n° 1376, 2013.

protection de la vie privée, même si les identités des individus avaient été pseudonymisées en remplaçant leurs attributs réels [….] par d'autres étiquettes.

5. Conclusions et recommandations

5.1. Conclusions

Les techniques d'anonymisation font l'objet de recherches intensives, et le présent document a invariablement montré que chaque technique a ses avantages et ses inconvénients. Le plus souvent, il n'est pas possible de formuler des recommandations minimales quant aux paramètres à utiliser, étant donné que chaque ensemble de données doit être envisagé au cas par cas.

Dans beaucoup de situations, un ensemble de données anonymisées peut encore présenter un risque résiduel pour les personnes concernées. En effet, même quand il n'est plus possible de reconstituer précisément l'enregistrement d'un individu, il reste parfois possible de glaner des informations à propos de cet individu à l'aide d'autres sources d'informations disponibles (publiquement ou non). Il faut souligner qu'au-delà de l'impact direct produit par les conséquences d'un processus d'anonymisation inefficace sur les personnes concernées (désagrément, temps perdu et sentiment de perte de contrôle du fait de l'inclusion dans un groupe sans notification ni accord préalable), d'autres effets secondaires indirects peuvent survenir quand une personne concernée est erronément prise pour cible par un quelconque attaquant, à la suite du traitement de données anonymisées – surtout si les intentions de l'attaquant sont malveillantes. C'est pourquoi le groupe de travail «Article 29» insiste sur le fait que les techniques d'anonymisation peuvent apporter des garanties en matière de respect de la vie privée, mais uniquement si leur application est correctement conçue – ce qui suppose que les conditions préalables (le contexte) et les objectif(s) du processus d'anonymisation soient clairement définis de façon à assurer le niveau d'anonymisation visé.

5.2. Recommandations

- Il existe des limitations inhérentes à certaines techniques d'anonymisation. Ces limitations doivent être envisagées avec attention par les responsables du traitement avant de recourir à une technique donnée pour élaborer un processus d'anonymisation. Il faut prendre en considération les finalités que l'anonymisation vise à atteindre – comme de protéger la vie privée des personnes lors de la publication d'un ensemble de données, ou de permettre l'obtention de certaines informations à partir d'un ensemble de données.
- Aucune des techniques décrites dans le présent document ne satisfait de façon certaine aux critères d'une anonymisation efficace (à savoir, empêcher l'individualisation d'une personne concernée, la corrélation entre les enregistrements se rapportant à un individu et l'obtention par inférence de données concernant un individu). Cependant, dès lors que certains de ces risques peuvent être évités complètement ou partiellement au moyen d'une technique donnée, il est nécessaire de concevoir avec soin l'application d'une technique individuelle à la situation concernée et d'opter pour une combinaison de ces techniques en vue de renforcer la fiabilité du résultat.

Le tableau présenté ci-après donne un aperçu des forces et des faiblesses des techniques considérées au regard des trois exigences fondamentales:

	Reste-t-il un risque d'individualisation?	Reste-t-il un risque de corrélation?	Reste-t-il un risque d'inférence?
Pseudonymisation	Oui	Oui	Oui
Ajout de bruit	Oui	Peut-être pas	Peut-être pas
Substitution	Oui	Oui	Peut-être pas
Agrégation ou k-anonymat	Non	Oui	Oui
l-diversité	Non	Oui	Peut-être pas
Confidentialité différentielle	Peut-être pas	Peut-être pas	Peut-être pas
Hachage/Tokenization	Oui	Oui	Peut-être pas

Tableau 6. Forces et faiblesses des techniques considérées

- La solution optimale devrait être choisie au cas par cas. Une solution (c'est-à-dire un processus d'anonymisation complet) répondant aux trois critères résisterait aux tentatives d'identification utilisant les moyens les plus susceptibles d'être raisonnablement mis en œuvre par le responsable du traitement des données ou par des tiers.
- Lorsqu'un des critères n'est pas rempli par une proposition, il convient de procéder à une évaluation approfondie des risques d'identification. Cette évaluation devrait être soumise à l'autorité compétente si le droit national requiert l'examen ou l'autorisation du processus d'anonymisation par ladite autorité.

Afin de réduire les risques d'identification, les bonnes pratiques suivantes devraient être prises en considération:

Bonne pratique d'anonymisation

En général:

- Ne pas se contenter de «publier et oublier». Compte tenu du risque résiduel d'identification, les responsables du traitement des données devraient:
  - 1. identifier les nouveaux risques et réévaluer régulièrement le(s) risque(s) résiduel(s);
  - 2. examiner si les contrôles des risques identifiés sont suffisants et les ajuster en conséquence; ET
  - 3. surveiller et contrôler les risques.
- Parmi ces risques résiduels, la possibilité d'identifier la partie non anonymisée d'un ensemble de données devrait (le cas échéant) être prise en considération, surtout en combinaison avec la partie anonymisée, ainsi que les corrélations possibles entre les attributs (par exemple entre les données relatives à la localisation géographique et celles concernant le niveau de prospérité).

Éléments contextuels:

- Les finalités visées par l'anonymisation d'un ensemble de données devraient être clairement définies, dans la mesure où elles jouent un rôle-clé dans la détermination du risque d'identification.
- Cela va de pair avec la prise en considération de tous les éléments contextuels pertinents – par exemple, la nature des données originales, les mécanismes de contrôle en place (y compris les mesures de sécurité restreignant l'accès aux ensembles de données), la taille de l'échantillon (aspects quantitatifs), la disponibilité de ressources d'informations

publiques (sur lesquelles peuvent s'appuyer les destinataires), la communication envisagée de données à des tiers (limitée ou illimitée, par exemple sur l'internet, etc.).

- Il convient de prendre en considération les attaquants possibles, compte tenu de l'attrait des données pour des attaques ciblées (là encore, le caractère sensible des informations et la nature des données seront des facteurs-clés à cet égard).

Éléments techniques:

- Les responsables du traitement des données devraient divulguer la technique d'anonymisation / la combinaison de techniques appliquée, surtout s'ils prévoient de diffuser l'ensemble de données anonymisées.
- Les attributs évidents (par exemple, rares) / quasi-identifiants devraient être supprimés de l'ensemble de données.
- Si des techniques d'ajout de bruit sont utilisées (dans le cadre de la randomisation), le niveau de bruit ajouté aux enregistrements devrait être déterminé en fonction de la valeur d'un attribut (c'est-à-dire qu'il ne faut pas injecter un bruit démesuré), de l'impact des attributs à protéger pour les personnes concernées et/ou du caractère clairsemé de l'ensemble de données.
- En cas de recours à la confidentialité différentielle (dans le cadre de la randomisation), il convient de tenir compte de la nécessité de conserver une trace des requêtes de façon à détecter celles qui présentent un risque d'intrusion dans la vie privée, car le caractère intrusif des requêtes est cumulatif.
- Si des techniques de généralisation sont appliquées, il est crucial que le responsable du traitement des données ne se limite pas à un critère de généralisation qui reste inchangé pour le même attribut; c'est-à-dire qu'il convient de sélectionner des granularités géographiques ou des intervalles de temps différents. Le choix du critère à appliquer doit être dicté par la distribution des valeurs des attributs dans la population concernée. Toutes les distributions ne se prêtent pas à une généralisation. Autrement dit, il n'existe pas d'approche universelle à suivre en matière de généralisation. Il importe de veiller à la variabilité au sein des classes d'équivalence; par exemple, un seuil spécifique devrait être sélectionné en fonction des «éléments contextuels» mentionnés ci-dessus (taille de l'échantillon, etc.) et, si ce seuil n'est pas atteint, il conviendrait de rejeter l'échantillon concerné (ou de définir un critère de généralisation différent).

ANNEXE
Un aperçu des techniques d'anonymisation

29

A.1. Introduction

Il existe dans l'Union différentes interprétations de l'anonymat: dans certains pays, la notion correspond à un anonymat informatique (c'est-à-dire qu'il doit être difficile, en termes de puissance de calcul, d'identifier directement ou indirectement une des personnes concernées, même pour le responsable du traitement des données, avec la collaboration de quelque autre partie) et dans d'autres pays, il s'agit d'un anonymat parfait (c'est-à-dire qu'il doit être impossible d'identifier directement ou indirectement une des personnes concernées, même pour le responsable du traitement des données, avec la collaboration de quelque autre partie). Néanmoins, l'«anonymisation» désigne dans les deux cas le processus au moyen duquel des données sont rendues anonymes. La différence réside dans ce qui est considéré comme un niveau acceptable de risque de ré-identification.

Divers usages peuvent être envisagés pour les données anonymisées: enquêtes sociales, analyses statistiques, développement de nouveaux services/produits. Aussi générales que soient les finalités poursuivies, il arrive parfois que ces activités puissent avoir un impact sur certaines personnes concernées, annulant le caractère prétendument anonyme des données traitées. On peut en citer de nombreux exemples, depuis le lancement d'actions de marketing ciblées jusqu'à la mise en œuvre de mesures publiques fondées sur les profils, les comportements ou les schémas de mobilité des utilisateurs[21].

Malheureusement, hormis les déclarations générales, il n'existe pas de système de mesure suffisamment évolué qui permette d'apprécier à l'avance le temps ou les efforts nécessaires pour parvenir à une ré-identification après le traitement, ou encore de sélectionner la procédure la plus appropriée à mettre en place si l'on veut réduire la probabilité qu'une base de données diffusée renvoie à un ensemble identifié de personnes concernées.

L'«art de l'anonymisation», ainsi qu'on désigne parfois ces pratiques dans la littérature scientifique[22], est une nouvelle branche scientifique encore balbutiante et il existe beaucoup de pratiques visant à réduire la capacité d'identification des ensembles de données; il doit être bien clair, cependant, que la majorité de ces pratiques n'empêchent pas la mise en relation des données traitées avec les personnes concernées. Dans certaines circonstances, les tentatives d'identification d'ensembles de données censés être anonymes ont été couronnées de succès; dans d'autres situations, des faux positifs ont été constatés.

Il existe, en gros, deux approches différentes: l'une se fonde sur la généralisation de l'attribut, l'autre sur la randomisation. Un examen des détails et des subtilités de ces pratiques nous aidera à mieux comprendre le potentiel d'identification des données et jettera un nouvel éclairage sur la notion même de données à caractère personnel.

A.2. L'«anonymisation» par randomisation

En matière d'anonymisation, une option consiste à modifier les valeurs réelles pour empêcher que les données anonymisées puissent être mises en relation avec les valeurs originales. Cet objectif peut être atteint au moyen de nombreuses méthodes, qui vont de l'injection de bruit à

[21] Par exemple, dans le cas de TomTom aux Pays-Bas (voir l'exemple expliqué à la section 2.2.3).
[22] Jun Gu,Yuexian Chen, Junning Fu, HuanchunPeng, Xiaojun Ye, *Synthesizing: Art of Anonymization, Database and Expert Systems Applications Lecture Notes in Computer Science*, Springer, volume 6261, 2010, p. 385 à 399.

30

la substitution de données (permutation). Il faut aussi souligner que la suppression d'un attribut équivaut à une forme extrême de randomisation dudit attribut (lequel est alors entièrement couvert par le bruit).

Dans certaines circonstances, l'objectif du traitement n'est pas tant de publier un ensemble de données randomisées, mais plutôt de permettre l'accès aux données au moyen de requêtes. Le risque pour les personnes concernées vient dans ce cas de la probabilité qu'un attaquant soit en mesure d'obtenir des informations en transmettant une série de requêtes différentes, sans que le responsable du traitement des données en ait connaissance. Pour garantir l'anonymat des individus auxquels se rapporte l'ensemble de données, il faudrait qu'il ne soit pas possible de conclure qu'une personne concernée a contribué à l'ensemble de données, de façon à rompre le lien avec d'éventuelles informations tirées du contexte qu'un attaquant pourrait avoir en sa possession.

En ajoutant du bruit, selon les modalités appropriées, à la réponse à une requête, il est possible de réduire encore le risque de ré-identification. Cette approche, désignée dans la littérature par les termes de «confidentialité différentielle»[23], s'écarte des méthodes décrites précédemment en ce qu'elle donne à ceux qui publient des données un plus grand contrôle sur l'accès aux données par rapport à une diffusion publique. L'ajout de bruit vise deux objectifs principaux: premièrement, protéger la vie privée des personnes concernées reprises dans l'ensemble de données et, deuxièmement, préserver l'utilité des informations communiquées. En particulier, l'ampleur du bruit doit être proportionnelle au niveau des requêtes (des réponses trop précises à de trop nombreuses requêtes concernant des individus augmentent le risque d'identification). Pour être efficace, l'application de la randomisation doit aujourd'hui être envisagée au cas par cas, car aucune technique ne constitue une méthodologie à toute épreuve. Il existe des exemples de fuites d'informations à propos des attributs d'une personne concernée (figurant ou non dans l'ensemble de données), alors même que le responsable du traitement considérait l'ensemble de données comme randomisé.

Il peut être utile d'examiner des exemples précis pour mettre en lumière les failles possibles de la randomisation, en tant que procédé d'anonymisation. Ainsi, dans le cas d'un accès interactif, des requêtes jugées anodines en termes de confidentialité pourraient représenter un risque pour la vie privée des personnes concernées. En fait, si l'attaquant sait qu'un sous-groupe S d'individus figure dans l'ensemble de données qui contient des informations relatives à l'incidence d'un attribut A dans une population P, en posant simplement les deux questions «Combien d'individus dans la population P possèdent l'attribut A?» et «Combien d'individus dans la population P, hormis ceux repris dans le sous-groupe S, possèdent l'attribut A?», il peut être possible de déterminer (par soustraction) le nombre d'individus du sous-groupe S qui possèdent effectivement l'attribut A – soit de façon certaine, soit par inférence probabiliste. En tout cas, le respect de la vie privée des individus du sous-groupe S pourrait être gravement compromis, selon la nature de l'attribut A.

On peut aussi considérer que la publication d'un ensemble de données peut présenter un risque pour la vie privée d'une personne concernée qui n'y est pas reprise, s'il existe un lien connu entre cette personne et des données figurant dans cet ensemble. Par exemple, si l'on sait que «la valeur de l'attribut A de la cible diffère dans une quantité X de la valeur moyenne de la population», en demandant simplement à l'administrateur de la base de données d'exécuter une opération – anodine en termes de confidentialité – d'extraction de la valeur

[23] Cynthia Dwork, *Differential Privacy, International Colloquium on Automata, Languages and Programming*, ICALP, 2006, p. 1 à 12

moyenne de l'attribut A, l'attaquant peut déduire avec exactitude des données à caractère personnel relatives à une personne concernée en particulier.

L'opération qui consiste à injecter certaines inexactitudes relatives dans les valeurs réelles d'une base de données doit être conçue correctement. Il faut ajouter suffisamment de bruit pour protéger la confidentialité, mais pas trop non plus, afin de préserver l'utilité des données. Par exemple, si le nombre de personnes concernées présentant un attribut particulier est très réduit ou si l'attribut a un caractère hautement sensible, il peut être préférable de s'en tenir à une fourchette, ou à une phrase générale, du genre «un petit nombre de cas, peut-être même zéro», plutôt que d'indiquer le chiffre exact. De cette façon, même si le mécanisme d'ajout de bruit est connu à l'avance, la vie privée des personnes concernées est respectée, puisqu'il subsiste un degré d'incertitude. Du point de vue de l'utilité, si l'inexactitude est correctement conçue, les résultats restent utiles à des fins d'analyse statistique ou de prise de décision.

La randomisation d'une base de données et l'accès en confidentialité différentielle requièrent une réflexion plus poussée. Premièrement, la juste dose de distorsion peut varier considérablement selon le contexte (le type de requête, la taille de la population de la base de données, la nature de l'attribut et le risque d'identification inhérent) et aucune solution universelle ne peut être envisagée. De plus, le contexte peut changer avec le temps et le mécanisme interactif devrait être modifié en conséquence. Le calibrage du bruit nécessite une surveillance des risques cumulatifs qu'un mécanisme interactif représente pour le respect de la vie privée des personnes concernées. Le mécanisme d'accès aux données devrait donc disposer d'alertes qui se déclenchent lorsqu'un budget «coût pour la confidentialité» est épuisé et que les personnes concernées pourraient être exposées à des risques spécifiques si une nouvelle requête est transmise, afin d'aider le responsable du traitement des données à déterminer le niveau approprié de distorsion qu'il y a lieu d'injecter à chaque fois dans les données à caractère personnel.

D'un autre côté, il faut aussi envisager le cas où des valeurs d'attributs sont supprimées (ou modifiées). Une solution souvent employée pour traiter certaines valeurs d'attributs atypiques est la suppression de l'ensemble de données relatives aux individus atypiques ou des valeurs atypiques. Dans ce dernier cas, il est important de veiller à ce que l'absence de la valeur ne devienne pas en elle-même un élément permettant l'identification d'une personne concernée.

Passons à présent à la randomisation par substitution d'attribut. Une des principales idées fausses qui circulent à propos de l'anonymisation consiste à l'assimiler au chiffrement ou au codage à clé. Cette erreur repose sur deux suppositions, à savoir a) que lorsque certains attributs d'un enregistrement dans une base de données (par exemple, le nom, l'adresse, la date de naissance) font l'objet d'un chiffrement ou qu'une chaîne apparemment aléatoire leur est substituée à la suite d'une opération de codage à clé, comme une fonction de hachage, cet enregistrement est «anonymisé», et b) que l'anonymisation est plus efficace si la longueur de la clé est appropriée et si l'algorithme de chiffrement est conforme à l'état de la technique. Cette idée fausse est largement répandue parmi les responsables du traitement des données et appelle des éclaircissements, car elle se rapporte aussi à la pseudonymisation et à ses risques prétendument moindres.

Premièrement, les objectifs de ces techniques sont radicalement différents: le chiffrement, en tant que mesure de sécurité, vise à garantir la confidentialité d'un canal de communication entre des parties identifiées (êtres humains, appareils ou éléments logiciels/matériels) afin d'éviter une interception ou une divulgation involontaire. Le codage à clé correspond à une traduction sémantique des données qui dépend d'une clé secrète. L'objectif de

l'anonymisation, en revanche, est d'éviter l'identification d'individus en empêchant que des attributs puissent être mis en relation avec une personne concernée à son insu.

Ni le chiffrement ni le codage à clé ne se prêtent, en eux-mêmes, à l'objectif de rendre une personne concernée non identifiable, puisque les données originales, entre les mains du responsable du traitement au moins, peuvent encore être consultées ou reconstituées par déduction. La seule traduction sémantique de données à caractère personnel, telle qu'elle est appliquée dans le cas du codage à clé, n'exclut pas la possibilité de rétablir la structure originale des données, en exécutant l'algorithme en sens inverse ou au moyen d'attaques par force brute, selon la nature des mécanismes employés, ou à la suite d'une violation de données. Un chiffrement conforme à l'état de la technique peut garantir une meilleure protection des données, c'est-à-dire empêcher leur consultation par des entités qui ignorent la clé de décryptage, mais il ne se traduit pas nécessairement par une anonymisation. Tant que la clé ou les données originales sont accessibles (même dans le cas de leur conservation par un tiers de confiance, tenu par contrat d'assurer un service de séquestre), la possibilité d'identifier une personne concernée n'a pas été éliminée.

Le fait de se fonder exclusivement sur la robustesse du mécanisme de chiffrement comme mesure du degré d'«anonymisation» d'un ensemble de données est trompeur, car de nombreux autres facteurs techniques et organisationnels affectent la sécurité générale d'un mécanisme de chiffrement ou d'une fonction de hachage. La littérature fait état de beaucoup d'attaques couronnées de succès, qui contournent totalement l'algorithme, en exploitant les faiblesses de la conservation des clés (par exemple, l'existence d'un mode par défaut moins sécurisé) ou d'autres facteurs humains (par exemple, des mots de passe faibles permettant de récupérer la clé). Enfin, un système de chiffrement sélectionné, avec une clé d'une taille donnée, est conçu pour garantir la confidentialité pendant une certaine période (la taille de la plupart des clés actuelles devra être revue vers 2020), tandis qu'un processus d'anonymisation ne devrait pas être limité dans le temps.

Il peut être intéressant d'examiner en détail les limites de la randomisation (ou de la substitution et de la suppression) de l'attribut, à la lumière de divers exemples d'anonymisation par randomisation inefficaces recensés ces dernières années et des raisons qui expliquent ces échecs.

Un cas bien connu de diffusion d'un ensemble de données mal anonymisé est celui du prix Netflix[24]. En examinant un enregistrement générique dans une base de données dont plusieurs attributs relatifs à une personne concernée ont été randomisés, chaque enregistrement peut encore être scindé en deux sous-enregistrements comme suit: {attributs randomisés, attributs en clair}, où les attributs en clair peuvent constituer n'importe quelle combinaison de données qui ne sont pas censées avoir un caractère personnel. Dans le cas de l'ensemble de données du prix Netflix, il est à noter que chaque enregistrement peut être représenté par un point dans un espace multidimensionnel, où chaque attribut en clair est une coordonnée. En appliquant cette technique, tout ensemble de données peut être considéré comme une constellation de points dans cet espace multidimensionnel, qui présente parfois un caractère très clairsemé, c'est-à-dire que les points sont distants les uns des autres. En fait, ils peuvent être si éloignés qu'après avoir divisé l'espace en vastes régions, chaque région ne contient qu'un seul enregistrement. Même l'injection de bruit ne parvient pas à rapprocher suffisamment les enregistrements pour qu'ils partagent la même région multidimensionnelle. Dans l'expérience de Netflix, par exemple, 8 évaluations de films attribuées au cours d'une période s'étendant sur 14 jours

[24] Arvind Narayanan, Vitaly Shmatikov, «Robust De-anonymization of Large Sparse Datasets», in *IEEE Symposium on Security and Privacy*, 2008, p. 111 à 125

suffisaient à rendre les enregistrements uniques. Après l'ajout de bruit aux évaluations et aux dates, aucune superposition de régions ne pouvait être constatée. Autrement dit, cette même sélection de 8 films évalués constituait une empreinte digitale des évaluations attribuées, qui n'était pas partagée par deux personnes concernées dans la base de données. Sur la base de cette observation géométrique, les chercheurs ont comparé l'ensemble de données prétendument anonyme de Netflix avec une autre base de données publique contenant des évaluations de films (IMDB) et découvert ainsi des utilisateurs qui avaient attribué des évaluations pour les mêmes films au cours de la même période. Comme la majorité des utilisateurs présentaient une correspondance biunivoque, les informations auxiliaires récupérées dans la base de données IMDB ont pu être importées dans l'ensemble de données publiées par Netflix, de façon à identifier tous les enregistrements censés être anonymes.

Il est important de souligner qu'il s'agit d'une propriété générale: la part résiduelle de toute base de données «randomisée» conserve un potentiel d'identification très élevé, selon la rareté de la combinaison des attributs résiduels. C'est une mise en garde que les responsables du traitement des données devraient toujours avoir à l'esprit en choisissant la randomisation comme moyen de parvenir à l'anonymisation recherchée.

De nombreuses expériences de ré-identification de ce type ont été menées selon une approche similaire de projection de deux bases de données sur le même sous-espace. C'est une méthode de ré-identification très puissante, qui a récemment été appliquée dans de nombreux domaines différents. Par exemple, une expérience d'identification réalisée à l'encontre d'un réseau social[25] a exploité le graphe social d'utilisateurs pseudonymisés au moyen d'étiquettes. Dans ce cas, les attributs utilisés à des fins d'identification étaient les listes de contacts des différents utilisateurs, puisqu'il avait été démontré que la probabilité que deux individus aient une liste de contacts identique est très faible. Sur la base de cette hypothèse intuitive, il a été constaté qu'un sous-graphe de liens internes comportant un nombre très limité de nœuds constitue une empreinte topologique exploitable, cachée au sein du réseau, et qu'une large portion de l'ensemble du réseau social peut être identifiée dès lors que ce sous-réseau a été délimité. Pour ne donner que quelques chiffres sur les performances d'une attaque similaire, il a été démontré qu'en utilisant moins de 10 nœuds (qui peuvent déboucher sur des millions de configurations de sous-réseaux différentes, chacun constituant potentiellement une empreinte topologique) un réseau social de plus de 4 millions de nœuds pseudonymisés et de 70 millions de liens peut être vulnérable à des attaques de ré-identification susceptibles de compromettre un grand nombre de relations. Il faut ajouter que cette approche de ré-identification n'est pas limitée au contexte spécifique des réseaux sociaux, mais est suffisamment générale pour pouvoir être adaptée à d'autres bases de données où les relations entre les utilisateurs sont enregistrées (par exemple, un répertoire téléphonique, une messagerie électronique, des sites de rencontre, etc.).

Un autre moyen d'identifier un enregistrement supposé anonyme repose sur l'analyse du style de rédaction (stylométrie)[26]. Plusieurs algorithmes ont déjà été mis au point pour extraire des mesures de texte analysé, qui couvrent la fréquence d'utilisation d'un mot particulier, l'occurrence de constructions grammaticales spécifiques et le type de ponctuation. Toutes ces propriétés peuvent être utilisées pour associer un texte censé être anonyme au style de rédaction d'un auteur identifié. Des chercheurs ont extrait le style de rédaction de plus de 100 000 blogs et sont aujourd'hui capables d'identifier automatiquement l'auteur d'un

[25] L. Backstrom, C. Dwork, et J. M. Kleinberg, «Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography», compte rendu de la 16e Conférence internationale sur le World Wide Web WWW'07, p. 181 à 190 (2007).
[26] http://33bits.org/2012/02/20/is-writing-style-sufficient-to-deanonymize-material-posted-online/

34

message avec une précision approchant déjà de 80 %; l'efficacité de cette technique devrait aussi se renforcer avec l'exploitation d'autres indications, comme la localisation ou des métadonnées contenues dans le texte.

Le potentiel d'identification au moyen de la sémantique d'un enregistrement (à savoir la part résiduelle non randomisée d'un enregistrement) est un problème qui mérite davantage de considération de la part des milieux de la recherche et de l'industrie. L'exemple récent d'une tentative couronnée de succès visant à rétablir les identités de donneurs d'ADN (2013)[27] montre que peu de progrès ont été accomplis depuis la célèbre affaire AOL (2006), où une base de données contenant vingt millions de mots-clés figurant dans les recherches effectuées par plus de 650 000 utilisateurs au cours d'une période de 3 mois avait été diffusée publiquement. À la suite de quoi, l'identité et la localisation de certains utilisateurs avaient été rendues publiques.

Les données de localisation constituent une autre famille de données dont l'anonymat est rarement garanti par le simple fait de supprimer les identités des personnes concernées ou par le chiffrement partiel de certains attributs. Les schémas de mobilité sont peut-être suffisamment uniques pour que la partie sémantique des données de localisation (le lieu où la personne concernée se trouvait à un certain moment), même en l'absence d'autres attributs, permette de révéler bon nombre de caractéristiques d'une personne concernée[28]. Cela a été démontré bien des fois dans des travaux universitaires représentatifs[29].

À cet égard, il faut se garder de considérer les pseudonymes comme un moyen d'assurer une protection adéquate des personnes concernées contre les fuites d'identité ou d'attribut. Si la pseudonymisation se fonde sur le remplacement d'une identité par un autre code unique, il serait naïf de supposer qu'un tel procédé constitue une solution d'anonymisation fiable, sans tenir compte de la complexité des méthodes d'identification et des multiples contextes dans lesquels elles pourraient être appliquées.

A.3. L'«anonymisation» par généralisation

Un exemple simple peut contribuer à clarifier l'approche fondée sur la généralisation de l'attribut.

Prenons le cas d'un responsable du traitement des données qui décide de publier un simple tableau contenant trois éléments d'information, ou attributs: un numéro d'identification, unique pour chaque enregistrement, une identification de localisation, qui relie la personne concernée au lieu où elle vit, et une identification de propriété, qui spécifie la propriété de la personne concernée. Supposons en outre que cette propriété correspond à une valeur parmi deux valeurs distinctes, indiquée de façon générique par {P1, P2}:

[27] Les données génétiques constituent un exemple particulièrement important de données sensibles, qui peuvent être exposées à un risque de ré-identification si le seul mécanisme censé les «anonymiser» est la suppression des identités des donneurs. Voir l'exemple cité à la section 2.2.2 ci-dessus. Voir aussi John Bohannon, «Genealogy Databases Enable Naming of Anonymous DNA Donors», *Science*, vol. 339, n° 6117 (18 janvier 2013), p. 262.
[28] Ce problème a été pris en compte dans certaines législations nationales. Par exemple, en France, les statistiques de localisation publiées sont anonymisées par des techniques de généralisation et de permutation. Ainsi, l'INSEE publie des statistiques qui sont généralisées en agrégeant toutes les données au niveau d'une superficie de 40 000 mètres carrés. La granularité de l'ensemble de données est suffisante pour préserver l'utilité des données et des permutations empêchent des attaques de ré-identification dans les zones clairsemées. D'une manière plus générale, l'agrégation de cette famille de données et la permutation apportent de solides garanties contre les attaques par inférence et les tentatives de ré-identification (http://www.insee.fr/fr/).
[29] De Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M. et Blondel, V.D., «Unique in the Crowd: The privacy bounds of human mobility», *Nature*, 3, 1376 (2013).

Identification par n° d'ordre	Localisation	Propriété
N° 1	Rome	P1
N° 2	Madrid	P1
N° 3	Londres	P2
N° 4	Paris	P1
N° 5	Barcelone	P1
N° 6	Milan	P2
N° 7	New York	P2
N° 8	Berlin	P1

Tableau A1. Échantillon de personnes concernées, avec leur localisation et leurs propriétés P1 ou P2

Si quelqu'un, qu'on appellera «l'attaquant», sait à l'avance qu'une personne concernée spécifique (la cible), qui vit à Milan, figure dans le tableau, il lui suffit d'examiner le tableau pour apprendre aussi que sa propriété est P2, le n° 6 étant la seule personne concernée identifiée par cette localisation.

Cet exemple très sommaire montre les principaux éléments de toute procédure d'identification appliquée à un ensemble de données qui a fait l'objet d'un processus d'anonymisation supposé. C'est-à-dire qu'un attaquant se trouve (accidentellement ou délibérément) en possession de connaissances tirées du contexte à propos de certaines ou de toutes les personnes concernées dans un ensemble de données. L'attaquant s'efforce de relier ces connaissances tirées du contexte avec les données figurant dans l'ensemble de données publié pour avoir une idée plus claire des caractéristiques de ces personnes concernées.

Afin de rendre moins efficace ou moins immédiate la mise en relation des données avec une forme quelconque de connaissances tirées du contexte, le responsable du traitement des données pourrait intervenir sur l'identification de localisation, en remplaçant la ville où vivent les personnes concernées par une zone plus large, comme le pays. De cette façon, le tableau se présenterait comme suit:

Identification par n° d'ordre	Localisation	Propriété
N° 1	Italie	P1
N° 2	Espagne	P1
N° 3	Royaume-Uni	P2
N° 4	France	P1
N° 5	Espagne	P1
N° 6	Italie	P2
N° 7	États-Unis	P2
N° 8	Allemagne	P1

Tableau A2. Généralisation du tableau A1 par nationalité

Avec cette nouvelle agrégation de données, les connaissances tirées du contexte dont dispose l'attaquant à propos d'une personne concernée identifiée (disons: «la cible vit à Rome et figure dans le tableau») ne permettent pas de parvenir à une conclusion claire concernant sa propriété, puisque les deux Italiens mentionnés dans le tableau ont des propriétés distinctes, respectivement P1 et P2. L'attaquant se trouve confronté à une incertitude de 50 % quant à la propriété de l'entité cible. Ce simple exemple montre l'effet de la généralisation sur la

pratique d'anonymisation. En fait, si ce procédé de généralisation peut être efficace pour réduire de moitié la probabilité d'identifier une cible italienne, il est sans effet dans le cas de cibles vivant à d'autres endroits (aux États-Unis, par exemple).

De plus, un attaquant peut encore obtenir des informations sur une cible espagnole. Si les connaissances tirées du contexte sont du type «la cible vit à Madrid et figure dans le tableau» ou «la cible vit à Barcelone et figure dans le tableau», l'attaquant peut en déduire avec 100 % de certitude que la cible a la propriété P1. Par conséquent, la généralisation ne garantit pas le même niveau de confidentialité ou de résistance aux attaques par inférence à toute la population de l'ensemble de données.

En suivant ce raisonnement, on pourrait être tenté de conclure qu'une généralisation accrue serait utile pour empêcher toute mise en relation – par exemple une généralisation par continent. De cette façon, le tableau se présenterait comme suit:

Identification par n° d'ordre	**Localisation**	**Propriété**
N° 1	Europe	P1
N° 2	Europe	P1
N° 3	Europe	P2
N° 4	Europe	P1
N° 5	Europe	P1
N° 6	Europe	P2
N° 7	Amérique du Nord	P2
N° 8	Europe	P1

Tableau A3. Généralisation du tableau A1 par continent

Avec ce genre d'agrégation, toutes les personnes concernées dans le tableau, hormis celle qui vit aux États-Unis, seraient protégées contre les attaques par corrélation et les tentatives d'identification, et toute information tirée du contexte du type «la cible vit à Madrid et figure dans le tableau» ou «la cible vit à Milan et figure dans le tableau» aboutirait à un certain niveau de probabilité quant à la propriété qui s'applique à la personne concernée (P1 avec une probabilité de 71,4 % et P2 avec une probabilité de 28,6%), plutôt qu'à une mise en relation directe. Mais cette généralisation supplémentaire s'opère au prix d'une perte évidente et radicale d'informations: le tableau ne permet pas de découvrir des corrélations potentielles entre les propriétés et la localisation, c'est-à-dire d'apprécier si un lieu spécifique serait plus susceptible de déclencher l'une des deux propriétés, puisqu'il ne fait apparaître que les distributions dites «marginales», à savoir la probabilité absolue de l'occurrence des propriétés P1 et P2 dans l'ensemble de la population (respectivement 62,5 % et 37,5 % dans notre exemple) et dans chaque continent (respectivement, comme il a été indiqué, 71,4 % et 28,6% en Europe et 100 % et 0 % en Amérique du Nord).

L'exemple montre aussi que le recours à la généralisation affecte l'utilité pratique des données. Il existe aujourd'hui certains outils qui permettent de déterminer au préalable (c'est-à-dire avant qu'un ensemble de données soit rendu public) quel est le niveau de généralisation de l'attribut le plus approprié, de façon à réduire les risques d'identification des personnes concernées dans un tableau sans affecter exagérément l'utilité des données publiées.

k-anonymat

Le k-anonymat est une technique fondée sur la généralisation des attributs qui vise à prévenir les attaques par corrélation. Cette pratique est issue d'une expérience de ré-identification menée à la fin des années 1990, aux États-Unis, où une entreprise privée, active dans le secteur de la santé, a rendu public un ensemble de données censé être anonymisé. Cette anonymisation consistait à effacer les noms des personnes concernées, mais l'ensemble de données contenait encore des informations d'ordre médical et d'autres attributs comme le code postal (identification de localisation indiquant où vivaient les personnes concernées), le sexe et la date de naissance complète. Le même triplet {code postal, sexe, date de naissance complète} figurait aussi dans d'autres registres accessibles au public (par exemple, la liste électorale) et a donc pu être utilisé par un chercheur pour mettre en relation l'identité de certaines personnes concernées avec les attributs de l'ensemble de données publié. Les connaissances tirées du contexte dont disposait l'attaquant (le chercheur) pouvaient être énoncées comme suit: «Je sais que la personne concernée figurant dans la liste électorale avec un triplet {code postal, sexe, date de naissance complète} spécifique est unique. Il existe un enregistrement correspondant à ce triplet dans l'ensemble de données publié.» Il a été constaté empiriquement[30] que la grande majorité (plus de 80 %) des personnes concernées dans le registre public utilisé pour cette expérience de recherche étaient associées de façon univoque à un triplet spécifique, ce qui rendait l'identification possible. Par conséquent, les données n'étaient pas correctement anonymisées dans ce cas.

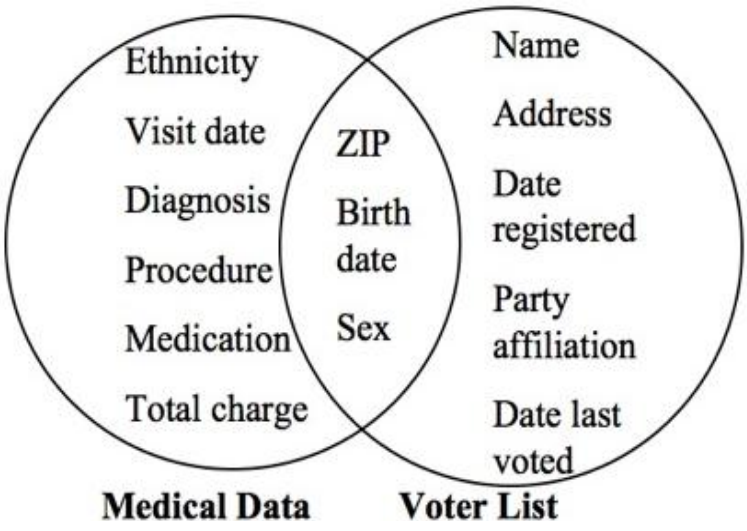


Figure A1. Ré-identification par corrélation entre les données

Afin de réduire l'efficacité d'attaques par corrélation similaires, il a été avancé que les responsables du traitement devraient d'abord examiner l'ensemble de données et regrouper les attributs qui pourraient raisonnablement être exploités par un attaquant pour mettre le tableau publié en relation avec une autre source auxiliaire; chaque groupe devrait inclure au moins *k* combinaisons identiques d'attributs généralisés (c'est-à-dire qu'il devrait représenter une classe d'équivalence d'attributs). Les ensembles de données ne seraient ensuite publiés qu'après avoir été répartis dans de tels groupes homogènes. Les attributs retenus en vue de

[30] L. Sweeney, «Weaving Technology and Policy Together to Maintain Confidentiality», *Journal of Law, Medicine & Ethics*, 25, n° 2 et 3 (1997), p. 98 à 110

leur généralisation sont appelés «quasi-identifiants», puisque leur connaissance, en clair, entraînerait l'identification immédiate des personnes concernées.

De nombreuses expériences d'identification ont démontré la faiblesse de tableaux k-anonymisés mal conçus. Cela peut être dû, par exemple, au fait que les autres attributs d'une classe d'équivalence sont identiques (comme dans le cas de la classe d'équivalence des personnes concernées espagnoles dans l'exemple du tableau A2) ou que leur distribution est très déséquilibrée, avec une forte prévalence d'un attribut spécifique, ou encore au fait que le nombre d'enregistrements dans une classe d'équivalence est très réduit, ce qui permet dans les deux cas une inférence probabiliste, ou qu'il n'existe pas de différence «sémantique» significative entre les attributs en clair des classes d'équivalence (ainsi, la mesure quantitative de ces attributs pourrait être effectivement différente, mais très proche en termes numériques, ou ils pourraient relever d'une gamme d'attributs sémantiquement similaires, par exemple, une même catégorie de risque de crédit ou une même famille de pathologies), de telle sorte que l'ensemble de données peut encore laisser filtrer une grande quantité d'informations sur les personnes concernées exploitables par des attaques par corrélation[31]. Un point important sur lequel il faut insister ici est que, dans tous les cas où les données sont clairsemées (si, par exemple, il y a peu d'occurrences d'une propriété spécifique dans une zone géographique) et où une première agrégation ne permet pas de regrouper les données avec un nombre suffisant d'occurrences de propriétés différentes (si, par exemple, il reste un petit nombre d'occurrences de quelques propriétés seulement qui peuvent être localisées dans une zone géographique), il est nécessaire de procéder à une agrégation d'attributs supplémentaire pour atteindre l'anonymisation recherchée.

l-diversité

À partir de ces observations, des variantes du k-anonymat ont été proposées au fil des années, et certains critères techniques de renforcement de la pratique d'anonymisation par généralisation ont été mis au point, en vue de réduire les risques des attaques par corrélation. Ils se fondent sur des propriétés probabilistes des ensembles de données. En particulier, une contrainte supplémentaire est ajoutée, à savoir que chaque attribut d'une classe d'équivalence apparaît au moins à *l* reprises, de telle sorte qu'un attaquant reste toujours confronté à un degré d'incertitude considérable concernant les attributs, malgré les connaissances tirées du contexte dont il pourrait disposer à propos d'une personne concernée. Cela revient à dire qu'un ensemble de données (ou un segment) doit posséder un nombre minimal d'occurrences d'une propriété sélectionnée: ce procédé permet d'atténuer le risque de ré-identification. Tel est l'objectif de la pratique d'anonymisation à l-diversité. Un exemple de cette pratique est donné dans les tableaux A4 (les données originales) et A5 (le résultat du traitement). Comme on le voit, en traitant correctement l'identification de localisation et les âges des individus du tableau A4, le processus de généralisation d'attributs se traduit par une augmentation considérable de l'incertitude quant aux attributs réels de chaque personne concernée dans l'enquête. Par exemple, même si l'attaquant sait qu'une personne concernée figure dans la première classe d'équivalence, il ne peut déterminer avec plus de certitude si une personne a la propriété X, Y ou Z, puisqu'il existe au moins un enregistrement dans cette classe (et dans n'importe quelle classe d'équivalence) présentant ces propriétés.

[31] Il faut souligner que des corrélations peuvent aussi être établies une fois que les enregistrements ont été regroupés par attributs. Quand le responsable du traitement des données sait quels sont les types de corrélations qu'il souhaite vérifier, il peut sélectionner les attributs les plus pertinents. Par exemple, les résultats des enquêtes du centre PEW ne sont pas vulnérables à des attaques par inférence à granularité fine et restent très utiles pour la recherche de corrélations entre les données démographiques et les interêts (http://www.pewinternet.org/Reports/2013/Anonymity-online.aspx).

Numéro d'ordre	Identification de localisation	Âge	Propriété
1	111	38	X
2	122	39	X
3	122	31	Y
4	111	33	Y
5	231	60	Z
6	231	65	X
7	233	57	Y
8	233	59	Y
9	111	41	Z
10	111	47	Z
11	122	46	Z
12	122	45	Z

Tableau A4. Un tableau où les individus sont regroupés par localisation, âge et trois propriétés X, Y et Z

Numéro d'ordre	Identification de localisation	Âge	Propriété
1	11*	<50	X
4	11*	<50	Y
9	11*	<50	Z
10	11*	<50	Z
5	23*	>50	Z
6	23*	>50	X
7	23*	>50	Y
8	23*	>50	Y
2	12*	<50	X
3	12*	<50	Y
11	12*	<50	Z
12	12*	<50	Z

Tableau A5. Un exemple de version à 1-diversité du tableau A4

t-proximité:

L'approche désignée par le terme «t-proximité» prend en considération le cas particulier des attributs qui sont distribués de manière inégale au sein d'un segment ou qui ne présentent qu'un faible écart de valeurs ou de contenus sémantiques. C'est une amélioration supplémentaire de l'anonymisation par généralisation consistant à organiser les données de façon à créer des classes d'équivalence qui reflètent autant que possible la distribution initiale des attributs dans l'ensemble de données original. À cet effet, une procédure en deux étapes est appliquée comme suit. Le tableau A6 constitue la base de données originale comprenant les enregistrements en clair des personnes concernées, groupées par localisation, âge, salaire et deux familles de propriétés sémantiquement similaires, respectivement {X1,X2, X3} et {Y1, Y2, Y3} (par exemple, des classes de risque de crédit similaires, des maladies similaires). Premièrement, le tableau est *l-diversifié* avec une valeur *l*=1 (tableau A7), en regroupant des enregistrements en classes d'équivalence sémantiquement similaires qui présentent un faible niveau d'anonymisation ciblée; puis il est traité en vue d'obtenir une t-proximité (tableau A8) et une plus grande variabilité au sein de chaque segment. En fait, après cette deuxième étape, chaque classe d'équivalence comprend des enregistrements des deux

40

familles de propriétés. Il est à noter que l'identification de localisation et l'âge ont des granularités différentes dans les diverses étapes du processus: il s'ensuit que chaque attribut peut nécessiter des critères de généralisation différents pour parvenir à l'anonymisation recherchée, ce qui à son tour requiert, de la part des responsables du traitement des données, un ajustement spécifique et un calcul informatique approprié.

Numéro d'ordre	Identification de localisation	Âge	Salaire	Propriété
1	1127	29	30 000	X1
2	1112	22	32 000	X2
3	1128	27	35 000	X3
4	1215	43	50 000	X2
5	1219	52	120 000	Y1
6	1216	47	60 000	Y2
7	1115	30	55 000	Y2
8	1123	36	100 000	Y3
9	1117	32	110 000	X3

Tableau A6. Un tableau où les individus sont regroupés par localisation, âge, salaire et deux familles de propriétés

Numéro d'ordre	Identification de localisation	Âge	Salaire	Propriété
1	11**	2*	30 000	X1
2	11**	2*	32 000	X2
3	11**	2*	35 000	X3
4	121*	>40	50 000	X2
5	121*	>40	120 000	Y1
6	121*	>40	60 000	Y2
7	11**	3*	55 000	Y2
8	11**	3*	100 000	Y3
9	11**	3*	110 000	X3

Tableau A7. Une version à 1-diversité du tableau A6

Numéro d'ordre	Identification de localisation	Âge	Salaire	Propriété
1	112*	<40	30 000	X1
3	112*	<40	35 000	X3
8	112*	<40	100 000	Y3
4	121*	>40	50 000	X2
5	121*	>40	120 000	Y1
6	121*	>40	60 000	Y2
2	111*	<40	32 000	X2
7	111*	<40	55 000	Y2
9	111*	<40	110 000	X3

Tableau A8. Une version à t-proximité du tableau A6

Il faut préciser que l'objectif de la généralisation des attributs des personnes concernées par des procédés aussi élaborés ne peut parfois être atteint que pour un petit nombre d'enregistrements et non pour l'ensemble d'entre eux. Les bonnes pratiques devraient veiller à ce que chaque classe d'équivalence contienne plusieurs individus et qu'aucune attaque par

inférence ne reste possible. En tout cas, cette approche requiert un examen approfondi des données disponibles de la part des responsables du traitement, ainsi qu'une analyse combinatoire de diverses alternatives (par exemple, des fourchettes d'amplitudes différentes, une granularité différente en termes de localisation ou d'âge, etc.). Autrement dit, l'anonymisation par généralisation ne peut être le résultat d'une tentative rudimentaire qui consisterait, pour les responsables du traitement des données, à remplacer des valeurs d'attributs analytiques dans un enregistrement par des fourchettes. Des approches quantitatives plus spécifiques sont nécessaires, de façon par exemple à évaluer l'entropie des attributs au sein de chaque segment ou à mesurer la distance entre les distributions originales des attributs et la distribution dans chaque classe d'équivalence.

42

Avis sur la notion d'intérêt légitime poursuivi par le responsable du traitement de données au sens de l'article 7 de la directive 95/46/CE (WP217)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

844/14/FR
WP 217

Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE

Adopté le 9 avril 2014

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Son secrétariat est assuré par la direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale «Justice» de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013.

Site internet: http://ec.europa.eu/justice/data-protection/index_fr.htm

Table des matières

Résumé

Le présent avis analyse les critères légitimant le traitement des données énoncés à l'article 7 de la directive 95/46/CE. Il se concentre sur l'intérêt légitime poursuivi par le responsable du traitement et formule des orientations pour l'application de l'article 7, point f), dans le cadre juridique actuel, ainsi que des recommandations d'améliorations futures.

L'article 7, point f), est le dernier des six motifs qui rendent licite le traitement des données à caractère personnel. Dans les faits, il requiert la mise en balance de l'intérêt légitime poursuivi par le responsable du traitement, ou par les tiers auxquels les données sont communiquées, et des intérêts ou des droits fondamentaux de la personne concernée. Le résultat de cette mise en balance déterminera si l'article 7, point f), peut être invoqué pour justifier le traitement.

Le groupe de travail «Article 29» mesure toute l'importance et l'utilité du critère fixé par l'article 7, point f), qui, lorsque les circonstances s'y prêtent et moyennant des garanties adéquates, permet d'éviter un recours excessif à d'autres fondements juridiques. L'article 7, point f), ne saurait servir uniquement «en dernier ressort», dans les situations rares ou inattendues où l'on considère que les autres motifs légitimant le traitement ne s'appliquent pas. Il faut néanmoins éviter de s'y référer automatiquement ou d'en élargir indûment l'utilisation au prétexte qu'il semble moins contraignant que les autres motifs.

Une appréciation correcte de l'article 7, point f), ne se borne pas à une simple mise en balance consistant à peser deux «poids» aisément quantifiables et comparables. Le critère suppose un examen complet de plusieurs facteurs, de façon à garantir que les intérêts et les droits fondamentaux des personnes concernées sont dûment pris en considération. Il s'agit néanmoins d'un examen modulable qui peut varier en complexité et qui ne doit pas être inutilement contraignant. Les facteurs à prendre en considération dans cette mise en balance sont notamment:

- la nature et la source de l'intérêt légitime, et la question de savoir si le traitement des données est nécessaire à l'exercice d'un droit fondamental, est d'intérêt public à quelque autre égard ou bénéficie d'une reconnaissance dans la collectivité concernée;

- l'incidence sur les personnes concernées et leurs attentes raisonnables quant à ce qu'il adviendra de leurs données, ainsi que la nature des données et la façon dont elles sont traitées;

- les garanties supplémentaires qui pourraient limiter toute incidence injustifiée sur la personne concernée, comme la minimisation des données, les technologies renforçant la protection de la vie privée; une plus grande transparence, un droit général et inconditionnel de s'opposer au traitement et la portabilité des données.

Le groupe de travail «Article 29» recommande à l'avenir d'intégrer, dans la proposition de règlement, un considérant sur les facteurs-clés à examiner lors de l'application du critère de mise en balance. Il préconise aussi d'ajouter un considérant imposant au responsable du traitement, s'il y a lieu, de documenter son appréciation dans un souci de plus grande responsabilisation. Enfin, le groupe de travail «Article 29» serait favorable à l'ajout d'une disposition de fond exigeant des responsables du traitement qu'ils expliquent pourquoi ils considèrent que l'intérêt ou les droits et libertés fondamentaux des personnes concernées ne prévalent pas sur l'intérêt qu'ils poursuivent.

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30, paragraphe 1, point a), et paragraphe 3, de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

I. Introduction

Le présent avis analyse les critères légitimant le traitement des données énoncés à l'article 7 de la directive 95/46/CE[1] (ci-après la «directive»). Il se concentre, en particulier, sur l'intérêt légitime poursuivi par le responsable du traitement, au sens de l'article 7, point f).

Les critères énumérés à l'article 7 sont liés au principe plus large de «licéité» posé à l'article 6, paragraphe 1, point a), qui requiert que les données à caractère personnel soient traitées «loyalement et licitement».

L'article 7 n'autorise le traitement de données à caractère personnel que si au moins un des six fondements juridiques énumérés audit article s'applique. Concrètement, les données à caractère personnel seront traitées uniquement si: a) la personne concernée a indubitablement donné son consentement[2]; ou si – en résumé[3] – le traitement est nécessaire:

b) à l'exécution d'un contrat conclu avec la personne concernée;
c) au respect d'une obligation légale imposée au responsable du traitement;
d) à la sauvegarde de l'intérêt vital de la personne concernée;
e) à l'exécution d'une mission d'intérêt public; ou
f) à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, sous réserve du respect d'un critère supplémentaire de mise en balance avec les droits et l'intérêt de la personne concernée.

Ce dernier motif permet le traitement «nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou[4] les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1». Autrement dit, l'article 7, point f), autorise le traitement, sous réserve d'une mise en balance qui compare l'intérêt légitime poursuivi par le responsable du traitement – ou

[1] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281, 23.11.1995, p. 31).
[2] Voir l'avis 15/2011 du groupe de travail «Article 29» sur la protection des données concernant la définition du consentement, adopté le 13.7.2011 (WP 187).
[3] Ces dispositions sont examinées plus en détail à un stade ultérieur.
[4] *[Sans objet dans la version française, concerne une faute de frappe dans la version originale anglaise – voir le point III.3.2.]*

par le ou les tiers auxquels les données sont communiquées – avec l'intérêt ou les droits fondamentaux des personnes concernées[5].

Nécessité d'une approche plus cohérente et harmonisée en Europe

Il ressort des études réalisées par la Commission dans le cadre de la révision de la directive[6], ainsi que de la coopération et des échanges de vues entre les autorités nationales chargées de la protection des données, que l'absence d'une interprétation harmonisée de l'article 7, point f), de la directive a conduit à des applications divergentes dans les États membres. Notamment, bien que plusieurs États membres imposent une véritable mise en balance, l'article 7, point f), est parfois perçu à tort comme une «porte ouverte» légitimant tout traitement de données qui ne cadre avec aucun autre fondement juridique.

L'absence d'approche cohérente peut entraîner un manque de sécurité juridique et de prévisibilité, affaiblir la position des personnes concernées et aussi imposer des contraintes réglementaires inutiles aux entreprises et à d'autres organisations exerçant des activités transfrontières. De telles incohérences ont déjà donné lieu à des litiges portés devant la Cour de justice de l'Union européenne[7].

Il est donc particulièrement opportun, alors que le travail d'élaboration d'un nouveau règlement général sur la protection des données se poursuit, de veiller à ce que le sixième motif justifiant le traitement («l'intérêt légitime») et sa relation avec les autres motifs soient mieux compris. En particulier, dès lors que les droits fondamentaux des personnes concernées sont en jeu, il convient de prendre dûment en considération le respect de ces droits lors de l'application de chacun des six motifs, sans discrimination. L'article 7, point f), ne doit pas devenir un moyen commode d'échapper à l'obligation de se conformer au droit applicable en matière de protection des données.

C'est pourquoi, dans le cadre de son programme de travail 2012-2013, le groupe de travail «Article 29» sur la protection des données (ci-après le «groupe de travail») a décidé d'examiner attentivement la question et s'est engagé – en application de son programme de travail[8] – à rédiger le présent avis.

[5] La référence à l'article 1er, paragraphe 1, ne doit pas être interprétée comme une limitation de la portée de l'intérêt et des droits et libertés fondamentaux de la personne concernée. Cette référence sert plutôt à insister sur l'objectif général de la législation en matière de protection des données et de la directive elle-même. En effet, l'article 1er, paragraphe 1, mentionne non seulement la protection de la vie privée, mais aussi la protection des autres «libertés et droits fondamentaux des personnes physiques» dans leur ensemble, dont la vie privée n'est qu'une composante.

[6] Le 25 janvier 2012, la Commission européenne a adopté un paquet de mesures visant à réformer le cadre européen de la protection des données. Ce paquet comprend: i) une communication [COM(2012)9 final], ii) une proposition de règlement général en matière de protection des données (ci-après «le règlement proposé») [COM(2012)11 final], et iii) une proposition de directive sur la protection des données dans le secteur répressif [COM(2012)10 final]. L'analyse d'impact qui l'accompagne, comportant 10 annexes, est présentée dans un document de travail des services de la Commission [SEC(2012)72 final]. Voir, en particulier, l'étude intitulée «Evaluation of the implementation of the Data Protection Directive» (évaluation de la mise en œuvre de la directive sur la protection des données), qui constitue l'annexe 2 de l'analyse d'impact accompagnant le paquet de mesures de la Commission européenne visant à réformer le cadre européen de la protection des données.

[7] Voir page 8, dans la section II.1 «Bref historique», *«Mise en œuvre de la directive: l'arrêt ASNEF et FECEMD»*.

[8] Voir le programme de travail 2012-2013 du groupe de travail «Article 29», adopté le 1er février 2012 (WP 190).

Mettre en œuvre le cadre juridique actuel et préparer l'avenir

Le programme de travail a lui-même clairement défini deux objectifs: «assurer la mise en œuvre correcte du cadre juridique actuel» et aussi «préparer l'avenir».

En conséquence, le premier objectif du présent avis est d'assurer une compréhension commune du cadre juridique existant. Cet objectif s'inscrit dans le prolongement d'avis antérieurs portant sur d'autres dispositions-clés de la directive[9]. Dans un deuxième temps, en s'appuyant sur l'analyse proposée, l'avis formulera aussi des recommandations à prendre en considération lors du réexamen du cadre juridique sur la protection des données.

Structure de l'avis

Après un bref survol, au chapitre II, de l'histoire et du rôle de l'intérêt légitime et d'autres motifs légitimant le traitement, le chapitre III examinera et interprétera les dispositions concernées de la directive, en tenant compte de ce qui est constant dans leur application nationale. Cette analyse sera illustrée d'exemples pratiques tirés des expériences nationales. Elle étayera les recommandations formulées au chapitre IV tant en ce qui concerne l'application du cadre réglementaire actuel que dans le contexte de la révision de la directive.

II. Observations générales et considérations politiques

II.1. Bref historique

Cet aperçu examine plus particulièrement le développement des notions de licéité et de fondements juridiques justifiant le traitement, dont l'intérêt légitime. Il explique notamment comment la nécessité d'une base juridique a d'abord constitué une condition dans le contexte des dérogations au droit à la vie privée, avant de devenir une exigence distincte dans le contexte de la protection des données.

La Convention européenne des droits de l'homme («CEDH»)

L'article 8 de la Convention européenne des droits de l'homme, adoptée en 1950, consacre le droit au respect de la vie privée – à savoir le droit de toute personne au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il proscrit toute ingérence dans l'exercice de ce droit, sauf si elle est «prévue par la loi» et nécessaire «dans une société démocratique», afin de répondre à certains types d'intérêts publics impératifs, expressément énumérés.

L'article 8 de la CEDH traite en particulier de la protection de la vie privée et exige que toute ingérence soit justifiée. Cette approche repose sur une interdiction générale de l'ingérence dans l'exercice du droit à la vie privée et n'autorise des exceptions que dans des conditions strictement définies. En cas d'«ingérence dans la vie privée», une base juridique est requise, de même que la spécification d'une finalité légitime comme condition préalable permettant

[9] Comme l'avis 3/2013 sur la limitation de la finalité, adopté le 3.4.2013 (WP 203), l'avis 15/2011 sur la définition du consentement (cité en note de bas de page 2), l'avis 8/2010 sur le droit applicable, adopté le 16.12.2010 (WP 179) et l'avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», adopté le 16.2.2010 (WP 169).

d'apprécier la nécessité de l'ingérence. Cette approche explique que la CEDH ne dresse pas la liste des fondements juridiques possibles, mais se concentre sur la nécessité d'une base juridique et sur les conditions que cette base juridique doit remplir.

La Convention 108

La Convention 108[10] du Conseil de l'Europe, ouverte à la signature en 1981, introduit la notion distincte de protection des données à caractère personnel. L'idée sous-jacente, à l'époque, n'était pas que le traitement des données à caractère personnel devrait toujours être perçu comme une «*ingérence* dans la vie privée», mais plutôt que, pour *protéger* les droits et libertés fondamentaux de toute personne, et notamment son droit au respect de sa vie privée, le traitement des données à caractère personnel devrait toujours remplir certaines conditions. L'article 5 établit donc les principes fondamentaux du droit en matière de protection des données, notamment l'exigence selon laquelle les «données à caractère personnel faisant l'objet d'un traitement automatisé sont: a) obtenues et traitées loyalement et licitement». La Convention ne mentionnait toutefois pas de motifs détaillés justifiant le traitement[11].

Les lignes directrices de l'OCDE[12]

Élaborées parallèlement à la Convention 108 et adoptées en 1980, les lignes directrices de l'OCDE s'inscrivent dans des idées similaires de «licéité», bien que la notion soit exprimée de manière différente. Les lignes directrices ont été mises à jour en 2013, sans modification sensible du principe de licéité. Leur article 7 prévoit en particulier qu'«[i]l conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement». Le fondement juridique constitué par le consentement est ici expressément mentionné comme une possibilité, à laquelle il convient de recourir «le cas échéant». Cela suppose une appréciation des intérêts et des droits en jeu, ainsi qu'une évaluation de la mesure dans laquelle le traitement est intrusif. En ce sens, l'approche de l'OCDE présente certaines similitudes avec les critères – nettement plus élaborés – prévus par la directive 95/46/CE.

La directive 95/46/CE

Lors de son adoption, en 1995, la directive était inspirée des premiers instruments adoptés en matière de protection des données, notamment la Convention 108 et les lignes directrices de l'OCDE. L'expérience encore balbutiante acquise par certains États membres dans le domaine de la protection des données avait elle aussi été prise en considération.

Outre une exigence plus générale énoncée à son article 6, paragraphe 1, point a), selon laquelle les données à caractère personnel doivent être traitées «loyalement et licitement», la

[10] Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.
[11] Le projet de texte de la Convention modernisée adopté en assemblée plénière par le T-PD en novembre 2012 prévoit que le traitement des données peut être effectué sur la base du consentement de la personne concernée ou en vertu «d'un autre fondement légitime prévu par la loi», à l'instar de la Charte des droits fondamentaux de l'Union européenne mentionnée ci-après en page 9.
[12] Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, 11 juillet 2013.

directive ajoutait un ensemble spécifique de conditions supplémentaires, qui ne figuraient pas en tant que telles dans la Convention 108 ni dans les lignes directrices de l'OCDE: le traitement des données à caractère personnel doit être basé sur l'un des six fondements juridiques mentionnés à l'article 7.

Mise en œuvre de la directive: l'arrêt ASNEF et FECEMD[13]

Le rapport de la Commission intitulé «Evaluation of the implementation of the Data Protection Directive» (évaluation de la mise en œuvre de la directive sur la protection des données)[14] souligne que la mise en œuvre des dispositions de la directive dans le droit national s'est parfois révélée peu satisfaisante. Dans l'analyse technique de la transposition de la directive par les États membres[15], la Commission donne des précisions sur l'application de l'article 7. L'analyse explique que, si la législation de la plupart des États membres énonce les six fondements juridiques en termes relativement semblables à ceux utilisés dans la directive, la souplesse de ces principes a, dans les faits, conduit à des applications divergentes.

Dans ce contexte, il est particulièrement intéressant de relever que la Cour de justice a considéré, dans son arrêt ASNEF et FECEMD du 24 novembre 2011, que l'Espagne n'avait pas transposé correctement l'article 7, point f), de la directive en imposant – en l'absence du consentement de la personne concernée – que les données traitées figurent dans des sources accessibles au public. L'arrêt déclarait en outre que l'article 7, point f), a un effet direct. L'arrêt limite la marge d'appréciation dont disposent les États membres pour appliquer l'article 7, point f). En particulier, ils ne doivent pas franchir la ligne ténue qui sépare, d'un côté, la clarification et, de l'autre, la formulation d'exigences supplémentaires, qui reviendrait à modifier le champ d'application de l'article 7, point f).

L'arrêt, en ce qu'il précise que les États membres ne sont pas autorisés à imposer des restrictions et exigences unilatérales supplémentaires quant aux fondements juridiques du traitement licite des données dans leur droit national, a des conséquences non négligeables. Les juridictions nationales et autres organes concernés doivent interpréter les dispositions nationales à la lumière de cet arrêt et, si nécessaire, écarter les règles et les pratiques non conformes.

Cet arrêt montre combien il importe que les autorités nationales chargées de la protection des données et/ou les législateurs européens parviennent à une compréhension claire et commune de l'applicabilité de l'article 7, point f). Il convient pour ce faire d'adopter une approche équilibrée, qui ne restreint ni n'élargit indument le champ d'application de cette disposition.

La Charte des droits fondamentaux

Depuis l'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, la Charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») a «la même valeur juridique que les traités»[16]. Son article 8 consacre la protection des données à caractère personnel comme un droit fondamental, distinct du droit au respect de sa vie privée et familiale, qui fait l'objet de

[13] Arrêt de la Cour de justice du 24.11.2011 dans les affaires C-468/10 et C-469/10 (ASNEF et FECEMD).
[14] Voir l'annexe 2 de l'analyse d'impact accompagnant le paquet de mesures de la Commission européenne visant à réformer le cadre européen de protection des données, cité précédemment, en note de bas de page 6.
[15] Analyse et étude d'impact sur la mise en œuvre de la directive 95/46/CE dans les États membres. Voir http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

l'article 7. Il énonce l'exigence d'un fondement légitime pour le traitement. Concrètement, il prévoit que les données à caractère personnel doivent être traitées «sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi»[17]. Ces dispositions renforcent aussi bien l'importance du principe de licéité que la nécessité de justifier le traitement des données à caractère personnel par une base juridique adéquate.

La proposition de règlement sur la protection des données

Dans le contexte du processus de révision du cadre de la protection des données, la portée des motifs fondant la licéité du traitement prévus à l'article 7, et en particulier le champ d'application de l'article 7, point f), font actuellement l'objet de discussions.

L'article 6 du règlement proposé énumère les motifs justifiant un traitement licite des données à caractère personnel. À quelques exceptions près (qui seront décrites plus loin), les six motifs susceptibles d'être invoqués demeurent largement inchangés par rapport à ceux actuellement prévus par l'article 7 de la directive. La Commission a cependant proposé de fournir des orientations supplémentaires sous la forme d'actes délégués.

Il est intéressant de noter que, dans le cadre des travaux de la commission du Parlement européen concernée[18], les députés se sont efforcés de clarifier la notion d'intérêt légitime dans la proposition de règlement elle-même. Une liste de cas dans lesquels l'intérêt légitime poursuivi par le responsable du traitement des données prévaudrait en principe sur l'intérêt légitime et les droits et libertés fondamentaux de la personne concernée a été dressée, ainsi qu'une deuxième liste de cas où ce serait l'inverse. Ces listes – mentionnées dans les dispositions ou dans les considérants – apportent une contribution utile pour apprécier l'équilibre entre les droits et intérêts du responsable du traitement et ceux de la personne concernée. Elles sont prises en compte dans le présent avis[19].

[16] Voir l'article 6, paragraphe 1, du TUE.
[17] Voir l'article 8, paragraphe 2, de la Charte.
[18] Projet de rapport de la commission des libertés civiles, de la justice et des affaires intérieures (LIBE) sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)], daté du 16.1.2013 (ci-après le «projet de rapport de la commission LIBE»). Voir, en particulier, les amendements 101 et 102. Voir aussi les amendements adoptés par la commission le 21.10.2013 dans son rapport final (ci-après le «rapport final de la commission LIBE»).
[19] Voir la section III.3.1 et, en particulier, la liste à puces en pages 27 et 28 énumérant de façon non exhaustive certains des contextes où la question de l'intérêt légitime au sens de l'article 7, point f), est le plus communément susceptible de se poser.

II.2. Le rôle de la notion

L'intérêt légitime poursuivi par le responsable du traitement: le critère de la mise en balance en dernier recours?

L'article 7, point f), constitue la dernière option parmi les six motifs qui rendent licite le traitement des données à caractère personnel. Il impose un critère reposant sur une mise en balance: ce qui est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement (ou par les tiers) doit être mis en balance avec l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Le résultat de cette mise en balance détermine si l'article 7, point f), peut servir de fondement juridique au traitement.

Le caractère ouvert de cette disposition suscite maintes questions importantes concernant sa portée exacte et son application, qui seront analysées successivement dans le présent avis. Toutefois, ainsi qu'il est expliqué ci-après, cette option ne doit pas pour autant être perçue comme pouvant uniquement être utilisée avec parcimonie pour combler les lacunes «en dernier ressort» dans des situations rares et imprévues, ou comme une dernière chance si aucun autre motif ne s'applique. Elle ne doit pas non plus apparaître comme une option privilégiée, ni son utilisation être indument encouragée pour la simple raison qu'elle est considérée comme moins contraignante que les autres motifs.

Il se pourrait bien, au contraire, que l'article 7, point f), ait, de par sa nature même, un intérêt propre et qu'il ait un rôle très utile à jouer comme motif fondant la licéité du traitement, si plusieurs conditions déterminantes sont remplies.

Un recours approprié à l'article 7, point f), dans les circonstances appropriées et moyennant des garanties adéquates, permet aussi d'éviter un mauvais usage et une invocation excessive d'autres fondements juridiques.

Les cinq premiers motifs de l'article 7 reposent sur le consentement de la personne concernée, sur une disposition contractuelle, sur une obligation légale ou sur d'autres justifications expressément identifiées comme conférant au traitement sa légitimité. Quand le traitement est fondé sur l'un de ces cinq motifs, il est considéré a priori comme légitime et donc uniquement subordonné au respect d'autres dispositions du droit applicables. Autrement dit, l'équilibre entre les différents droits et intérêts en jeu – y compris ceux du responsable du traitement et de la personne concernée – est présumé atteint, à condition, bien sûr, que toutes les autres dispositions du droit en matière de protection des données soient respectées. L'article 7, point f), quant à lui, impose un critère *spécifique*, dans les cas qui ne cadrent pas avec les scénarios prédéfinis des motifs a) à e). Il assure que tout traitement, en dehors de ces scénarios, doive répondre aux exigences d'un critère de mise en balance, en tenant dûment compte des intérêts et droits fondamentaux de la personne concernée.

Ce critère peut, dans certains cas, mener à la conclusion que la balance penche en faveur des intérêts et droits fondamentaux des personnes concernées et que, par conséquent, le traitement ne peut être effectué. D'un autre côté, une évaluation appropriée de l'équilibre requis par l'article 7, point f), souvent assortie d'une possibilité de s'opposer au traitement, peut, dans d'autres cas, être préférable à l'invocation inappropriée, par exemple, du motif du «consentement» ou du caractère «nécessaire à l'exécution d'un contrat». Vu sous cet angle, l'article 7, point f), présente des garanties complémentaires – qui imposent des mesures appropriées – par rapport aux autres motifs prédéfinis. Il ne doit donc pas être considéré

comme «le maillon faible» ni comme une porte ouverte à la légitimation de tous les traitements de données qui ne relèvent d'aucun des autres fondements juridiques.

Le groupe de travail insiste sur le fait que son interprétation du champ d'application de l'article 7, point f), vise à proposer une approche équilibrée, qui garantisse aux responsables du traitement des données la flexibilité nécessaire dans les situations où les personnes concernées ne subissent pas une incidence injustifiée, tout en offrant à ces personnes une sécurité juridique et des garanties suffisantes pour empêcher tout abus de cette disposition ouverte.

II.3. Les notions liées

La relation de l'article 7, point f), avec d'autres motifs fondant la licéité du traitement

L'article 7 commence par le consentement, et continue en énumérant les autres motifs fondant la licéité du traitement, dont les contrats et obligations légales, pour en arriver progressivement au critère de l'intérêt légitime, qui figure en dernière position parmi les six motifs susceptibles d'être invoqués. L'ordre dans lequel les fondements juridiques sont présentés à l'article 7 a parfois été interprété comme une indication de l'importance respective des différents motifs. Cependant, comme le groupe de travail l'a déjà souligné dans son avis sur la notion de consentement[20], le libellé de la directive n'établit pas de distinction juridique entre les six motifs et n'indique aucunement qu'il existe entre eux une hiérarchie. Rien n'indique que l'article 7, point f), ne doive être appliqué que dans des cas exceptionnels, et aucun autre élément dans le libellé ne suggère que l'ordre spécifique des six fondements juridiques ait un quelconque effet juridiquement pertinent. Néanmoins, la signification précise de l'article 7, point f), et sa relation avec d'autres motifs fondant la licéité du traitement sont longtemps demeurées assez obscures.

Dans ce contexte, diverses approches, favorisées par la formulation ouverte de la directive, sont apparues au gré des diversités historiques et culturelles: certains États membres ont eu tendance à envisager l'article 7, point f), comme un motif d'ordre inférieur, destiné à combler les lacunes uniquement dans des cas exceptionnels où aucun des cinq autres motifs ne s'appliquerait[21]. D'autres États membres, à l'inverse, n'y voient qu'une possibilité parmi six autres, qui n'est ni plus ni moins importante que les autres options et qui peut s'appliquer à des situations très nombreuses et variées, pour autant que les conditions nécessaires soient remplies.

Compte tenu de ces divergences, et également de l'arrêt ASNEF et FECEMD, il importe de clarifier la relation de «l'intérêt légitime» avec les autres motifs fondant la licéité du traitement – c'est-à-dire, par exemple, avec le consentement, les clauses contractuelles, les missions d'intérêt public – ainsi qu'avec le droit d'opposition de la personne concernée. On pourrait ainsi mieux définir le rôle et la fonction du motif de l'intérêt légitime et donc apporter plus de sécurité juridique.

[20] Voir la note de bas de page 2 ci-dessus.
[21] Il est aussi à noter que le projet de rapport de la commission LIBE proposait, par son amendement 100, de séparer l'article 7, point f), des autres fondements juridiques et aussi d'ajouter des exigences supplémentaires au cas où ce fondement juridique est invoqué, notamment un renforcement de la transparence et de la responsabilité, comme on le verra plus tard.

Il faut aussi relever que le motif de l'intérêt légitime, à l'instar des autres motifs hormis celui du consentement, comporte un critère de «nécessité» qui doit être rempli. Cela limite strictement le contexte dans lequel chacun de ces motifs peut s'appliquer. La Cour de justice de l'Union européenne a considéré que la «nécessité» constitue une notion autonome du droit communautaire[22]. La Cour européenne des droits de l'homme a, elle aussi, donné des orientations utiles[23].

De surcroît, le fait d'avoir un fondement juridique approprié ne dispense pas le responsable du traitement des données de respecter les obligations de loyauté, de licéité, de nécessité et de proportionnalité, mais aussi de qualité des données, qui lui incombent en vertu de l'article 6. Par exemple, même si le traitement des données à caractère personnel est justifié par l'intérêt légitime ou par l'exécution d'un contrat, cela n'autorise pas une collecte de données excessive au regard de la finalité spécifiée.

L'intérêt légitime et les autres motifs visés à l'article 7 sont des motifs alternatifs et il suffit donc qu'un seul d'entre eux s'applique. Cependant, ils viennent s'ajouter non seulement aux exigences de l'article 6, mais aussi à tous les autres principes et obligations de protection des données qui peuvent être applicables.

Autres critères de mise en balance

L'article 7, point f), n'est pas le seul critère de mise en balance prévu dans la directive. Par exemple, l'article 9 suppose un équilibre entre le droit à la protection des données à caractère personnel et la liberté d'expression. Cet article permet aux États membres d'accorder des exemptions et dérogations pour les traitements des données à caractère personnel «effectués aux seules fins de journalisme ou d'expression artistique ou littéraire» si elles sont «nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression».

De plus, de nombreuses autres dispositions de la directive requièrent aussi une analyse au cas par cas, une mise en balance des intérêts et des droits en jeu et une certaine souplesse dans l'appréciation de multiples facteurs. Il s'agit notamment des dispositions relatives à la nécessité, à la proportionnalité et à la limitation de la finalité, aux exceptions visées à l'article 13, et à la recherche scientifique, pour n'en citer que quelques-unes.

Il semble effectivement que la directive ait été conçue pour laisser place à l'interprétation et à la mise en balance des intérêts. L'intention était bien sûr, au moins en partie, de donner aux États membres une marge de manœuvre plus grande pour la transposition dans le droit national. Cependant, la nécessité d'une certaine flexibilité découle, en outre, de la nature

[22] Arrêt de la Cour de justice du 16 décembre 2008, dans l'affaire C-524/06 (Heinz Huber/Bundesrepublik Deutschland), point 52: «Dès lors, eu égard à l'objectif consistant à assurer un niveau de protection équivalent dans tous les États membres, la notion de nécessité telle qu'elle résulte de l'article 7, sous e), de la directive 95/46, qui vise à délimiter précisément une des hypothèses dans lesquelles le traitement de données à caractère personnel est licite, ne saurait avoir un contenu variable en fonction des États membres. Partant, il s'agit d'une notion autonome du droit communautaire qui doit recevoir une interprétation de nature à répondre pleinement à l'objet de cette directive tel que défini à l'article 1er, paragraphe 1, de celle-ci.»

[23] Arrêt de la Cour européenne des droits de l'homme du 25 mars 1983, dans l'affaire Silver et autres/Royaume-Uni, au point 97 à propos de l'expression «nécessaire dans une société démocratique»: «l'adjectif "nécessaire" n'est pas synonyme d'"indispensable", mais n'a pas non plus la souplesse de termes tels qu'"admissible", "normal", "utile", "raisonnable" ou "opportun" […].»

même du droit à la protection des données à caractère personnel et du droit au respect de la vie privée. En effet, ces deux droits, de même que la plupart (mais non la totalité) des autres droits fondamentaux, sont considérés comme des droits humains relatifs, ou qualifiés[24]. Les droits de ce type doivent toujours être interprétés dans leur contexte. Pour autant que des garanties appropriées soient prévues, ils peuvent être mis en balance avec les droits d'autrui. Dans certaines situations – toujours sous réserve de garanties appropriées – ils peuvent aussi être soumis à des restrictions pour des raisons d'intérêt public.

II.4. Contexte et conséquences stratégiques

Garantir la légitimité mais aussi la flexibilité: les moyens de préciser l'article 7, point f)

Le libellé actuel de l'article 7, point f), de la directive est ouvert. Il s'ensuit qu'il peut servir de fondement dans un large éventail de situations, du moment que ses exigences sont satisfaites, et notamment le critère de mise en balance. Cependant, une telle flexibilité peut aussi avoir des conséquences négatives. Des orientations complémentaires seraient donc utiles pour éviter une application incohérente de la directive dans les États membres ou un manque de sécurité juridique.

La Commission prévoit de telles orientations dans la proposition de règlement, sous la forme d'actes délégués. D'autres options consistent notamment à apporter des éclaircissements et introduire des dispositions détaillées dans le texte du règlement proposé lui-même[25] et/ou à confier au comité européen de la protection des données le soin de formuler des orientations complémentaires dans ce domaine.

Chacune de ces options a des avantages et des inconvénients. Si l'appréciation devait avoir lieu au cas par cas, sans autres orientations, cela risquerait d'entraîner une application incohérente et un manque de prévisibilité, comme c'était le cas précédemment.

D'un autre côté, le fait de prévoir, dans le texte même du règlement proposé, des listes détaillées et exhaustives de situations dans lesquelles l'intérêt légitime poursuivi par le responsable du traitement prévaut en règle générale sur les droits fondamentaux de la personne concernée, ou inversement, pourrait induire en erreur ou être inutilement coercitif, ou les deux à la fois.

Ces approches pourraient néanmoins inspirer une solution équilibrée, apportant certaines précisions complémentaires dans le règlement proposé lui-même et d'autres orientations dans des actes délégués ou dans les lignes directrices du comité européen de la protection des données[26].

[24] Il n'existe que peu de droits humains qui ne puissent être mis en balance avec les droits d'autrui ou avec l'intérêt collectif. On les appelle les droits absolus. Ces droits ne peuvent jamais être limités ni restreints, quelles que soient les circonstances – même en cas de guerre ou d'état d'urgence. Le droit de n'être pas soumis à la torture ni à un traitement inhumain ou dégradant en est un exemple. Il n'est jamais admissible de torturer quelqu'un ou de le traiter d'une manière inhumaine ou dégradante, quelles que soient les circonstances. Les exemples de droits humains non absolus comprennent notamment le droit au respect de la vie privée et familiale, le droit à la liberté d'expression et le droit à la liberté de pensée, de conscience et de religion.

[25] Voir la section II.1 «Bref historique», *«La proposition de règlement sur la protection des données»*, en page 9.

[26] En ce qui concerne les actes délégués et les orientations du comité européen de la protection des données, le groupe de travail «Article 29» a fait part, dans son avis 08/2012 apportant des contributions supplémentaires au

L'analyse présentée au chapitre III vise à jeter les bases d'une telle approche, ni trop générale au point d'en perdre toute signification, ni trop précise au point d'en devenir exagérément rigide.

III. Analyse des dispositions

III.1. Aperçu général de l'article 7

L'article 7 dispose que le traitement de données à caractère personnel ne peut être effectué que si au moins un des six motifs juridiques énumérés à cet article s'applique. Avant d'analyser chacun de ces motifs, la section III.1 donne un aperçu général de l'article 7 et de sa relation avec l'article 8, qui porte sur les catégories particulières de données.

III.1.1. Consentement ou «nécessaire à...»

Une distinction peut être établie entre le cas où le traitement des données à caractère personnel se fonde sur le consentement indubitable de la personne concernée [article 7, point a)] et les cinq autres cas [article 7, points b) à f)]. En résumé, ces derniers décrivent des scénarios où le traitement peut se révéler nécessaire dans un contexte spécifique, comme l'exécution d'un contrat conclu avec la personne concernée, le respect d'une obligation légale imposée au responsable du traitement, etc.

Dans le premier cas, visé à l'article 7, point a), ce sont les personnes concernées elles-mêmes qui autorisent le traitement de leurs données à caractère personnel. Il leur appartient de décider si elles permettent que leurs données soient traitées. Le consentement n'élimine pas pour autant la nécessité de respecter les principes énoncés à l'article 6[27]. De plus, le consentement doit encore remplir certaines conditions essentielles pour être légitime, comme l'explique l'avis 15/2011 du groupe de travail[28]. Dès lors que le traitement des données de l'utilisateur est, en définitive, laissé à sa discrétion, tout dépend de la validité et de la portée du consentement de la personne concernée.

Autrement dit, le premier motif, mentionné à l'article 7, point a), a trait à l'autodétermination de la personne concernée comme fondement de la légitimité. Tous les autres motifs, en revanche, autorisent le traitement – moyennant des garanties et des mesures définies – dans des situations où, indépendamment du consentement, il est approprié et nécessaire de traiter les données dans un certain contexte pour servir un intérêt légitime spécifique.

débat sur la réforme de la protection des données, adopté le 5.10.2012 (WP 199), de sa nette préférence pour les orientations (voir p. 14 et 15).

[27] Arrêt de la Cour suprême des Pays-Bas du 9 septembre 2011 dans l'affaire ECLI:NL:HR:2011:BQ8097, point 3.3, e), à propos du principe de proportionnalité. Voir aussi la page 8 de l'avis 15/2011 du groupe de travail «Article 29», cité en note de bas de page 2, ci-dessus: «[...] l'obtention d'un consentement n'annule pas les obligations imposées au responsable du traitement par l'article 6 en termes d'équité, de nécessité, de proportionnalité ainsi que de qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de l'utilisateur, cela ne justifie pas la collecte de données excessives au regard d'une fin particulière.»

[28] Voir les pages 12 à 28 de l'avis 15/2011, cité en note 2 ci-dessus.

Les points b), c), d) et e) spécifient chacun un critère légitimant le traitement:

b) l'exécution d'un contrat conclu avec la personne concernée;
c) le respect d'une obligation légale imposée au responsable du traitement;
d) la sauvegarde de l'intérêt vital de la personne concernée;
e) l'exécution d'une mission d'intérêt public.

Le point f) est moins précis et renvoie, plus généralement, à un (quelconque) intérêt légitime poursuivi par le responsable du traitement (dans n'importe quel contexte). Cette disposition générale est cependant expressément subordonnée à un critère supplémentaire de mise en balance, qui vise à protéger l'intérêt et les droits des personnes concernées, comme on le verra à la section III.2.

Dans tous les cas, c'est au responsable du traitement des données qu'il revient initialement d'apprécier si les critères énoncés à l'article 7, points a) à f), sont remplis, sous réserve du respect du droit applicable et des orientations relatives à la façon dont ce droit doit être appliqué. Ensuite, la légitimité du traitement peut faire l'objet d'une autre évaluation, et éventuellement être contestée, par les personnes concernées, par d'autres parties prenantes, par les autorités chargées de la protection des données, et en définitive la question peut être tranchée par les tribunaux.

Pour compléter ce bref aperçu, il convient d'indiquer que, comme on le verra à la section III.3.6, au moins dans les cas visés aux points e) et f), la personne concernée peut exercer son droit d'opposition, ainsi que le prévoit l'article 14[29]. Cela donnera lieu à une nouvelle évaluation des intérêts en jeu ou, si le traitement des données à caractère personnel est envisagé à des fins de prospection [article 14, point b)], cela contraindra le responsable du traitement à y mettre un terme, sans évaluation complémentaire.

III.1.2. Relation avec l'article 8

L'article 8 de la directive régit de façon plus détaillée le traitement de certaines catégories particulières de données à caractère personnel. Il concerne plus spécialement le traitement des données «qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle» (article 8, paragraphe 1), et les données «relatives aux infractions [ou] aux condamnations pénales» (article 8, paragraphe 5).

Le traitement de ces données est en principe interdit, sous réserve de certaines exceptions. L'article 8, paragraphe 2, prévoit plusieurs exceptions à cette interdiction, aux points a) à e). L'article 8, paragraphes 3 et 4, prévoit d'autres exceptions. Certaines de ces dispositions sont analogues – mais non identiques – à celles énoncées à l'article 7, points a) à f).

[29] Selon l'article 14, point a), ce droit s'applique «sauf en cas de disposition contraire du droit national». En Suède, par exemple, le droit national ne reconnaît pas la possibilité de s'opposer à un traitement fondé sur l'article 7, point e).

Les conditions spécifiques de l'article 8, ainsi que le fait que certains des motifs énumérés à l'article 7 ressemblent aux conditions énoncées à l'article 8, conduisent à s'interroger sur la relation entre les deux dispositions.

Si l'article 8 est conçu comme une *lex specialis*, il convient d'examiner s'il exclut complètement l'applicabilité de l'article 7. Dans l'affirmative, cela signifierait que des catégories particulières de données à caractère personnel peuvent être traitées sans que les critères de l'article 7 doivent être satisfaits, pour autant qu'une des exceptions de l'article 8 s'applique. Il est cependant également possible que la relation soit plus complexe et que les articles 7 et 8 doivent être appliqués cumulativement[30].

Quoi qu'il en soit, il est clair que l'objectif de la mesure est d'assurer une protection supplémentaire pour des catégories particulières de données. Par conséquent, le résultat final de l'analyse devrait être tout aussi clair: l'application de l'article 8, en soi ou cumulé avec l'article 7, vise à garantir un niveau de protection plus élevé de certaines catégories particulières de données.

Dans la pratique, bien que, dans certains cas, l'article 8 énonce des exigences plus strictes – comme le consentement «explicite» requis à l'article 8, paragraphe 2, point a), par rapport au consentement «indubitablement donné» prévu à l'article 7 – il n'en va pas ainsi de toutes les dispositions. Certaines exceptions prévues par l'article 8 ne semblent pas équivalentes ou plus strictes que les motifs visés à l'article 7. Il serait inapproprié de conclure, par exemple, que le fait que des catégories particulières de données ont été manifestement rendues publiques par quelqu'un, comme l'envisage l'article 8, paragraphe 2, point e), serait – toujours et en soi – une condition suffisante pour autoriser tout type de traitement des données, sans mettre en balance les intérêts et les droits en jeu, comme l'exige l'article 7, point f)[31].

Dans certaines situations, le fait que le responsable du traitement des données soit un parti politique lèverait aussi l'interdiction du traitement de catégories particulières de données selon l'article 8, paragraphe 2, point d). Cela ne veut pas dire pour autant que tout traitement entrant dans le champ d'application de cette disposition soit nécessairement licite. Cette question doit être appréciée séparément et le responsable du traitement devra éventuellement démontrer, par exemple, que le traitement des données est nécessaire à l'exécution d'un contrat [article 7, point b)], ou que son intérêt légitime prévaut, conformément à l'article 7, point f). Dans ce dernier cas, le critère de mise en balance prévu par l'article 7, point f), doit être appliqué après l'appréciation du respect des exigences de l'article 8 par le responsable du traitement des données.

De même, le simple fait que «le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la

[30] Puisque l'article 8 se présente comme *une interdiction avec des exceptions*, celles-ci peuvent être perçues comme des exigences, qui limitent seulement la portée de l'interdiction mais ne constituent pas, en tant que telles, un fondement juridique suffisant pour justifier le traitement. Selon cette lecture, l'applicabilité des exceptions de l'article 8 n'exclut pas l'applicabilité des exigences de l'article 7, et les unes comme les autres doivent, le cas échéant, s'appliquer cumulativement.

[31] De plus, l'article 8, paragraphe 2, point e), ne saurait être interprété a contrario comme signifiant que, si les données rendues publiques par la personne concernée ne sont pas des données sensibles, elles peuvent être traitées sans satisfaire à d'autres conditions. Les données accessibles au public restent des données à caractère personnel soumises aux exigences de la protection des données, notamment au respect de l'article 7, qu'il s'agisse ou non de données sensibles.

gestion de services de santé» et l'obligation de secret qui s'applique au traitement de ces données – comme indiqué à l'article 8, paragraphe 3 – impliquent qu'un tel traitement de données sensibles est *exempté de l'interdiction* visée à l'article 8, paragraphe 1. Ce n'est pourtant pas nécessairement suffisant pour garantir aussi la licéité au titre de l'article 7, et un fondement juridique comme l'exécution d'un contrat conclu avec le patient conformément à l'article 7, point b), une obligation légale conformément à l'article 7, point c), l'exécution d'une mission d'intérêt public conformément à l'article 7, point e), ou l'appréciation du critère énoncé à l'article 7, point f), sera requis.

En conclusion, le groupe de travail considère qu'il faut analyser au cas par cas si l'article 8 prévoit, en soi, des conditions plus strictes et suffisantes[32], ou s'il convient d'appliquer cumulativement les articles 8 et 7 pour garantir une protection complète des personnes concernées. Le résultat de l'examen ne peut en aucun cas aboutir à une moindre protection des catégories particulières de données[33].

Il s'ensuit aussi que le responsable du traitement qui s'occupe de catégories particulières de données ne peut jamais invoquer *uniquement* un fondement juridique relevant de l'article 7 pour légitimer une activité de traitement des données. Le cas échéant, l'article 7 ne *prévaudra* pas, mais s'appliquera toujours de manière *cumulative* avec l'article 8, afin que toutes les garanties et les mesures pertinentes soient respectées. Cela vaudra d'autant plus dans les cas où les États membres décident d'ajouter des exemptions à celles énoncées à l'article 8, ainsi que le prévoit l'article 8, paragraphe 4.

III.2. Article 7, points a) à e)

La présente section III.2 donne un bref aperçu de chacun des fondements juridiques mentionnés à l'article 7, points a) à e), de la directive, avant d'examiner plus particulièrement, à la section III.3, l'article 7, point f). Cette analyse mettra aussi en lumière certaines des corrélations les plus courantes entre ces fondements juridiques, faisant intervenir par exemple un «contrat», une «obligation légale» et un «intérêt légitime», selon le contexte particulier et les circonstances.

III.2.1. Consentement

Le consentement, en tant que fondement juridique, a été analysé dans l'avis 15/2011 du groupe de travail sur la définition du consentement. L'avis concluait essentiellement que le consentement n'est qu'un fondement juridique parmi d'autres, plutôt que le fondement principal légitimant le traitement de données à caractère personnel. Il joue un rôle important mais n'exclut pas la possibilité que, compte tenu du contexte, d'autres fondements juridiques puissent être jugés plus appropriés par le responsable du traitement ou par la personne concernée. S'il est utilisé à bon escient, le consentement est un instrument qui permet à la

[32] Voir l'analyse présentée dans l'avis «AMA» du groupe de travail «Article 29», point 3.3, qui prend en considération aussi bien l'article 7 que l'article 8 de la directive: Deuxième avis 4/2009 sur le standard international pour la protection des renseignements personnels de l'Agence mondiale antidopage (AMA), sur les dispositions du code de l'AMA s'y rapportant et sur d'autres questions relatives à la vie privée dans le cadre de la lutte contre le dopage dans le sport par l'AMA et les organisations (nationales) antidopage, adopté le 6.4.2009 (WP 162).

[33] Il va sans dire que, dans le cas de l'application de l'article 8 également, le respect des autres dispositions de la directive, y compris son article 6, doit être assuré.

personne concernée de contrôler le traitement de ses données. Au contraire, s'il est mal utilisé, le contrôle de la personne concernée devient illusoire et le consentement constitue alors une base inappropriée pour le traitement de données.

Parmi ses recommandations, le groupe de travail soulignait la nécessité de clarifier le sens de la notion de «consentement indubitable»: «[c]ette clarification devrait insister sur le fait qu'un consentement indubitable impose de recourir à des mécanismes qui ne laissent aucun doute sur l'intention de la personne concernée de consentir au traitement. Dans le même temps, il conviendrait d'expliquer que l'utilisation d'options par défaut, que la personne concernée doit modifier pour refuser le traitement (consentement fondé sur le silence), ne constitue pas, en soi, un consentement indubitable. Cette observation vaut tout particulièrement dans l'environnement en ligne[34].» Il proposait aussi d'exiger des responsables du traitement qu'ils mettent en place des mécanismes pour démontrer le consentement (dans le cadre de l'obligation générale de rendre compte) et invitait le législateur à ajouter une exigence explicite concernant la qualité et l'accessibilité des informations servant de base au consentement.

III.2.2. Contrat

L'article 7, point b), constitue un fondement juridique dans les situations où le traitement «est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci». Cela recouvre deux scénarios différents.

i) Dans le premier cas de figure, la disposition s'applique aux situations dans lesquelles le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie. Il peut s'agir, par exemple, du traitement de son adresse pour que des produits achetés en ligne puissent être livrés, ou du traitement des informations figurant sur une carte de crédit afin d'effectuer une transaction. Dans le contexte des relations de travail, ce motif peut autoriser, par exemple, le traitement des informations relatives aux salaires et des coordonnées de comptes bancaires pour que les salariés puissent être payés.

   La disposition doit être interprétée de façon restrictive et ne couvre pas les situations dans lesquelles le traitement n'est pas véritablement *nécessaire* à l'exécution d'un contrat, mais plutôt imposé unilatéralement à la personne concernée par le responsable du traitement. Le fait qu'un certain traitement de données soit couvert par un contrat ne signifie pas non plus automatiquement que le traitement soit nécessaire à son exécution. Par exemple, l'article 7, point b), ne peut pas servir de fondement juridique pour établir un profil des goûts et du mode de vie de l'utilisateur à partir de son historique de navigation sur un site internet et des articles achetés. En effet, le responsable du traitement des données n'a pas été chargé, dans le contrat, d'établir un profil mais de fournir des produits et des services, par exemple. Même si ces activités de traitement sont expressément mentionnées en petits caractères dans le contrat, elles n'en deviennent pas pour autant «nécessaires» à l'exécution de ce dernier.

[34] Voir la page 41 de l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement.

Il existe ici un lien évident entre l'appréciation de la nécessité et le respect du principe de limitation de la finalité. Il importe de déterminer la raison d'être exacte du contrat, c'est-à-dire sa substance et son objectif fondamental, car c'est ce qui permettra de vérifier si le traitement des données est nécessaire à l'exécution du contrat.

Dans certaines situations limites, on peut être amené à s'interroger ou à recueillir des éléments complémentaires plus précis, afin de déterminer si le traitement est nécessaire à l'exécution du contrat. Ainsi, la constitution d'une base de données de contact à usage interne contenant les noms, les adresses professionnelles, les numéros de téléphone et les adresses de courrier électronique de tous les salariés d'une entreprise, destinée à faciliter les échanges d'informations entre collègues, peut dans certains cas être considérée comme nécessaire à l'exécution d'un contrat au titre de l'article 7, point b), mais elle peut aussi être licite en vertu de l'article 7, point f), s'il est démontré que l'intérêt du responsable du traitement prévaut et si toutes les mesures appropriées ont été prises, par exemple, en consultant dûment les représentants du personnel.

D'autres cas, comme la surveillance électronique de l'utilisation de l'internet, du courriel ou du téléphone par les salariés, ou la vidéosurveillance de ces derniers, constituent plus manifestement un traitement qui risque d'aller au-delà de ce qui est nécessaire à l'exécution d'un contrat de travail, bien que cela puisse, ici aussi, dépendre de la nature de l'emploi. La prévention de la fraude – qui peut inclure, entre autres, la surveillance et l'établissement de profils des clients – est un autre aspect généralement susceptible d'être considéré comme allant au-delà de ce qui est nécessaire à l'exécution d'un contrat. Un tel traitement pourrait tout de même être légitime en vertu d'un autre motif mentionné à l'article 7, par exemple, selon les circonstances, le consentement, une obligation légale ou l'intérêt légitime du responsable du traitement [article 7, point a, c) ou f)][35]. Dans ce dernier cas, le traitement devrait être subordonné à des garanties et mesures supplémentaires en vue de protéger l'intérêt ou les droits et libertés des personnes concernées.

L'article 7, point b), s'applique uniquement à ce qui est nécessaire à *l'exécution* d'un contrat. Il ne couvre pas les diverses actions déclenchées par le non-respect du contrat ni quelque autre incident dans son exécution. Tant que le traitement relève de l'exécution normale d'un contrat, il peut entrer dans le champ d'application de l'article 7, point b). S'il survient un incident qui donne lieu à un conflit, le traitement des données peut prendre un cours différent. Le traitement des informations de base relatives à la personne concernée, comme le nom, l'adresse et la référence à des obligations contractuelles en souffrance, pour l'envoi de rappels, devrait encore être considéré comme relevant du traitement de données nécessaire à l'exécution d'un

[35] Un autre exemple de fondements juridiques multiples est présenté dans l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement (cité en note de bas de page 2). Pour l'achat d'une voiture, le responsable du traitement peut être habilité à traiter des données à caractère personnel à différentes fins et sur la base de différents motifs:
- les données sont nécessaires à l'achat de la voiture: article 7, point b);
- pour traiter les documents du véhicule: article 7, point c);
- pour les services de gestion de la clientèle (par exemple, pour l'entretien du véhicule dans différentes entreprises du même groupe au sein de l'UE): article 7, point f);
- pour transférer les données à des tiers aux fins de leurs propres activités de commercialisation: article 7, point a).

contrat. Quant aux traitements plus élaborés de données, dans lesquels des tiers peuvent ou non intervenir, comme le recouvrement de créances, ou une action en justice à l'encontre d'un client en défaut de paiement, on pourrait faire valoir qu'un tel traitement ne relève plus de l'exécution «normale» du contrat et n'entre donc plus dans le champ d'application de l'article 7, point b). Cela ne rendrait cependant pas le traitement illégitime pour autant, car le responsable du traitement a un intérêt légitime à former un recours pour faire respecter ses droits contractuels. D'autres fondements juridiques, comme l'article 7, point f), pourraient être invoqués, sous réserve de garanties et de mesures appropriées, et du respect du critère de mise en balance[36].

ii) Dans le second cas de figure, l'article 7, point b), couvre aussi le traitement de données qui a lieu *avant* la conclusion d'un contrat. Il peut donc s'appliquer aux relations précontractuelles, pour autant que les démarches soient accomplies à la demande de la personne concernée, plutôt qu'à l'initiative du responsable du traitement ou d'un tiers. Par exemple, si une personne demande à un détaillant de lui faire une offre de prix pour un produit, le traitement de données effectué à cette fin, tel que la conservation, pour une durée limitée, de l'adresse et des informations à propos de ce qui est demandé, pourra s'appuyer sur ce fondement juridique. De même, si quelqu'un demande un devis à un assureur pour sa voiture, l'assureur est en droit de traiter les données nécessaires, par exemple, la marque et l'âge de la voiture, ainsi que d'autres données pertinentes et proportionnées, afin d'établir le devis.

En revanche, des vérifications détaillées comme, par exemple, le traitement de données d'examens médicaux par une compagnie d'assurances avant de proposer une assurance maladie ou une assurance vie ne seraient pas considérées comme une étape nécessaire accomplie à la demande de la personne concernée. Les vérifications de la cote de crédit avant d'accorder un prêt ne sont pas non plus effectuées *à la demande* de la personne concernée conformément à l'article 7, point b), mais plutôt au titre de l'article 7, point f), ou de l'article 7, point c), en vertu d'une obligation légale faite aux banques de consulter une liste officielle de débiteurs enregistrés.

Le traitement à des fins de prospection directe sur l'initiative du détaillant/responsable du traitement ne pourra pas non plus s'appuyer sur ce motif. Dans certains cas, l'article 7, point f), pourrait se substituer à l'article 7, point b), en tant que fondement juridique, sous réserve de garanties et de mesures appropriées, et du respect du critère de mise en balance. Dans d'autres circonstances, notamment en cas d'établissement de profils détaillés, de partage de données, de prospection directe en ligne ou de publicité comportementale, il convient d'examiner si la personne concernée a donné son consentement, conformément à l'article 7, point a), comme le montre l'analyse présentée plus bas[37].

III.2.3. Obligation légale

L'article 7, point c), constitue un fondement juridique dans les situations où le traitement «est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est

[36] Pour les catégories particulières de données, il convient peut-être aussi être de prendre en compte l'article 8, paragraphe 1, point e): «nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice».
[37] Voir la section III.3.6, point b), sous l'intitulé: «Illustration: l'évolution de l'approche de la prospection directe», aux pages 51 et 52.

soumis». Cela peut être le cas, par exemple, lorsque les employeurs doivent communiquer des données relatives aux rémunérations de leurs salariés à la sécurité sociale ou à l'administration fiscale, ou lorsque les institutions financières sont tenues de signaler certaines opérations suspectes aux autorités compétentes en vertu de règles visant à lutter contre le blanchiment d'argent. Il pourrait s'agir aussi d'une obligation à laquelle une autorité publique est soumise, puisque rien ne limite l'application de l'article 7, point c), au secteur privé ou public. Cette disposition s'appliquerait, par exemple, à la collecte de données par une autorité locale aux fins du traitement des amendes pour stationnement irrégulier.

L'article 7, point c), présente des similitudes avec l'article 7, point e), dans la mesure où une mission d'intérêt public repose souvent sur une disposition légale, ou en découle. Le champ d'application de l'article 7, point c), est néanmoins strictement délimité.

Pour que l'article 7, point c), puisse s'appliquer, l'obligation doit être imposée par la loi (et non, par exemple, par une cause contractuelle). La loi doit remplir toutes les conditions requises pour rendre l'obligation valable et contraignante, et doit aussi être conforme au droit applicable en matière de protection des données, notamment aux principes de nécessité, de proportionnalité[38] et de limitation de la finalité.

Il importe également de souligner que l'article 7, point c), se rapporte aux lois de l'Union européenne ou d'un État membre. Les obligations imposées par les lois de pays tiers (comme, par exemple, l'obligation de mettre en place des mécanismes de dénonciation des dysfonctionnements, instaurée en 2002 par la loi Sarbanes-Oxley aux États-Unis) ne relèvent pas de ce motif. Pour être valable, une obligation légale imposée par un pays tiers devrait être officiellement reconnue et intégrée dans l'ordre juridique de l'État membre concerné, par exemple sous la forme d'une convention internationale[39]. En revanche, la nécessité de satisfaire à une obligation étrangère peut représenter un intérêt légitime poursuivi par le responsable du traitement, mais uniquement sous réserve de respecter le critère de mise en balance de l'article 7, point f), et pour autant que des garanties adéquates aient été mises en place, comme celles approuvées par l'autorité compétente chargée de la protection des données.

Le responsable du traitement ne doit pas avoir le choix de se conformer ou non à l'obligation. Les engagements volontaires unilatéraux et les partenariats public-privé qui supposent le traitement de données au-delà de ce qui est requis par la loi n'entrent donc pas dans le champ d'application de l'article 7, point c). Par exemple, si un fournisseur de services internet décide – sans y être contraint par une obligation légale claire et précise – de surveiller ses utilisateurs afin de lutter contre le téléchargement illégal, l'article 7, point c), ne pourra pas être invoqué comme fondement juridique approprié à cet effet.

[38] Voir aussi l'avis 01/2014 du groupe de travail «Article 29» sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif, adopté le 27. 2.2014 (WP 211).

[39] Voir, à ce propos, la section 4.2.2 de l'avis 10/2006 groupe de travail «Article 29» sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), adopté le 20.11.2006 (WP 128) et l'avis 1/2006 du groupe de travail «Article 29» relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, adopté le 1.2.2006 (WP 117).

De surcroît, l'obligation légale elle-même doit être suffisamment claire à propos du traitement de données à caractère personnel qu'elle requiert. En conséquence, l'article 7, point c), s'applique sur la base de dispositions juridiques mentionnant explicitement la nature et l'objet du traitement. Le responsable du traitement ne devrait pas avoir de marge d'appréciation injustifiée quant à la façon de se conformer à l'obligation légale.

La législation peut, dans certains cas, définir seulement un objectif général, tandis que des obligations plus spécifiques sont imposées à un niveau différent, par exemple, dans le droit dérivé ou dans une décision contraignante d'une autorité publique dans un cas concret. Cela peut aussi déboucher sur des obligations légales au sens de l'article 7, point c), pour autant que la nature et l'objet du traitement soient bien définis et qu'il existe une base juridique adéquate.

Il en va toutefois autrement si une autorité réglementaire formule uniquement des lignes directrices générales et énonce les conditions auxquelles elle pourrait envisager de faire usage de ses pouvoirs d'exécution (par exemple, des orientations réglementaires à l'intention des institutions financières portant sur certaines normes de vigilance). Dans de tels cas, les activités de traitement doivent être appréciées au regard de l'article 7, point f), et ne peuvent être considérées comme légitimes que sous réserve du respect du critère supplémentaire de mise en balance[40].

D'une manière générale, il convient de noter que certaines activités de traitement peuvent sembler relever, à peu de chose près, de l'article 7, point c), ou de l'article 7, point b), sans remplir pleinement les critères pour que ces motifs puissent s'appliquer. Cela ne veut pas dire qu'un tel traitement est toujours nécessairement illicite: il peut parfois être légitime, mais plutôt au titre de l'article 7, point f), sous réserve du respect du critère supplémentaire de mise en balance.

III.2.4. Intérêt vital

L'article 7, point d), constitue un fondement juridique dans les situations où le traitement «est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée». Ce libellé est différent des termes employés à l'article 8, paragraphe 2, point c), qui est plus précis et renvoie à des situations où «le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement».

Les deux dispositions paraissent néanmoins indiquer que ce fondement juridique devrait avoir une application limitée. Premièrement, l'expression «intérêt vital» semble limiter l'application de ce motif à des questions de vie ou de mort, ou, à tout le moins, à des menaces qui comportent un risque de blessure ou une autre atteinte à la santé de la personne concernée [ou aussi d'une autre personne, dans le cas de l'article 8, paragraphe 2, point c)].

Le considérant 31 confirme que l'objectif de ce fondement juridique est de «protéger un intérêt essentiel à la vie de la personne concernée». La directive n'indique cependant pas

[40] Des orientations émanant d'une autorité réglementaire peuvent néanmoins jouer un rôle dans l'appréciation de l'intérêt légitime poursuivi par le responsable du traitement [voir la section III.3.4, point a), notamment en page 40].

précisément si la menace doit être immédiate. Cela suscite des questions quant à la portée de la collecte de données, par exemple, à titre de mesure préventive ou à grande échelle, comme la collecte des données relatives aux passagers transportés par une compagnie aérienne en cas de risque d'épidémie ou d'incident de sûreté.

Le groupe de travail considère qu'il convient de donner une interprétation restrictive à cette disposition, conformément à l'esprit de l'article 8. Bien que l'article 7, point d), ne limite pas expressément l'utilisation de ce motif à des situations où le consentement ne peut servir de fondement juridique, pour les raisons mentionnées à l'article 8, paragraphe 2, point c), il est raisonnable de supposer que, lorsqu'il est possible et nécessaire de demander un consentement valable, il y a effectivement lieu d'obtenir ce consentement chaque fois que les conditions le permettent. Cette disposition verrait ainsi son application limitée à une analyse au cas par cas et elle ne pourrait normalement servir à légitimer ni la collecte massive de données à caractère personnel ni leur traitement. Au cas où cela s'avérerait nécessaire, les points c) ou e) de l'article 7 représenteraient des motifs plus appropriés pour justifier le traitement.

III.2.5. Mission d'intérêt public

L'article 7, point e), constitue un fondement juridique dans les situations où le traitement «est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées».

Il importe de noter que, tout comme l'article 7, point c), l'article 7, point e), se rapporte à l'intérêt public de l'Union européenne ou d'un État membre. De même, «l'autorité publique» désigne une autorité conférée par l'Union européenne ou par un État membre. Autrement dit, les missions menées dans l'intérêt public d'un pays tiers ou relevant de l'exercice d'une autorité publique conférée en vertu d'une législation étrangère n'entrent pas dans le champ d'application de cette disposition[41].

L'article 7, point e), recouvre deux situations et s'applique tant au secteur public qu'au secteur privé. Premièrement, il concerne des situations où le responsable du traitement est lui-même investi d'une autorité publique ou d'une mission d'intérêt public (sans nécessairement être lui aussi soumis à une obligation légale de traiter des données) et où le traitement est nécessaire à l'exercice de cette autorité ou de cette mission. Par exemple, une administration fiscale peut collecter et traiter la déclaration de revenus d'une personne afin d'établir et de vérifier le montant de l'impôt à payer. Ou une association professionnelle, comme un barreau d'avocats ou un ordre des médecins, investie de l'autorité publique requise, peut engager des procédures disciplinaires à l'encontre de certains de ses membres. Un autre exemple pourrait être celui d'une collectivité locale, comme une administration municipale, chargée de gérer une bibliothèque, une école ou une piscine.

Deuxièmement, l'article 7, point e), couvre aussi des situations où le responsable du traitement n'est pas investi d'une autorité publique, mais est invité à communiquer des données à un tiers investi d'une telle autorité. Par exemple, un agent d'un service public

[41] Voir la section 2.4 du document de travail du groupe de travail «Article 29» relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, adopté le 25 novembre 2005 (WP 114), pour une interprétation similaire de la notion de «sauvegarde d'un intérêt public important» visée à l'article 26, paragraphe 1, point d).

compétent pour enquêter sur un crime peut demander au responsable du traitement sa coopération dans le cadre d'une enquête en cours, plutôt que de lui ordonner de se soumettre à une demande de coopération spécifique. L'article 7, point e), peut en outre couvrir des situations où le responsable du traitement communique des données, de manière proactive, à un tiers investi de cette autorité publique. Cela peut être le cas, par exemple, quand un responsable du traitement constate qu'une infraction pénale a été commise et transmet l'information aux services répressifs compétents de sa propre initiative.

À la différence de l'article 7, point c), il n'est pas nécessaire que le responsable du traitement soit soumis à une obligation légale. Pour reprendre l'exemple donné ci-dessus, un responsable du traitement qui remarquerait par hasard qu'une fraude ou un vol a été commis n'aurait peut-être pas l'obligation légale de le signaler à la police, mais il pourrait néanmoins, le cas échéant, le faire volontairement en vertu de l'article 7, point e).

Il faut cependant que le traitement soit «nécessaire à l'exécution d'une mission d'intérêt public», ou encore que le responsable du traitement ou le tiers auquel il communique les données soit investi d'une autorité publique et que le traitement des données soit nécessaire à l'exercice de cette autorité[42]. Il importe aussi de souligner que cette autorité publique ou cette mission d'intérêt public aura généralement été attribuée par une loi ou une autre règle de droit. Si le traitement suppose une ingérence dans la vie privée ou si le droit national l'exige par ailleurs afin de garantir la protection des personnes concernées, la base juridique encadrant le genre de traitement de données qui peut être autorisé devra être suffisamment précise et spécifique.

Ces situations deviennent de plus en plus courantes et se répandent aussi en dehors du secteur public, du fait de la tendance à sous-traiter des missions de l'administration à des entités du secteur privé. Cela peut être le cas, par exemple, pour les activités de traitement du secteur des transports ou de la santé (études épidémiologiques, recherches, etc.). Ce motif pourrait aussi être invoqué dans le cadre de l'action répressive, comme l'ont déjà montré les exemples ci-dessus. Cependant, la mesure dans laquelle une société privée peut être autorisée à coopérer avec les services répressifs, par exemple pour lutter contre la fraude ou le partage de contenu illégal sur l'internet, requiert une analyse au regard non seulement de l'article 7, mais aussi de l'article 6, afin de prendre en considération les exigences de limitation de la finalité, de licéité et de loyauté[43].

L'article 7, point e), a potentiellement un champ d'application très large, ce qui plaide en faveur d'une interprétation stricte et d'une définition précise, au cas par cas, de l'intérêt public en jeu et de l'autorité publique justifiant le traitement. Ce large champ d'application explique aussi pourquoi, comme dans le cas de l'article 7, point f), un droit d'opposition a été prévu à

[42] Autrement dit, dans ces cas, l'intérêt public des missions et la responsabilité correspondante subsisteront, même si l'exercice de la mission a été confié à d'autres entités, y compris dans le secteur privé.
[43] Voir, en ce sens, l'avis du groupe de travail «Article 29» sur SWIFT (cité précédemment, en note de bas de page 39), l'avis 4/2003 du groupe de travail «Article 29» sur le niveau de protection assuré aux États-Unis pour la transmission des données passagers, adopté le 13.6.2003 (WP 78) et le document de travail sur les questions de protection des données liées aux droits de propriété intellectuelle, adopté le 18.1.2005 (WP 104).

l'article 14 quand le traitement est fondé sur l'article 7, point e)[44]. Des garanties et des mesures supplémentaires similaires peuvent donc s'appliquer dans les deux cas[45].

En ce sens, l'article 7, point e), présente des similitudes avec l'article 7, point f), et, dans certains contextes, pour les pouvoirs publics en particulier, le premier peut remplacer le second.

Pour apprécier la mesure dans laquelle ces dispositions s'appliquent aux organismes du secteur public, à la lumière notamment des propositions de changements à apporter au cadre juridique de la protection des données, il est utile de noter que texte actuel du règlement n° 45/2001[46], qui fixe les règles de protection des données applicables aux institutions et organes de l'Union européenne, ne contient aucune disposition comparable à l'article 7, point f).

Le considérant 27 de ce règlement prévoit néanmoins que «[l]e traitement de données à caractère personnel effectué pour l'exécution de *missions d'intérêt public* par les institutions et les organes communautaires comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de ces institutions et organes». Cette disposition autorise donc le traitement des données pour un motif «d'intérêt public» au sens large dans des situations très variées, qui auraient pu, sinon, être couvertes par une disposition analogue à l'article 7, point f). La vidéosurveillance de locaux pour des raisons de sécurité, le contrôle électronique des échanges de courriels, ou les évaluations du personnel ne sont que quelques exemples des situations qui peuvent relever de cette disposition relative à «l'exécution de missions d'intérêt public» interprétée de manière large.

Dans une perspective d'avenir, il importe également de tenir compte du fait que le règlement proposé prévoit expressément, à l'article 6, paragraphe 1, point f), que les considérations relatives au motif de l'intérêt légitime «ne s'appliquent pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions». Si cette disposition est adoptée et interprétée au sens large, de façon à interdire totalement aux autorités publiques d'invoquer l'intérêt légitime comme fondement juridique, les motifs de la «mission d'intérêt public» et de «l'exercice de l'autorité publique» énoncés à l'article 7, point e), devraient recevoir une interprétation qui laisse aux pouvoirs publics une certaine latitude, pour au moins leur permettre d'assurer correctement leur gestion et leur fonctionnement, à l'instar de l'interprétation du règlement n° 45/2001 qui prévaut actuellement.

Une autre possibilité serait d'interpréter la dernière phrase de l'article 6, paragraphe 1, point f), du règlement proposé de façon à ne pas interdire totalement aux autorités publiques d'invoquer l'intérêt légitime comme fondement juridique. Dans ce cas, l'expression «traitement effectué par les autorités publiques dans l'exécution de leurs missions» figurant à l'article 6, paragraphe 1, point f), tel qu'il est proposé, devrait recevoir une interprétation restrictive, ne couvrant pas le traitement effectué aux fins d'assurer correctement la gestion et

[44] Comme indiqué précédemment, cette possibilité de s'opposer au traitement des données en vertu de l'article 7, point e), n'existe pas dans certains États membres (par exemple, en Suède).
[45] Comme on le verra plus loin, le projet de rapport de la commission LIBE recommandait d'autres garanties – en particulier, une transparence renforcée – dans le cas où l'article 7, point f), s'applique.
[46] Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8, 12.1.2001, p. 1).

le fonctionnement de ces autorités publiques. De ce fait, il resterait possible d'invoquer le motif de l'intérêt légitime pour justifier le traitement nécessaire à la bonne gestion et au fonctionnement correct de ces pouvoirs publics.

III.3. Article 7, point f): intérêt légitime

L'article 7, point f)[47], impose un critère de mise en balance: l'intérêt légitime poursuivi par le responsable du traitement (ou par des tiers) doit être comparé avec l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Le résultat de cette mise en balance détermine dans une large mesure si l'article 7, point f), peut servir de fondement juridique justifiant le traitement.

Il convient de préciser d'emblée que ce critère ne se borne pas à une simple mise en balance consistant à peser deux «poids» aisément quantifiables et comparables. Comme on le verra plus en détail dans la description présentée ci-après, cette mise en balance peut nécessiter une appréciation complexe de divers facteurs. Afin de mieux structurer et de simplifier l'évaluation, nous avons scindé le processus en plusieurs étapes pour garantir l'application effective du critère de mise en balance.

La section III.3.1 commence par examiner un plateau de la balance: ce qui constitue «l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées». Dans la section III.3.2, nous nous pencherons sur l'autre plateau de la balance, à savoir «l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, paragraphe 1».

Les sections III.3.3 et III.3.4 expliquent la manière dont le critère de mise en balance doit être appliqué. La section III.3.3 présente une introduction générale à l'aide de trois scénarios différents. Ensuite, la section III.3.4 expose les principales considérations dont il faut tenir compte pour appliquer le critère, et notamment les garanties et les mesures à prévoir par le responsable du traitement des données.

Enfin, dans les sections III.3.5 et III.3.6, nous examinerons aussi certains mécanismes particuliers tels que le principe de responsabilité, la transparence et le droit d'opposition, qui peuvent contribuer à assurer – et approfondir – une mise en balance correcte des divers intérêts en jeu.

III.3.1. Intérêt légitime poursuivi par le responsable du traitement (ou par des tiers)

La notion d'«intérêt»

La notion d'«intérêt» et celle de «finalité», mentionnée à l'article 6 de la directive, sont étroitement liées, mais néanmoins distinctes. En matière de protection des données, la «finalité» est la raison spécifique pour laquelle les données sont traitées: le but ou l'intention de leur traitement. L'intérêt, quant à lui, est l'enjeu plus large poursuivi par le responsable du traitement, ou le bénéfice qu'il tire – ou que la société pourrait tirer - du traitement.

[47] Pour le libellé complet de l'article 7, point f), voir la page 4 ci-dessus.

Par exemple, une entreprise peut avoir un *intérêt* à préserver la santé et la sécurité du personnel qui travaille dans sa centrale nucléaire. Pour ce faire, l'entreprise peut avoir comme *finalité* d'appliquer des procédures de contrôle d'accès spécifiques qui justifient le traitement de certaines données à caractère personnel afin de contribuer à protéger la santé et la sécurité des employés.

Un intérêt doit être formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée. De plus, l'intérêt en jeu doit aussi être «poursuivi par le responsable du traitement». Cela suppose un intérêt réel et présent, qui correspond à des activités menées actuellement ou à des bénéfices escomptés dans un avenir très proche. Autrement dit, des intérêts trop vagues ou hypothétiques ne seront pas suffisants.

La nature de l'intérêt peut varier. Certains intérêts peuvent être impérieux et profitables à la société en général, comme l'intérêt de la presse à publier des informations sur des faits de corruption dans l'administration ou l'intérêt d'effectuer des recherches scientifiques (sous réserve de garanties appropriées). D'autres intérêts peuvent être moins pressants pour l'ensemble de la société ou, en tout cas, leur poursuite peut avoir une incidence plus mitigée ou controversée sur la collectivité. Cela peut s'appliquer, par exemple, à l'intérêt économique d'une entreprise à en savoir le plus possible sur ses clients potentiels afin de mieux cibler la publicité pour ses produits ou services.

Qu'est-ce qui rend un intérêt «légitime» ou «illégitime»?

Cette question vise à déterminer le seuil de ce qui constitue un intérêt légitime. Si l'intérêt poursuivi par le responsable du traitement des données est illégitime, le critère de mise en balance n'aura pas à être appliqué, puisque le seuil initial permettant d'invoquer l'article 7, point f), n'aura pas été atteint.

Le groupe de travail considère que la notion d'intérêt légitime pourrait inclure des intérêts très variés, qu'ils soient futiles ou incontestables, évidents ou plus controversés. C'est donc dans un deuxième temps, lorsqu'il s'agira de mettre en balance ces intérêts avec les intérêts et droits fondamentaux des personnes concernées, qu'il conviendra d'adopter une approche plus restreinte et de procéder à une analyse plus approfondie.

La liste qui suit énumère de façon non exhaustive certains des contextes où la question de l'intérêt légitime au sens de l'article 7, point f), est le plus communément susceptible de se poser. Elle est présentée ici sans préjuger si l'intérêt poursuivi par le responsable du traitement prévaudra en définitive sur l'intérêt et les droits des personnes concernées après la mise en balance.

- Exercice du droit à la liberté d'expression ou d'information, notamment dans les médias et dans les arts;
- prospection directe conventionnelle et autres formes de prospection commerciale ou de publicité;
- messages non commerciaux non sollicités, notamment à des fins de campagne politique ou de collecte de fonds pour des actions caritatives;
- exécution de demandes en justice, y compris le recouvrement de créances via des procédures extrajudiciaires;

- prévention de la fraude, de l'utilisation abusive de services, ou du blanchiment d'argent;
- surveillance du personnel à des fins de sécurité ou de gestion;
- mécanismes de dénonciation des dysfonctionnements;
- sécurité physique, sécurité des systèmes et réseaux informatiques;
- traitement à finalité historique, scientifique ou statistique;
- traitement à des fins de recherche (y compris la recherche commerciale).

En conséquence, un intérêt peut être considéré comme légitime dès lors que le responsable du traitement est en mesure de poursuivre cet intérêt dans le respect de la législation sur la protection des données et d'autres législations. Autrement dit, un intérêt légitime doit être «acceptable au regard du droit»[48].

Pour être pertinent au regard de l'article 7, point f), un «intérêt légitime» doit donc:

- être licite (c'est-à-dire conforme au droit en vigueur dans l'Union et dans le pays concerné);
- être formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée (c'est-à-dire suffisamment précis);
- constituer un intérêt réel et présent (c'est-à-dire non hypothétique).

Le fait que le responsable du traitement poursuive un tel intérêt légitime en traitant certaines données ne signifie pas qu'il puisse nécessairement invoquer l'article 7, point f), comme fondement juridique justifiant le traitement. La légitimité de l'intérêt poursuivi n'est qu'un point de départ, un des éléments qui doivent être analysés en vertu de l'article 7, point f). La possibilité d'invoquer cette disposition dépendra du résultat de la mise en balance qui suit.

À titre d'illustration: des responsables du traitement peuvent avoir un intérêt légitime à connaître les préférences de leurs clients pour être en mesure de mieux personnaliser leurs offres et, en fin de compte, de proposer des produits et des services qui correspondent mieux aux besoins et aux désirs des clients. Dans cette perspective, l'article 7, point f), peut constituer un fondement juridique approprié pour certains types d'activités de prospection, en ligne ou hors ligne, pour autant qu'il existe des garanties appropriées [incluant, entre autres, un mécanisme fonctionnel permettant de s'opposer à ce traitement conformément à

[48] Les observations concernant la nature de la «légitimité» formulées à la section III.1.3 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité en note de bas de page 9 ci-dessus) s'appliquent aussi ici, mutatis mutandis. Comme il est indiqué aux pages 19 et 20 de cet avis, la notion de «droit» est utilisée ici dans son sens le plus large. Cela inclut d'autres législations applicables, par exemple en matière d'emploi, de contrats, ou de protection des consommateurs. De plus, la notion de droit «inclut toutes les formes de droit écrit et coutumier, le droit primaire et le droit dérivé, les arrêtés municipaux, les précédents judiciaires, les principes constitutionnels, les droits fondamentaux, d'autres principes juridiques, ainsi que la jurisprudence, tel que ce "droit" serait interprété et pris en compte par des juridictions compétentes. Dans les limites du droit, d'autres éléments comme les coutumes, les codes de conduite, les codes de déontologie, les accords contractuels, ainsi que les circonstances et le contexte général peuvent aussi être pris en considération pour déterminer si une finalité particulière est légitime. Cela peut comprendre la nature de la relation sous-jacente entre le responsable du traitement et les personnes concernées, qu'elle soit commerciale ou autre». En outre, ce qui peut être considéré comme un intérêt légitime «peut aussi changer au fil du temps, en fonction des progrès scientifiques et technologiques, et des évolutions de la société et des attitudes culturelles».

l'article 14, paragraphe b), comme on le verra à la section III.3.6, *Le droit d'opposition et au-delà*].

Cela ne signifie pas pour autant que les responsables du traitement pourraient invoquer l'article 7, point f), pour surveiller indûment les activités en ligne ou hors ligne de leurs clients, pour compiler d'importants volumes de données à leur propos en provenance de différentes sources, collectées à l'origine dans d'autres contextes et à des fins différentes, et pour créer – mais aussi, par exemple, échanger en passant par des courtiers en informations – des profils complexes concernant la personnalité et les préférences des clients, sans les en informer ni mettre à leur disposition un mécanisme fonctionnel permettant d'exprimer leur opposition, pour ne rien dire de leur consentement éclairé. Une telle activité de profilage risque de constituer une violation grave de la vie privée du client et, dans ce cas, l'intérêt et les droits de la personne concernée prévaudraient sur l'intérêt poursuivi par le responsable du traitement[49].

Pour donner un autre exemple, dans son avis sur SWIFT[50], le groupe de travail concluait, tout en reconnaissant l'intérêt légitime de la société à se conformer aux sommations du droit des États-Unis pour éviter le risque d'être sanctionnée par les autorités américaines, que l'article 7, point f), ne pouvait pas être invoqué. Le groupe de travail considérait notamment qu'en raison des conséquences considérables pour les particuliers du traitement de données effectué d'une manière «cachée, systématique, massive et de longue durée», «les intérêts des nombreuses personnes concernées sur le plan des libertés et des droits fondamentaux prévalent [contre] ceux de SWIFT à ne pas être sanctionnée par les États-Unis pour non-soumission éventuelle à une sommation».

Comme on le verra plus tard, si l'intérêt poursuivi par le responsable du traitement n'est pas impérieux, l'intérêt et les droits de la personne concernée ont plus de chances de prévaloir contre l'intérêt légitime – mais moins important – du responsable du traitement. Il ne s'ensuit pas, cependant, que des intérêts moins impérieux poursuivis par le responsable du traitement ne puissent pas, parfois, prévaloir contre l'intérêt et les droits des personnes concernées: cela arrive généralement quand les conséquences du traitement pour les personnes concernées sont aussi moins importantes.

L'intérêt légitime dans le secteur public

Le texte actuel de la directive n'exclut pas expressément que les responsables du traitement qui sont des autorités publiques puissent se servir de l'article 7, point f), comme fondement juridique pour traiter des données[51].

[49] La question des techniques de traçage et le rôle du consentement exigé par l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» seront discutés séparément. Voir la section III.3.6, point b), sous l'intitulé: «Illustration: l'évolution de l'approche de la prospection directe».

[50] Voir la section 4.2.3 de l'avis déjà cité en note de bas de page 39. L'intérêt légitime poursuivi par le responsable du traitement dans cette affaire était aussi lié à l'intérêt public d'un pays tiers, qui ne saurait relever de la directive 95/46/CE.

[51] À l'origine, la première proposition de directive de la Commission couvrait séparément le traitement des données dans le secteur privé et les activités de traitement dans le secteur public. Cette distinction formelle entre les règles applicables au secteur public et au secteur privé a été abandonnée dans la proposition modifiée. Cela aurait aussi pu entraîner des divergences d'interprétation et de mise en œuvre par les divers États membres.

Cependant, la proposition de règlement[52] exclut cette possibilité pour le «traitement effectué par les autorités publiques dans l'exécution de leurs missions».

Le changement législatif proposé fait ressortir l'importance du principe selon lequel, en règle générale, les autorités publiques ne devraient traiter des données à caractère personnel dans l'exécution de leurs missions que si elles y sont dûment autorisées par la loi. Le respect de ce principe est particulièrement important – et clairement requis par la jurisprudence de la Cour européenne des droits de l'homme – dans les cas où la vie privée des personnes concernées est en jeu et où les activités de l'autorité publique constitueraient une ingérence dans cette vie privée.

Une autorisation suffisamment *détaillée et précise* prévue par la loi est donc exigée – dans la directive actuelle également – lorsque le traitement par les autorités publiques suppose une ingérence dans la vie privée des personnes concernées. Cela peut prendre la forme d'une obligation légale spécifique de traiter des données, conformément à l'article 7, point c), ou d'une autorisation spécifique (sans qu'il s'agisse nécessairement d'une obligation) de traiter des données, dans le respect des exigences de l'article 7, point e) ou f)[53].

L'intérêt légitime des tiers

Le texte actuel de la directive ne mentionne pas seulement «l'intérêt légitime poursuivi par le responsable du traitement» mais autorise aussi l'invocation de l'article 7, point f), quand l'intérêt légitime est poursuivi par «les tiers auxquels les données sont communiquées»[54]. Les exemples suivants illustrent certaines des situations où cette disposition peut s'appliquer.

Publication de données à des fins de transparence et de responsabilité. Un contexte important où l'article 7, point f), peut être pertinent est celui où la publication de données vise à assurer la transparence et la responsabilité (par exemple, les salaires des dirigeants d'une entreprise). Dans ce cas, on peut considérer que la divulgation publique est effectuée principalement non pas dans l'intérêt du responsable du traitement qui publie les données, mais dans celui d'autres parties prenantes, comme les salariés, la presse ou l'opinion publique, à qui les données sont communiquées.

Dans une perspective de protection des données et de respect de la vie privée, et afin de garantir la sécurité juridique, en général, il est souhaitable que les données à caractère personnel soient rendues publiques en vertu d'une loi qui l'autorise et, s'il y a lieu, qui

[52] Voir l'article 6, paragraphe 1, point f), de la proposition de règlement.

[53] À cet égard, voir aussi la section III.2.5 ci-dessus à propos des missions d'intérêt public (pages 23 à 25) ainsi que les considérations présentées ci-après sous l'intitulé *L'intérêt légitime des tiers* (pages 30 à 32). Voir aussi les réflexions sur les limites de «l'application du droit par la sphère privée», en page 39 sous l'intitulé «Intérêt public/intérêt de la collectivité». Dans toutes ces situations, il importe particulièrement de veiller au respect absolu des limites définies par l'article 7, point f), et aussi par l'article 7, point e).

[54] La proposition de règlement entend restreindre l'utilisation de ce motif aux «intérêts légitimes poursuivis par un responsable du traitement». Il n'apparaît pas clairement, à la lecture du texte seul, si le libellé proposé correspond uniquement à une volonté de simplification du texte ou si son intention est d'exclure les situations où un responsable du traitement pourrait communiquer des données dans l'intérêt légitime poursuivi par d'autres. Ce texte n'est cependant pas définitif. L'intérêt des tiers a, par exemple, été réintroduit dans le rapport final de la commission LIBE à l'occasion du vote des amendements de compromis par cette commission du Parlement européen le 21 octobre 2013. Voir l'amendement 100 sur l'article 6. Le groupe de travail est favorable à la réintroduction de l'intérêt des tiers dans la proposition, étant donné que son utilisation peut demeurer appropriée dans certaines situations, notamment celles décrites ci-après.

spécifie clairement les données à publier, la finalité de la publication et toutes les garanties nécessaires[55]. Il s'ensuit également qu'il peut être préférable que l'article 7, point c), plutôt que l'article 7, point f), serve de fondement juridique quand des données à caractère personnel sont divulguées à des fins de transparence et de responsabilité[56].

Cependant, en l'absence d'une obligation légale expresse ou de la permission de publier des données, il serait néanmoins possible de communiquer des données à caractère personnel à des parties intéressées. Dans des circonstances appropriées, il serait aussi possible de publier des données à caractère personnel à des fins de transparence et de responsabilité.

Dans les deux cas – c'est-à-dire indépendamment du fait que les données à caractère personnel soient divulguées en vertu d'une loi l'autorisant ou non – la divulgation dépend directement du résultat de la mise en balance prévue à l'article 7, point f), et de la mise en œuvre de garanties et de mesures appropriées[57].

En outre, l'utilisation ultérieure, dans un souci de plus grande transparence, de données à caractère personnel déjà publiées (par exemple, la republication des données par la presse, ou la diffusion ultérieure d'un ensemble de données publiées initialement, d'une manière plus innovante ou conviviale par une ONG), peut aussi être souhaitable. La possibilité ou non de republier et de réutiliser les données dépendra également du résultat de la mise en balance, qui devrait tenir compte, en autres, de la nature des informations et des conséquences pour les particuliers de la republication ou de la réutilisation[58].

Recherche historique ou autres formes de recherche scientifique. Un autre contexte important dans lequel la divulgation dans l'intérêt légitime poursuivi par des tiers peut être pertinente se rapporte à la recherche historique ou à d'autres formes de recherche scientifique, en particulier lorsque ces travaux nécessitent un accès à certaines bases de données. La directive reconnaît expressément ces activités, sous réserve de garanties et de mesures appropriées[59],

[55] Cette recommandation de bonnes pratiques ne devrait pas remettre en cause les dispositions nationales en matière de transparence et d'accès public aux documents.

[56] En effet, dans certains États membres, il faut respecter des règles différentes pour le traitement effectué par des parties du secteur public ou privé. Par exemple, selon le code italien de la protection des données, la diffusion de données à caractère personnel par un organisme public n'est autorisée que si elle est prévue par une loi ou un règlement (article 19.3).

[57] Comme l'explique l'avis 06/2013 du groupe de travail «Article 29» sur les données ouvertes (voir page 9 de cet avis, cité en note de bas de page 88 ci-après), «la législation nationale doit respecter l'article 8 de la Convention européenne des droits de l'homme (CEDH) et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne («Charte de l'UE»). Cela implique, comme l'a déclaré la Cour de justice de l'UE dans ses arrêts Österreichischer Rundfunk et Schecke, qu'il faut établir que la divulgation «est nécessaire et proportionnée au but légitime recherché». Voir l'arrêt de la Cour du 20 mai 2003 dans les affaires jointes C-465/00, C-138/01 et C-139/01, Rundfunk, et l'arrêt de la Cour du 9 novembre 2010, dans les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke.

[58] La limitation de la finalité constitue également une considération importante à cet égard. En page 22 de son avis 06/2013 sur les données ouvertes (cité en note de bas de page 88 ci-après), le groupe de travail recommande «que toute loi qui demande un accès public à des données énonce clairement les finalités de la divulgation des données à caractère personnel. Si ce n'est pas le cas, ou si seuls des termes généraux et vagues sont employés, la sécurité juridique et la prévisibilité en souffriront. En particulier, pour toute demande de réutilisation, l'organisme du secteur public et les réutilisateurs potentiels éprouveront de grandes difficultés à déterminer la finalité première de la publication et, ensuite, les autres finalités qui seraient compatibles avec cette finalité. Comme cela a été dit précédemment, même si les données à caractère personnel sont publiées sur l'internet, cela n'implique pas qu'elles peuvent faire l'objet d'un traitement ultérieur pour toute autre finalité.»

[59] Voir, par exemple, l'article 6, paragraphe 1, points b) et e).

mais il ne faut pas oublier que le fondement légitime de ces activités résidera souvent dans une utilisation mûrement réfléchie de l'article 7, point f)[60].

Intérêt général ou intérêt d'un tiers. Enfin, l'intérêt légitime des tiers peut aussi être pertinent à d'autres égards. C'est le cas lorsqu'un responsable du traitement – parfois encouragé par les autorités publiques – poursuit un intérêt qui correspond à l'intérêt général ou à l'intérêt d'un tiers. Il peut s'agir notamment de situations où le responsable du traitement va plus loin que les obligations légales spécifiques qui lui sont imposées par des lois ou des réglementations afin d'aider les services répressifs ou des acteurs privés dans leur lutte contre des activités illégales, comme le blanchiment d'argent, la séduction malintentionnée de mineurs ou le partage illégal de fichiers en ligne. Dans ces situations, cependant, il importe particulièrement de veiller à ce que les limites prévues par l'article 7, point f), soient pleinement respectées[61].

Le traitement doit être nécessaire à la/aux finalité(s) visée(s)

Enfin, le traitement des données à caractère personnel doit aussi être «nécessaire à la réalisation de l'intérêt légitime» poursuivi par le responsable du traitement ou – en cas de communication des données – par le tiers. Cette condition complète l'exigence de nécessité au titre de l'article 6 et suppose l'existence d'un lien entre le traitement et l'intérêt poursuivi. Cette exigence de «nécessité» s'applique dans toutes les situations mentionnées à l'article 7, points b) à f), mais elle est particulièrement pertinente dans le cas du point f), afin de garantir que le traitement des données fondé sur l'intérêt légitime ne débouche pas sur une interprétation trop large de la nécessité de traiter des données. Comme dans les autres cas, cela signifie qu'il y a lieu d'examiner s'il existe d'autres moyens plus respectueux de la vie privée susceptibles de servir la même finalité.

III.3.2. L'intérêt ou les droits de la personne concernée

L'intérêt ou les droits (et non, comme il est écrit dans la version anglaise, «interests for rights»)

Le texte anglais de l'article 7, point f), de la directive mentionne «the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)».

Le groupe de travail a cependant constaté, en comparant les différentes versions linguistiques de la directive, que l'expression «interests for» a été traduite avec le sens de «interests or» dans d'autres langues importantes utilisées lorsque le texte a été négocié[62].

[60] Comme l'explique l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité en note de bas de page 9 ci-dessus), l'utilisation ultérieure de données à des fins secondaires devrait être subordonnée à une double condition. Premièrement, il convient de veiller à ce que les données servent à des finalités compatibles. Deuxièmement, il y a lieu de vérifier si le traitement est fondé sur une base juridique appropriée au titre de l'article 7.

[61] Voir à cet égard, par exemple, le document de travail sur les questions de protection des données liées aux droits de propriété intellectuelle, adopté le 18.1.2005 (WP 104).

[62] Par exemple, «l'intérêt ou les droits et libertés fondamentaux de la personne concernée» en français, «l'interesse o i diritti e le libertà fondamentali della persona interessata» en italien; «das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person», en allemand.

Une analyse plus approfondie donne à penser que le libellé anglais de la directive est simplement le résultat d'une faute de frappe: «or» a été erronément dactylographié «for»[63]. Le texte anglais correct devrait donc être: «interests or fundamental rights and freedoms».

Il convient de donner une interprétation large aux notions d'«intérêt» et de «droits»

La mention de «l'intérêt ou les droits et libertés fondamentaux» a une incidence directe sur le champ d'application de la disposition. Elle accorde davantage de protection à la personne concernée, c'est-à-dire qu'elle requiert que l'«intérêt» des personnes concernées soit lui aussi pris en considération, et non pas seulement ses droits et libertés fondamentaux. Il n'y a cependant aucune raison de supposer que la restriction de l'article 7, point f), aux droits fondamentaux «qui appellent une protection au titre de l'article 1er paragraphe 1» – et donc la référence explicite à l'objet de la directive[64] – ne s'appliquerait pas aussi au terme «intérêt». Le message sans équivoque est néanmoins que tous les intérêts pertinents de la personne concernée devraient être pris en compte.

Cette interprétation du texte paraît logique, non seulement du point de vue grammatical, mais aussi compte tenu de la large interprétation de la notion d'«intérêt légitime» du responsable du traitement. Si le responsable du traitement – ou le tiers en cas de communication des données – peut poursuivre n'importe quel intérêt, pour autant qu'il ne soit pas illégitime, la personne concernée devrait aussi pouvoir s'attendre à ce que ses intérêts de toutes sortes soient pris en considération et mis en balance avec ceux du responsable du traitement, pour autant qu'ils soient pertinents dans le champ d'application de la directive.

En ces temps où croît le déséquilibre du «pouvoir de l'information», à l'heure où administrations et entreprises amassent des volumes sans précédent de données concernant les individus et se donnent de plus en plus les moyens de constituer des profils détaillés qui prédiront leurs comportements (au risque de renforcer encore le déséquilibre informationnel et d'amoindrir l'autonomie des citoyens), il est plus crucial que jamais de protéger l'intérêt des personnes à préserver leur vie privée et leur autonomie.

Enfin, il importe de relever qu'à la différence de l'«intérêt» du responsable du traitement, l'«intérêt» des personnes concernées n'est pas suivi ici de l'adjectif «légitime». Cela suppose que la protection de l'intérêt et des droits des individus a une portée plus vaste. Même les personnes qui se livrent à des activités illégales ne devraient pas faire l'objet d'une ingérence disproportionnée dans l'exercice de leurs droits et de leurs intérêts[65]. Par exemple, un individu

[63] Le groupe de travail «Article 29» observe que, pour être correcte du point de vue grammatical, la version anglaise aurait dû être «interests in» plutôt que «interests for», si telle avait été la signification voulue. De plus, l'expression «interests for» ou «interest in» paraît être redondante, puisque, si le sens avait été celui-là, la mention «fundamental rights and freedoms» aurait normalement suffi. L'interprétation selon laquelle il s'agit d'une faute de frappe est aussi confirmée par le fait que la position commune (CE) n° 1/95 adoptée par le Conseil le 20 février 1995 mentionne aussi «interests or fundamental rights and freedoms». Enfin, le groupe de travail «Article 29» note que la Commission entendait corriger cette faute de frappe dans le règlement proposé: l'article 6, paragraphe 1, point f), mentionne «the interests or fundamental rights and freedoms of the data subject which require protection of personal data» et non «interests for».

[64] Voir l'article 1er, paragraphe 1: «Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.»

[65] Bien sûr, l'une des conséquences de la criminalité pourrait être la collecte et l'éventuelle publication de données à caractère personnel concernant les criminels et les suspects, sous réserve cependant de garanties et de conditions strictes.

qui peut avoir commis un vol dans un supermarché pourrait encore voir son intérêt prévaloir contre la publication par le propriétaire du magasin de sa photo et de son adresse privée sur les murs du supermarché ou et/ou sur l'internet.

III.3.3. Introduction à l'application du critère de mise en balance

Il est utile d'imaginer que l'intérêt légitime poursuivi par le responsable du traitement et les incidences sur l'intérêt et les droits de la personne concernée se présentent sous la forme d'un spectre. L'intérêt légitime peut être, selon les cas, minime, relativement important ou impérieux. De même, les incidences sur l'intérêt et les droits des personnes concernées peuvent présenter plus ou moins de gravité et peuvent être anodines ou très préoccupantes.

L'intérêt légitime poursuivi par le responsable du traitement, quand il est peu important, ne prévaut généralement sur l'intérêt et les droits des personnes concernées que dans les cas où les incidences sont encore plus insignifiantes. D'un autre côté, un intérêt légitime impérieux peut justifier, dans certains cas et sous réserve de garanties et de mesures adéquates, une ingérence même grave dans la vie privée ou d'autres conséquences importantes pour l'intérêt ou les droits des personnes concernées[66].

Il importe ici de souligner le rôle essentiel que les garanties peuvent jouer[67] pour réduire les incidences injustifiées sur les personnes concernées et, partant, modifier l'équilibre des droits et des intérêts, au point que ceux de ces personnes ne prévalent plus sur l'intérêt légitime poursuivi par le responsable du traitement des données. Le recours à des garanties ne suffit bien sûr pas à justifier, à lui seul, n'importe quel traitement dans toutes les situations envisageables. Il faut en outre que les garanties en question soient adéquates et suffisantes, et qu'elles réduisent indubitablement et sensiblement les incidences sur les personnes concernées.

[66] Voir, à titre d'illustration, le raisonnement suivi par le groupe de travail «Article 29» dans plusieurs avis et documents de travail:
- Avis 4/2006 sur la *Notice of Proposed Rulemaking* (notification de proposition de règlement) du US Department of Health and Human Services, du 20 novembre 2005, relative au contrôle des maladies contagieuses et à la collecte d'informations sur les passagers (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71), adopté le 14.6.2006 (WP 121, en anglais), qui traite de graves menaces spécifiques pour la santé publique.
- Avis 1/2006 sur les mécanismes de dénonciation des dysfonctionnements (cité précédemment en note de bas page note 39), qui fait intervenir la gravité d'une infraction alléguée parmi les éléments du critère de mise en balance.
- Document concernant la surveillance des communications électroniques sur le lieu de travail, adopté le 29.5.2002 (WP 55), qui met en balance le droit de l'employeur à gérer efficacement son entreprise avec la dignité humaine du travailleur, ainsi qu'avec le secret de la correspondance.

[67] Les garanties peuvent inclure, notamment, des limitations strictes du volume de données collectées, la suppression immédiate des données après utilisation, des mesures techniques et organisationnelles visant à garantir une séparation fonctionnelle, l'utilisation appropriée de techniques d'anonymisation, l'agrégation des données, et des technologies renforçant la protection de la vie privée, mais aussi plus de transparence, de responsabilité et la possibilité de s'opposer au traitement. Voir aussi la section III.3.4, point d) et plus bas.

Scénarios de présentation

Avant de passer aux orientations sur les modalités d'application du critère de mise en balance, les trois scénarios de présentation suivants peuvent illustrer, en guise d'introduction, comment se présente l'équilibre des intérêts et des droits dans la réalité. Les trois exemples reposent sur un scénario simple et anodin, qui commence avec une offre promotionnelle pour la livraison à domicile de plats italiens. Les exemples introduisent progressivement de nouveaux éléments qui montrent comment la balance se met à pencher d'un côté, tandis que l'incidence sur les personnes concernées augmente.

Scénario 1: offre spéciale d'une chaîne de pizzérias

Claudia commande une pizza via une application mobile de son smartphone, mais ne s'oppose pas à l'envoi d'offres commerciales sur le site internet. Son adresse et les informations de sa carte de crédit sont enregistrées en vue de la livraison. Quelques jours plus tard, Claudia reçoit des coupons de réduction pour des produits similaires de la chaîne de pizzérias dans la boîte à lettres de son domicile.

Analyse succincte: la chaîne de pizzérias a un intérêt légitime, mais pas particulièrement impérieux, à chercher à vendre davantage de ses produits à ses clients. D'un autre côté, il ne semble pas y avoir d'ingérence importante dans la vie privée de Claudia, ni aucune incidence injustifiée sur son intérêt et ses droits. Les données et le contexte sont relativement anodins (consommation de pizzas). La chaîne de pizzérias a mis en place certaines garanties: les informations utilisées sont relativement limitées (coordonnées de contact) et les coupons sont envoyés par courrier traditionnel. De plus, une possibilité de refuser l'envoi de publicités est prévue sur le site internet et est relativement facile à utiliser.

Tout bien pesé, et compte tenu des garanties et mesures en place (dont un outil permettant facilement de s'opposer au traitement), l'intérêt et les droits de la personne concernée ne semblent pas prévaloir sur l'intérêt légitime de la chaîne de pizzérias à procéder à ce traitement de données minimal.

Scénario 2: publicité ciblée pour la même offre promotionnelle

Le contexte est le même, mais cette fois la chaîne de pizzérias conserve non seulement l'adresse et les informations de la carte de crédit de Claudia, mais aussi son historique de commandes récent (au cours des trois dernières années). En outre, l'historique des achats est combiné avec des données provenant du supermarché où Claudia fait ses courses en ligne, qui est géré par la même société que celle qui exploite la chaîne de pizzérias. Claudia se voit proposer par la chaîne de pizzérias des offres promotionnelles et des publicités ciblées fondées sur son historique de commandes pour les deux services différents. Elle reçoit les offres promotionnelles en ligne et hors ligne, par courrier ordinaire, par courrier électronique, et par l'affichage des offres sur le site internet de la société, ainsi que sur le site de plusieurs partenaires commerciaux (quand elle accède à ces sites sur son ordinateur ou via son téléphone mobile). Son historique de navigation est aussi suivi. Ses données de localisation sont tracées via son téléphone mobile. Un logiciel analyse les données et prédits ses préférences, ainsi que les moments et les lieux où elle sera le plus encline à effectuer un achat plus important, disposée à payer un prix plus élevé, susceptible d'être influencée par un taux

de réduction particulier, ou quand elle a le plus envie de ses desserts ou plats préparés favoris[68]. Claudia est fortement agacée par les publicités qui s'affichent constamment sur son téléphone mobile quand elle vérifie l'horaire des bus pour rentrer chez elle, avec les dernières offres de plats à emporter auxquelles elle tente de résister. Elle n'a pas réussi à trouver des informations conviviales ou un moyen simple pour faire cesser ces publicités, bien que la société prétende avoir mis en place un mécanisme d'opposition au traitement des données qui couvre tout le secteur. Elle a aussi été surprise de constater qu'après avoir déménagé dans un quartier moins aisé, elle ne recevait plus d'offres promotionnelles. Sa facture mensuelle pour les achats d'alimentation a de ce fait augmenté d'environ 10 %. Un ami plus versé dans les nouvelles technologies lui a fait lire certaines hypothèses publiées sur un blog, selon lesquelles le supermarché facturerait plus cher les commandes provenant de «mauvais quartiers», en raison des risques statistiquement plus élevés de fraude à la carte de crédit. La société se refuse à tout commentaire et se retranche derrière la confidentialité de sa politique d'offres promotionnelles et le caractère propriétaire de l'algorithme utilisé pour fixer les prix.

Analyse succincte: les données et le contexte demeurent relativement bénins. Toutefois l'ampleur de la collecte de données et les méthodes utilisées pour influencer Claudia (y compris diverses techniques de traçage, la prévision des moments et des lieux propices aux envies de nourriture et le fait que Claudia est alors plus vulnérable et risque de céder à la tentation) sont des facteurs à prendre en considération pour apprécier l'impact du traitement. Le manque de transparence quant à la logique du traitement de données effectué par la société, qui peut avoir entraîné une discrimination de fait en matière de prix sur la base du lieu où une commande est passée, et les conséquences financières potentiellement importantes pour les clients font, en fin de compte, pencher la balance, même dans le contexte assez anodin des courses alimentaires et des repas à emporter. Au lieu de donner simplement la possibilité de refuser ce type de profilage et de publicité ciblée, un consentement informé serait nécessaire, conformément à l'article 7, point a), de la directive 95/46/CE, mais aussi à l'article 5, paragraphe 3) de la directive «vie privée et communications électroniques». En conséquence, l'article 7, point f), ne devrait pas pouvoir être invoqué comme fondement juridique justifiant le traitement.

Scénario 3: utilisation des commandes de denrées alimentaires pour adapter les primes d'assurance santé

Les habitudes de consommation de Claudia, y compris le moment et la nature de ses commandes de nourriture, sont vendues par la chaîne de pizzérias à une compagnie d'assurances, qui s'en sert pour ajuster ses primes d'assurance santé.

Analyse succincte: la compagnie d'assurance santé peut avoir un intérêt légitime – dans la mesure où la législation applicable l'y autorise – à évaluer les risques sanitaires auxquels s'exposent ses assurés et à leur faire payer des primes variables selon les différents risques. Cependant, la façon dont les données sont collectées et l'ampleur même de la collecte de

[68] Voir, par exemple, http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards: *«Des recherches récentes indiquent que la volonté est une ressource limitée que l'on peut épuiser ou reconstituer au fil du temps. Imaginez que la crainte de l'obésité incite une consommatrice à essayer de résister à son penchant pour la malbouffe. Il y aura forcément des moments et des endroits où elle en sera incapable. À l'aide d'un volume considérable de données, les publicitaires peuvent parvenir à comprendre exactement quand et comment approcher cette consommatrice lorsqu'elle est le plus vulnérable – surtout dans un monde constamment connecté où même nos appareils électroménagers sont capables de nous baratiner.»*

données sont excessives. Une personne raisonnable se trouvant dans la situation de Claudia ne s'attendrait probablement pas à ce que des informations sur sa consommation de pizzas puissent servir à calculer ses primes d'assurance santé.

En plus du caractère excessif du profilage et de la possibilité de suppositions inexactes (les pizzas pourraient avoir été commandées pour quelqu'un d'autre), le fait de déduire des données sensibles (risque sanitaire) à partir de données apparemment anodines (commande de repas à domicile) contribue à faire pencher la balance en faveur de l'intérêt et des droits de la personne concernée. Enfin, le traitement a aussi un impact financier considérable sur elle.

Tout bien pesé, dans ce cas spécifique, l'intérêt et les droits de la personne concernée prévalent sur l'intérêt légitime de la compagnie d'assurance santé. En conséquence, l'article 7, point f), ne devrait pas pouvoir être invoqué comme fondement juridique justifiant le traitement. Il est par ailleurs douteux que l'article 7, point a), puisse être utilisé, au regard de l'ampleur excessive de la collecte de données et peut-être aussi d'autres restrictions spécifiques imposées par le droit national.

Les scénarios présentés ci-dessus et la possibilité d'introduire des variantes comportant d'autres éléments soulignent la nécessité de disposer d'un nombre limité de facteurs-clés qui aideront à focaliser le travail d'appréciation, ainsi que d'une approche pragmatique permettant d'employer des hypothèses pratiques («méthode empirique») fondées principalement sur ce qu'une personne raisonnable jugerait acceptable selon les circonstances («attentes raisonnables») et compte tenu des conséquences de l'activité de traitement des données pour les personnes concernées («incidence»).

III.3.4. Facteurs-clés à prendre en considération pour appliquer le critère de mise en balance

Les États membres ont défini plusieurs facteurs utiles à prendre en considération pour appliquer le critère de mise en balance. La présente section examine ces facteurs dans quatre rubriques principales: a) appréciation de l'intérêt légitime du responsable du traitement, b) incidence sur les personnes concernées, c) bilan provisoire et d) garanties supplémentaires mises en place par le responsable du traitement afin de prévenir toute incidence injustifiée sur les personnes concernées[69].

Pour appliquer le critère de mise en balance, il importe, tout d'abord, d'examiner la nature et la source de l'intérêt légitime, d'une part, et l'incidence sur les personnes concernées, d'autre part. Cette appréciation devrait déjà tenir compte des mesures que le responsable du traitement prévoit d'adopter pour se conformer à la directive (afin, par exemple, de respecter la limitation de la finalité et la proportionnalité, comme l'exige l'article 6, ou d'informer les personnes concernées, conformément aux articles 10 et 11).

Après une analyse et un examen attentif de tous les aspects du problème, un bilan provisoire pourra être établi. Si le résultat de l'évaluation laisse encore quelques doutes, l'étape suivante consistera à apprécier si des garanties supplémentaires, apportant davantage de protection à la

[69] Compte tenu de leur importance, certaines questions spécifiques liées aux garanties seront examinées plus en détail dans des rubriques distinctes des sections III.3.5 et III.3.6.

personne concernée, peuvent faire pencher la balance dans un sens qui légitimerait le traitement.

a) Appréciation de l'intérêt légitime du responsable du traitement

Alors que la notion d'intérêt légitime est plutôt large, comme expliqué à la section III.3.1 ci-dessus, sa nature joue un rôle crucial quand il s'agit de mettre en balance ce type d'intérêt avec les droits et intérêts des personnes concernées. S'il est impossible de porter des jugements de valeur à l'égard de toutes les formes d'intérêt légitime envisageables, il est possible de formuler certaines orientations. Comme indiqué précédemment, cet intérêt peut être insignifiant ou impérieux, manifeste ou plus controversé.

i) Exercice d'un droit fondamental

Plusieurs droits et libertés fondamentaux parmi ceux consacrés par la Charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»)[70] et par la Convention européenne des droits de l'homme (ci-après la «CEDH») peuvent entrer en conflit avec le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, comme la liberté d'expression et d'information[71], la liberté des arts et des sciences[72], le droit d'accès aux documents[73], ainsi, par exemple, que le droit à la liberté et à la sûreté[74], la liberté de pensée, de conscience et de religion[75], la liberté d'entreprise[76], le droit de propriété[77], le droit à un recours effectif et à accéder à un tribunal impartial[78], ou la présomption d'innocence et les droits de la défense[79].

Pour que l'intérêt légitime du responsable du traitement prévale, le traitement des données doit être «nécessaire» et «proportionné» à l'exercice du droit fondamental concerné.

À titre d'illustration, selon les circonstances, il peut s'avérer nécessaire et proportionné qu'un journal publie certains éléments incriminants à propos du train de vie d'un haut fonctionnaire impliqué dans un scandale de corruption présumé. D'un autre côté, il ne s'agit pas de donner aux médias toute latitude de publier sans motif valable n'importe quel détail sur la vie privée des personnalités publiques. Ce genre de cas suscite généralement des questions d'appréciation complexes et il peut être utile, pour éclairer l'évaluation, de s'appuyer sur une législation et une jurisprudence spécifiques, sur des lignes directrices, des codes de conduite et d'autres critères formels ou informels[80].

[70] Les dispositions de la Charte s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union.
[71] Article 11 de la Charte et article 10 de la CEDH.
[72] Article 13 de la Charte et articles 9 et 10 de la CEDH.
[73] Article 42 de la Charte: «Tout citoyen de l'Union ainsi que toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre a un droit d'accès aux documents des institutions, organes et organismes de l'Union, quel que soit leur support..» Des droits d'accès similaires existent dans plusieurs États membres concernant les documents détenus par les organes publics de ces États membres.
[74] Article 6 de la Charte et article 5 de la CEDH.
[75] Article 10 de la Charte et article 9 de la CEDH.
[76] Article 16 de la Charte.
[77] Article 17 de la Charte et article 1er du protocole n°1 à la CEDH.
[78] Article 47 de la Charte et article 6 de la CEDH.
[79] Article 48 de la Charte et articles 6 et 13 de la CEDH.
[80] À propos des critères à appliquer dans les situations touchant à la liberté d'expression, la jurisprudence de la Cour européenne des droits de l'homme apporte aussi des orientations utiles. Voir, par exemple, l'arrêt de la

Dans ce contexte aussi, des garanties supplémentaires peuvent, éventuellement, jouer un rôle important et aider à trouver des moyens de parvenir à un équilibre – parfois fragile.

ii) Intérêt public/intérêt de la collectivité

Dans certains cas, le responsable du traitement peut choisir d'invoquer l'intérêt public ou l'intérêt de la collectivité (que ce soit prévu ou non par les lois ou les réglementations nationales). Par exemple, des données à caractère personnel peuvent être traitées par une association caritative aux fins de la recherche médicale, ou par une organisation sans but lucratif dans le cadre d'une action de mobilisation contre la corruption.

Il peut aussi arriver que l'intérêt commercial d'une société privée coïncide dans une certaine mesure avec un intérêt public. Cela peut être le cas, par exemple, pour lutter contre la fraude financière ou l'utilisation abusive de services[81]. Un prestataire de services peut avoir un intérêt commercial légitime à veiller à ce que ses clients n'abusent pas du service (ou ne puissent pas obtenir des services sans payer), mais, en même temps, les clients de l'entreprise, les contribuables et l'ensemble des citoyens ont aussi un intérêt légitime à ce que les activités frauduleuses soient découragées et détectées quand elles sont commises.

En général, le fait qu'un responsable du traitement agisse non seulement dans son propre intérêt légitime (commercial, par exemple), mais aussi dans l'intérêt de la collectivité, peut donner plus de «poids» à cet intérêt. Plus l'intérêt public ou collectif est impérieux, et plus la collectivité et les personnes concernées reconnaissent sans équivoque au responsable du traitement la possibilité d'agir et de procéder au traitement de données pour servir ces intérêts et s'attendent à ce qu'il l'utilise, plus l'intérêt légitime pèse dans la balance.

D'un autre côté, «l'application du droit par la sphère privée» ne doit pas servir à légitimer des pratiques qui, si elles étaient le fait d'un organisme public, seraient interdites au regard de la jurisprudence de la Cour européenne des droits de l'homme, au motif qu'elles constitueraient une ingérence d'une autorité publique dans la vie privée des personnes concernées sans satisfaire au critère rigoureux prévu par l'article 8, paragraphe 2, de la CEDH.

iii) Autres intérêts légitimes

Dans certains cas, ainsi qu'il a été expliqué à la section III.2, le contexte dans lequel un intérêt légitime apparaît peut se rapprocher de ceux où certains autres fondements juridiques peuvent être retenus, en particulier les motifs visés aux points b) (contrat), c) (obligation légale), ou e) (mission d'intérêt public), de l'article 7. Par exemple, il se peut qu'une activité de traitement des données ne soit pas strictement nécessaire, mais qu'elle reste néanmoins pertinente pour l'exécution d'un contrat, comme il est possible qu'une loi autorise, le traitement de certaines

Cour dans l'affaire von Hannover/Allemagne (n° 2) du 7 février 2012, notamment les points 95 à 126. Il faut aussi tenir compte du fait que l'article 9 de la directive (sous l'intitulé *Traitement de données à caractère personnel et liberté d'expression*) autorise les États membres à «prévoi[r], pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire, des exemptions et dérogations [à certaines dispositions de la directive]» pour autant qu'elles soient «nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression».

[81] Voir, par exemple, «Exemple 21: extraction des données de compteurs intelligents pour détecter l'utilisation frauduleuse d'énergie» en page 67 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note 9).

données,sans pour autant l'exiger. Comme on l'a vu, il n'est pas toujours facile de tracer une ligne de séparation claire entre les différents motifs, mais il n'en est que plus important d'inclure dans l'analyse le test de mise en balance visé à l'article 7, point f).

Ici encore, comme dans tous les autres cas possibles qui n'ont pas été mentionnés jusqu'à présent, plus l'intérêt poursuivi par le responsable du traitement est impérieux, et plus la collectivité reconnaît sans équivoque au responsable du traitement la possibilité d'agir et de et procéder au traitement des données pour servir cet intérêt légitime et s'attend à ce qu'il l'utilise, plus ledit intérêt pèse dans la balance[82]. Cela nous amène au point suivant, d'ordre plus général.

iv) Reconnaissance juridique et culturelle/sociétale de la légitimité des intérêts

Dans tous les contextes présentés ci-dessus, il importe également de savoir si le droit de l'Union ou d'un État membre permet expressément (même s'il ne l'exige pas) que les responsables du traitement prennent des mesures pour poursuivre l'intérêt public ou privé concerné. L'existence d'orientations non contraignantes dûment adoptées, élaborées par des autorités telles que des agences disposant de pouvoirs réglementaires, qui encouragent les responsables du traitement à traiter les données pour poursuivre l'intérêt concerné entre aussi en ligne de compte.

Le respect d'éventuelles orientations non contraignantes formulées par des autorités chargées de la protection des données ou d'autres organismes compétents concernant les modalités du traitement des données pourra probablement contribuer à une appréciation favorable lors de la mise en balance. Les attentes culturelles et sociétales, même si elles ne se reflètent pas directement dans les instruments législatifs ou réglementaires, peuvent aussi jouer un rôle et faire pencher la balance dans un sens ou dans l'autre.

Plus il est reconnu explicitement dans la législation ou dans d'autres instruments réglementaires – contraignants ou non pour les responsables du traitement – ou même dans la culture de la collectivité concernée, sans qu'il existe de base juridique précise, que les responsables du traitement peuvent prendre des mesures et traiter des données afin de poursuivre un intérêt particulier, plus cet intérêt légitime pèse lourd dans la balance[83].

b) Incidence sur les personnes concernées

L'autre plateau de la balance, à savoir l'incidence du traitement sur l'intérêt ou les droits et libertés fondamentaux de la personne concernée, constitue un critère crucial. La première sous-section présentée ci-dessous aborde en termes généraux les modalités d'évaluation de l'impact sur la personne concernée.

Plusieurs éléments peuvent être utiles ici. Ils seront analysés dans d'autres sous-sections, notamment la nature des données à caractère personnel, la façon dont les informations sont traitées, les attentes raisonnables des personnes concernées et le statut du responsable du traitement et de la personne concernée. Nous examinerons aussi brièvement certaines

[82] Bien sûr, l'appréciation doit aussi comprendre une réflexion sur le préjudice que le responsable du traitement, des tiers ou la collectivité pourraient subir si le traitement des données n'est pas effectué.
[83] Cet intérêt ne peut cependant pas servir à légitimer des pratiques d'ingérence qui, autrement, ne satisferaient pas au critère de l'article 8, paragraphe 2, de la CEDH.

questions liées aux sources de risques potentiels qui peuvent avoir des conséquences pour les individus concernés, à la gravité de ces conséquences potentielles et à la probabilité de les voir se concrétiser.

i) Évaluation de l'incidence

Pour apprécier l'incidence[84] du traitement, il convient de prendre en considération les conséquences aussi bien positives que négatives. Il peut s'agir notamment de décisions ou de mesures éventuelles qui seront prises ultérieurement par des tiers et de situations où le traitement peut aboutir à l'exclusion de certaines personnes, à une discrimination à leur encontre, à de la diffamation ou, plus généralement, de situations qui comportent un risque de nuire à la réputation, au pouvoir de négociation ou à l'autonomie de la personne concernée.

En plus des conséquences négatives qui peuvent être spécifiquement prévues, il faut aussi tenir compte des répercussions morales, comme l'irritation, la crainte et le désarroi qui peuvent résulter de la perte du contrôle exercé par la personne concernée sur ses informations à caractère personnel, ou de la découverte d'une utilisation abusive ou d'une compromission effective ou potentielle de ces informations – du fait, par exemple, de leur divulgation sur l'internet. L'effet dissuasif sur un comportement protégé, comme la liberté de recherche ou la liberté d'expression, qui peut résulter d'une surveillance constante ou d'un traçage, doit aussi être dûment pris en considération.

Le groupe de travail insiste sur l'importance cruciale de comprendre que l'«incidence» dont il faut tenir compte constitue une notion beaucoup plus large qu'un préjudice ou un dommage occasionné à une ou plusieurs personnes concernées en particulier. Le terme «incidence», tel qu'il est employé dans le présent avis, couvre toutes les conséquences possibles (potentielles ou effectives) du traitement de données. Dans un souci de clarté, nous soulignons aussi le fait que cette notion n'est pas liée à celle de violation de données et va au-delà des incidences qui peuvent résulter d'une violation de données. La notion d'incidence, telle qu'elle est utilisée ici, englobe plutôt les diverses façons dont un individu peut être affecté – positivement ou négativement – par le traitement de ses données à caractère personnel[85].

Il importe aussi de comprendre que, bien souvent, l'incidence négative subie par la personne concernée résulte de l'accumulation d'un ensemble de circonstances liées ou non et qu'il peut

[84] Cette évaluation de l'incidence doit s'entendre dans le contexte de l'article 7, point f). Autrement dit, nous ne nous référons pas à une «analyse des risques» ou à une «analyse d'impact relative à la protection des données» au sens de la proposition de règlement (articles 33 et 34) et des divers amendements proposés par la commission LIBE. La question de la méthodologie à suivre dans le cadre d'une «analyse des risques» ou d'une «analyse d'impact relative à la protection des données» déborde du cadre du présent avis. D'un autre côté, il ne faut pas perdre de vue que – d'une manière ou d'une autre –, l'analyse d'impact au regard de l'article 7, point f), peut constituer une part importante d'une «analyse des risques» ou d'une «analyse d'impact relative à la protection des données» éventuelle et peut aussi contribuer à identifier des situations où il y a lieu de consulter l'autorité chargée de la protection des données.

[85] Par exemple, le risque de préjudice financier si une violation de données provoque la diffusion d'informations financières censées être conservées dans un environnement sûr, et aboutit à un vol d'identité ou à d'autres formes de fraude, ou les risques de lésion, de douleur, de souffrance et d'inconfort qui pourraient découler, par exemple, d'une altération non autorisée de dossiers médicaux entraînant une erreur dans le traitement d'un patient, doivent toujours être dûment pris en compte, bien que cela ne se limite en aucune façon à des situations entrant dans le champ d'application de l'article 7, point f). Ces risques ne sont cependant pas les seuls à prendre en considération pour l'évaluation d'impact au regard de l'article 7, point f).

se révéler difficile d'établir quelle activité de traitement a été déterminante pour cette incidence négative et par quel responsable du traitement elle a été effectuée.

Étant donné que, dans ce contexte, il est souvent difficile, pour les personnes concernées, de constituer un dossier de demande d'indemnisation pour un préjudice ou un dommage subi, même si l'effet lui-même est très réel, il n'en est que plus important de privilégier la prévention et de veiller à ce que les activités de traitement des données ne puissent avoir lieu que si le risque d'une incidence négative indue sur l'intérêt ou les droits et libertés fondamentaux des personnes concernées est nul ou très faible.

Pour évaluer l'incidence, la terminologie et la méthodologie employées en matière d'analyse des risques traditionnelle peuvent être utiles dans une certaine mesure. C'est pourquoi quelques éléments de cette méthodologie seront évoqués succinctement ci-après. L'élaboration d'une méthodologie complète d'évaluation d'impact – dans le contexte de l'article 7, point f), ou d'une manière plus générale – sortirait cependant du cadre du présent avis.

Dans ce contexte comme dans d'autres, il est important d'identifier les sources d'incidences potentielles sur les personnes concernées.

La probabilité qu'un risque se concrétise est un des éléments à prendre en considération. Par exemple, l'accessibilité via l'internet, les échanges de données avec des sites hébergés en dehors de l'Union, les interconnexions avec d'autres systèmes et un degré élevé d'hétérogénéité ou de variabilité peuvent représenter des vulnérabilités que des pirates pourraient exploiter. À cette source de risque correspond une probabilité élevée de voir le risque de compromission de données se matérialiser. À l'inverse, un système homogène et stable qui n'a pas d'interconnexions et est déconnecté de l'internet comporte un risque beaucoup plus faible de compromission de données.

Un autre élément de l'analyse des risques tient à la gravité des conséquences d'un risque qui se concrétise. Il peut s'agir, dans les cas les moins préoccupants, de la simple contrariété liée à la nécessité de réencoder les coordonnées perdues par le responsable du traitement des données mais, dans les cas les plus extrêmes, les conséquences peuvent être fatales, par exemple quand la localisation d'individus placés sous protection tombe entre les mains de criminels ou en cas de coupure de l'alimentation électrique à distance via des compteurs intelligents alors que les conditions météorologiques ou l'état de santé des personnes concernées sont critiques.

Chacun de ces deux éléments-clés – la probabilité que le risque se concrétise d'une part, et la gravité des conséquences de l'autre – contribue à l'évaluation générale de l'incidence potentielle.

Enfin, en appliquant la méthodologie, il ne faut pas perdre de vue que l'évaluation d'impact au regard de l'article 7, point f), ne saurait aboutir à un exercice mécanique et purement quantitatif. Dans les scénarios d'analyse des risques traditionnels, la «gravité» peut prendre en compte le nombre d'individus susceptibles d'être affectés. Néanmoins, il convient de rappeler qu'un traitement des données à caractère personnel ayant une incidence sur un petit nombre de personnes – voire sur un seul individu – requiert quand même une analyse très minutieuse, surtout si l'incidence sur chaque individu concerné est potentiellement importante.

ii) Nature des données

Il serait important, tout d'abord, d'évaluer si le traitement porte sur des données sensibles, soit qu'elles relèvent des catégories particulières de données visées à l'article 8 de la directive, soit pour d'autres raisons, comme dans le cas des données biométriques, des informations génétiques, des données de communication, des données de localisation et d'autres formes d'informations personnelles nécessitant une protection spéciale[86].

À titre d'illustration, le groupe de travail considère, en règle générale, que l'utilisation de la biométrie pour satisfaire à des exigences générales en matière de sécurité des biens ou des personnes constitue un intérêt légitime sur lequel prévaudrait l'intérêt ou les droits et libertés fondamentaux de la personne concernée. D'un autre côté, des données biométriques comme les empreintes digitales et/ou l'image de l'iris pourraient servir à assurer la sécurité d'un lieu à haut risque comme un laboratoire effectuant des recherches sur des virus dangereux, pour autant que le responsable du traitement ait apporté la preuve concrète de l'existence d'un risque considérable[87].

En général, plus les informations sont sensibles, plus les conséquences qu'elles peuvent avoir pour la personne concernée sont importantes. Cela ne veut pas dire, cependant, qu'il est permis de traiter librement, en vertu de l'article 7, point f), des données qui, en elles-mêmes, peuvent paraître anodines. En effet, selon la façon dont elles sont traitées, même ces données peuvent avoir une incidence importante sur les individus, comme on le verra dans la sous-section iii) ci-dessous.

À cet égard, le fait que les données aient déjà été rendues publiques par la personne concernée ou par des tiers peut être un élément pertinent. Il importe avant tout de souligner ici que les données à caractère personnel, même si elles ont été rendues publiques, restent considérées comme des données à caractère personnel et que leur traitement continue donc à requérir des garanties appropriées[88]. Il n'existe aucune autorisation générale permettant de réutiliser et de traiter de nouveau des données à caractère personnel publiquement disponibles en vertu de l'article 7, point f).

Cela dit, le fait que des données à caractère personnel soient publiquement disponibles est un facteur qui peut être pris en considération dans l'évaluation, surtout si leur publication s'accompagnait d'une attente raisonnable d'utilisation ultérieure des données à certaines fins

[86] Les données biométriques et les informations génétiques sont considérées comme des catégories particulières de données dans la proposition de règlement sur la protection des données de la Commission, lue conjointement avec les amendements proposés par la commission LIBE. Voir l'amendement 103 sur l'article 9 dans le rapport final de la commission LIBE. À propos de la relation entre les articles 7 et 8 de la directive 95/46/CE, voir la section III.1.2 ci-dessus, en pages 15 à 17.

[87] Voir l'avis 3/2012 du groupe de travail «Article 29» sur l'évolution des technologies biométriques (WP 193). Pour donner un autre exemple, dans son avis 4/2009 sur l'Agence mondiale antidopage (cité précédemment en note de bas de page 32), le groupe de travail a souligné que l'article 7, point f), ne constituerait pas un motif valable pour justifier le traitement des données médicales et des données relatives aux infractions dans le contexte des enquêtes antidopage, au regard de la «gravité des intrusions dans la vie privée» qui en résulteraient. Le traitement des données doit être prévu par la loi et doit satisfaire aux exigences de l'article 8, paragraphe 4 ou 5, de la directive.

[88] Voir l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité en note de bas de page 9 ci-dessus) et l'avis 06/2013 du groupe de travail «Article 29» sur la réutilisation des informations du secteur public (ISP) et des données ouvertes, adopté le 5.6.2013 (WP 207).

(par exemple, pour des travaux de recherche ou dans un souci de transparence et de responsabilité).

iii) La façon dont les données sont traitées

L'analyse d'impact au sens large peut consister notamment à examiner si les données ont été publiées ou rendues accessibles par quelque autre moyen à un grand nombre de personnes, ou si des volumes considérables de données à caractère personnel sont traités ou combinés avec d'autres données (par exemple, en cas d'établissement de profils, à des fins commerciales, judiciaires, ou autres). Le traitement à grande échelle de données apparemment anodines et leur combinaison avec d'autres données peuvent parfois permettre des inférences à propos de données plus sensibles, comme l'a montré le scénario 3 ci-dessus, qui illustrait la mise en relation des habitudes de consommation de pizzas avec les primes d'assurance santé.

Outre le fait qu'elle risque de permettre le traitement de données plus sensibles, ce genre d'analyse peut aussi conduire à des prévisions saugrenues, inattendues, voire inexactes concernant, par exemple, le comportement ou la personnalité des individus concernés. Selon la nature et l'incidence de ces prévisions, l'intrusion dans la vie privée de ces personnes peut être considérable[89].

Le groupe de travail a aussi insisté, dans un avis précédent, sur les risques inhérents à certaines solutions de sécurité (notamment les pare-feu, antivirus ou anti-spam), susceptibles de donner lieu au déploiement à grande échelle de l'analyse des paquets en profondeur , ce qui peut influencer sensiblement l'appréciation de l'équilibre des droits[90].

En général, plus l'incidence du traitement pourrait se révéler négative ou incertaine, moins il est probable que ce traitement sera jugé légitime au regard du critère de mise en balance. Dans ce contexte, il sera certainement utile d'examiner s'il n'existe pas d'autres méthodes, aux conséquences moins négatives pour la personne concernée, pour atteindre les objectifs poursuivis par le responsable du traitement. Si nécessaire, des analyses d'impact relatives à la vie privée et à la protection des données peuvent servir à déterminer si cette possibilité peut être envisagée.

iv) Attentes raisonnables de la personne concernée

Les attentes raisonnables de la personne concernée quant à l'utilisation et à la divulgation des données sont aussi très pertinentes à cet égard. Ainsi qu'il a été indiqué à propos de l'analyse du principe de limitation de la finalité[91], il est «important d'examiner si le statut du responsable du traitement des données[92], la nature de la relation ou du service fourni[93] ou les

[89] Voir la section III.2.5 et l'annexe 2 (gros volumes de données et données ouvertes) de l'avis sur la limitation de la finalité (cité précédemment en note de bas de page 9).
[90] Voir la section 3.1 de l'avis 1/2009 du groupe de travail «Article 29» concernant les propositions modifiant la directive 2002/58/CE sur la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques») (WP 159).
[91] Voir les pages 24 et 25 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note de bas de page 9).
[92] «Comme, par exemple, un avocat ou un médecin».
[93] «Comme, par exemple, des services d'informatique en nuage pour la gestion des documents personnels, des services de messagerie électronique, des agendas électroniques, des liseuses équipées de fonctions de prise de notes et diverses applications de journal qui peuvent contenir des informations très personnelles.»

obligations légales ou contractuelles applicables (ou d'autres engagements pris lors de la collecte) pourraient susciter des attentes raisonnables de confidentialité plus stricte et de limitations plus strictes en cas d'utilisation ultérieure». En général, plus le contexte de la collecte est spécifique et restrictif, plus les limitations susceptibles de s'appliquer à l'utilisation des données sont strictes. Là encore, il est nécessaire de tenir compte des circonstances factuelles, plutôt que de s'appuyer simplement sur des clauses imprimées en petits caractères.

v) Statut du responsable du traitement des données et de la personne concernée

Le statut de la personne concernée et du responsable du traitement des données est aussi pertinent pour apprécier l'incidence du traitement. Selon que le responsable du traitement des données est un individu ou une petite organisation, une grande multinationale, ou un organisme du secteur public et en fonction des circonstances, le rapport de force avec la personne concernée peut être plus ou moins grand. Une grande multinationale dispose, par exemple, de ressources et d'un pouvoir de négociation considérables vis-à-vis d'une personne concernée, à titre individuel, et elle peut par conséquent être à même d'imposer ce qu'elle considère comme son «intérêt légitime» à la personne concernée, surtout si l'entreprise occupe une position dominante sur le marché. En l'absence de contrôle, ce genre de situation peut tourner au désavantage des personnes concernées. De même que les lois sur la protection des consommateurs et sur la concurrence contribuent à éviter que ce pouvoir ne soit pas utilisé à bon escient, le droit applicable en matière de protection des données pourrait aussi jouer un rôle important en matière de prévention des atteintes aux droits et aux intérêts des personnes concernées.

D'un autre côté, le statut de la personne concernée a aussi son importance. Si, en principe, il y a lieu d'appliquer le critère de mise en balance par rapport à un individu moyen, certaines situations spécifiques appellent plutôt une approche au cas par cas: par exemple, il serait pertinent de prendre en considération le fait que la personne concernée est un enfant[94] ou appartient à une catégorie de population plus vulnérable qui requiert une protection spéciale, comme, par exemple, les malades mentaux, les demandeurs d'asile ou les personnes âgées. Bien sûr, il faut aussi examiner si la personne concernée est un salarié, un étudiant, un patient ou s'il existe de quelque autre façon un déséquilibre dans la relation entre la position de la personne concernée et celle du responsable du traitement. Il est important d'apprécier l'effet concret du traitement sur les individus en particulier.

Enfin, il faut souligner que toutes les incidences négatives sur les personnes concernées ne «pèsent» pas du même poids dans la balance. La finalité du critère de mise en balance prévu par l'article 7, point f), n'est pas d'éviter toute incidence négative sur la personne concernée. Il s'agit plutôt de prévenir une incidence disproportionnée. La différence est cruciale. Par exemple, la publication dans un journal d'un article fondé sur une enquête sérieuse et sur des faits précis à propos de soupçons de corruption au sein de l'administration peut être préjudiciable à la réputation des fonctionnaires concernés et peut avoir des conséquences

[94] Voir l'avis 2/2009 du groupe de travail «Article 29» sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles), adopté le 11.2.2009 (WP 160). Cet avis insiste sur la vulnérabilité spécifique de l'enfant et, dans le cas où l'enfant est représenté, sur la nécessité de prendre en compte son intérêt propre et non celui de ses représentants.

importantes, notamment l'atteinte à la réputation, la défaite aux élections, ou l'emprisonnement, mais elle pourrait néanmoins être fondée en vertu de l'article 7, point f)[95].

c) Bilan provisoire

Lors de la mise en balance des intérêts et des droits en jeu, comme décrit précédemment, les mesures prises par le responsable du traitement pour se conformer aux obligations générales que lui impose la directive, notamment en termes de proportionnalité et de transparence, contribueront grandement à garantir le respect par le responsable du traitement des données des exigences énoncées à l'article 7, point f). Un respect absolu de ces conditions devrait signifier que l'incidence sur les individus est réduite, qu'une ingérence dans la poursuite des intérêts et l'exercice des droits ou libertés fondamentaux des personnes concernées est *moins probable* et qu'il est, par conséquent, *plus probable* que l'article 7, point f), puisse être invoqué par le responsable du traitement des données. Cela devrait encourager les responsables du traitement à mieux se conformer à toutes les dispositions horizontales de la directive[96].

Cela ne veut pas dire, cependant, que le respect de ces exigences horizontales sera toujours, en soi, suffisant pour garantir une base juridique en application de l'article 7, point f). Si tel était le cas, en effet, l'article 7, point f), serait superflu ou créerait une faille privant de sa signification l'article 7 tout entier, qui prévoit que le traitement doit se fonder sur une base juridique précise adéquate.

C'est pourquoi il importe d'approfondir l'évaluation lors de l'exercice de mise en balance lorsque l'analyse préliminaire ne permet pas d'établir clairement dans quel sens penche la balance. Le responsable du traitement peut envisager d'introduire des mesures supplémentaires, qui vont au-delà du respect des dispositions horizontales de la directive, afin de contribuer à réduire toute incidence indue du traitement sur les personnes concernées.

Ces mesures supplémentaires peuvent comprendre, par exemple, la mise à disposition d'un mécanisme accessible et facile à utiliser offrant aux personnes concernées la possibilité inconditionnelle de s'opposer au traitement. Dans certains cas (mais pas toujours), de telles mesures peuvent contribuer à faire pencher la balance et à permettre le traitement en vertu de l'article 7, point f), tout en protégeant aussi les droits et les intérêts des personnes concernées.

d) Garanties supplémentaires mises en place par le responsable du traitement

Comme expliqué ci-dessus, la façon dont le responsable du traitement appliquerait des mesures appropriées pourrait, dans certaines situations, contribuer à «faire pencher la balance». C'est l'évaluation dans son ensemble qui déterminera si le résultat est acceptable ou non. Plus l'incidence sur la personne concernée est significative, plus il convient de prêter attention aux garanties pertinentes.

[95] Comme expliqué précédemment, les éventuelles dérogations pertinentes pour le traitement à des fins de journalisme en vertu de l'article 9 de la directive doivent aussi être prises en compte.
[96] À propos du rôle important du «respect des dispositions horizontales», voir aussi la page 54 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité, cité en note de bas de page 9, ci-dessus.

À titre d'exemple, les mesures concernées peuvent inclure, entre autres, une limitation stricte du volume de données collectées, ou la suppression immédiate des données après utilisation. Si certaines de ces mesures sont peut-être déjà obligatoires au titre de la directive, elles sont souvent modulables et laissent aux responsables du traitement une certaine latitude pour assurer une meilleure protection des personnes concernées. Par exemple, le responsable du traitement peut collecter moins de données, ou fournir des informations complémentaires par rapport à ce que prévoient spécifiquement les articles 10 et 11 de la directive.

Dans certains autres cas, les garanties ne sont pas *explicitement* requises par la directive, mais pourraient bien figurer à l'avenir dans le règlement proposé, ou elles ne sont exigées que dans des situations particulières. Il peut s'agir, par exemple:

- de mesures techniques et organisationnelles garantissant que les données ne peuvent servir à la prise de décisions ou de mesures à l'endroit des individus («séparation fonctionnelle», comme c'est souvent le cas dans le contexte de la recherche);
- d'un large recours aux techniques d'anonymisation;
- de l'agrégation de données;
- de technologies renforçant la protection de la vie privée, de la prise en compte du respect de la vie privée dès la conception, d'analyses d'impact relatives à la vie privée et à la protection des données;
- d'une transparence accrue;
- d'un droit d'opposition général et inconditionnel;
- de la portabilité des données et d'autres mesures connexes destinées à renforcer le pouvoir des personnes concernées.

Le groupe de travail observe qu'en ce qui concerne certaines questions-clés, notamment la séparation fonctionnelle et les techniques d'anonymisation, certaines orientations ont déjà été données dans les parties correspondantes de ses avis sur la limitation de la finalité, sur les données ouvertes et sur les techniques d'anonymisation[97].

En ce qui concerne la pseudonymisation et le chiffrement, le groupe de travail tient à souligner que, si les données ne sont pas directement identifiables, cela n'a, en soi, aucune incidence sur l'appréciation de la légitimité du traitement: il ne faudrait pas croire que ces techniques permettent de rendre légitime un traitement qui ne l'est pas[98].

Cependant, la pseudonymisation et le chiffrement, comme toutes les autres mesures techniques et organisationnelles introduites pour protéger les informations personnelles, joueront un rôle dans l'évaluation de l'incidence potentielle du traitement sur la personne concernée et, de ce fait, pourront dans certains cas contribuer à faire pencher la balance en faveur du responsable du traitement. L'utilisation de formes moins risquées de traitement des données à caractère personnel (par exemple, le chiffrement des données à caractère personnel

[97] Voir les sections III.2.3, III.2.5 et l'annexe 2 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité, cité précédemment en note de bas de page 9, à propos du traitement ultérieur à des fins de recherche historique, statistique et scientifique, des gros volumes de données et des données ouvertes; voir aussi les sections concernées de l'avis 06/2013 du groupe de travail «Article 29» sur les données ouvertes (cité en note de bas de page 88 ci-dessus) et de l'avis 5/2014 sur les techniques d'anonymisation.

[98] Voir sur ce point les amendements votés par la commission LIBE dans le rapport final de la commission LIBE, et en particulier l'amendement 15 sur le considérant 38, qui met en relation la pseudonymisation et les attentes légitimes de la personne concernée.

en vue de leur stockage ou de leur transit, ou le fait de rendre les données à caractère personnel moins directement et moins aisément identifiables) devrait généralement réduire les risques d'interférence avec l'intérêt ou les droits et libertés fondamentaux des personnes concernées.

À propos de ces garanties – et de l'appréciation générale résultant de la mise en balance – le groupe de travail souhaite mettre en avant trois aspects spécifiques qui jouent souvent un rôle crucial dans le contexte de l'article 7, point f):

- la relation entre le critère de mise en balance, la transparence et le principe de responsabilité;
- le droit de la personne concernée de s'opposer au traitement, et au-delà de cette opposition, la possibilité de refuser sans avoir à donner de justification; et
- le renforcement du pouvoir des personnes concernées: portabilité des données et disponibilité de mécanismes fonctionnels permettant à la personne concernée d'accéder à ses propres données, de les modifier, de les effacer, de les transférer, ou de les traiter ultérieurement d'une autre façon (ou de confier à des tiers leur traitement ultérieur).

Compte tenu de leur importance, ces sujets seront examinés dans des sections séparées.

III.3.5. Responsabilité et transparence

Tout d'abord, avant qu'une opération de traitement en vertu de l'article 7, point f), puisse avoir lieu, il appartient au responsable du traitement d'apprécier s'il a un intérêt légitime, si le traitement est nécessaire à cet intérêt légitime et si, dans le cas envisagé, les intérêts et les droits des personnes concernées ne prévalent pas sur cet intérêt.

C'est pourquoi l'article 7, point f), repose sur le principe de responsabilité. Le responsable du traitement doit au préalable procéder à une analyse minutieuse et effective, fondée sur les circonstances factuelles particulières plutôt que sur une réflexion abstraite, en tenant compte aussi des attentes raisonnables des personnes concernées. Une bonne pratique consisterait, éventuellement, à documenter ce travail d'analyse d'une manière suffisamment détaillée et transparente pour permettre la vérification de l'application complète et correcte du critère de mise en balance par les parties intéressées, notamment les personnes concernées et les autorités chargées de la protection des données, et enfin par les tribunaux, si besoin est.

Le responsable du traitement définira d'abord l'intérêt légitime qu'il poursuit et appliquera ensuite le critère de mise en balance, mais il ne s'agit pas là nécessairement d'une appréciation définitive: si, en réalité, l'intérêt poursuivi n'est pas celui qui a été spécifié par le responsable du traitement ou si la définition de l'intérêt n'est pas suffisamment détaillée, il faut réévaluer la mise en balance, sur la base de l'intérêt réel, qui sera déterminé soit par une autorité chargée de la protection des données soit par un tribunal[99]. Comme dans le cas d'autres aspects essentiels de la protection des données, par exemple l'identification du responsable du traitement des données ou la spécification de la finalité[100], ce qui importe, c'est la réalité que recouvre toute affirmation faite par le responsable du traitement.

[99] Par exemple, à la suite d'une plainte ou d'une opposition exprimée en vertu de l'article 14.
[100] Voir les avis cités en note de bas de page 9.

La notion de responsabilité est étroitement liée à celle de transparence. Afin de permettre aux personnes concernées de faire valoir leurs droits et, plus généralement, aux parties prenantes d'exercer un contrôle public, le groupe de travail recommande que les responsables du traitement expliquent aux personnes concernées d'une manière claire et conviviale les raisons qu'ils ont de penser que l'intérêt ou les droits et libertés fondamentaux des personnes concernées ne prévalent pas sur l'intérêt qu'ils poursuivent et leur présentent aussi les garanties qu'ils ont prises pour protéger les données à caractère personnel, y compris, le cas échéant, le droit de s'opposer au traitement[101].

À cet égard, le groupe de travail souligne que la législation en matière de protection des consommateurs et, en particulier, les lois qui protègent les consommateurs contre les pratiques commerciales déloyales revêtent aussi une grande importance ici.

Si un responsable du traitement dissimule, dans une clause contractuelle formulée en termes juridiques techniques et imprimée en petits caractères, des informations importantes concernant une utilisation ultérieure inattendue des données, cette pratique peut tomber sous le coup des règles de protection des consommateurs relatives aux clauses abusives (notamment l'interdiction des «clauses surprenantes») et, par ailleurs, elle ne satisfait ni aux conditions de l'article 7, point a), qui supposent un consentement valide et informé, ni aux exigences de l'article 7, point f), du point de vue des attentes raisonnables de la personne concernée et d'un équilibre globalement acceptable des intérêts. Cela soulèverait bien sûr aussi des questions quant à la conformité avec l'article 6, qui requiert un traitement loyal et licite des données à caractère personnel.

Par exemple, dans un certain nombre de cas, les utilisateurs de services en ligne «gratuits», comme les moteurs de recherche, les messageries électroniques, les médias sociaux, le stockage de fichiers ou d'autres applications en ligne ou mobile, ne sont pas pleinement conscients de la mesure dans laquelle leur activité est enregistrée et analysée afin d'engendrer de la valeur pour le prestataire de services et, de ce fait, ils ne se préoccupent pas des risques que cela comporte.

Afin de renforcer le pouvoir des personnes concernées dans ces situations, une condition préalable nécessaire – mais nullement suffisante en elle-même – consiste d'abord à préciser que les services ne sont pas gratuits et que ce sont les données à caractère personnel des consommateurs qui servent de moyen de paiement[102]. Les conditions et les garanties sous réserve desquelles les données peuvent être utilisées doivent aussi être clairement énoncées

[101] Comme expliqué en page 46 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note de bas de page 9), en cas d'établissement de profil et d'automatisation du processus décisionnel, «afin de garantir la transparence, les personnes concernées/consommateurs devraient avoir accès à leurs "profils", ainsi qu'à la logique du processus de décision (algorithme) qui aboutit à l'élaboration du profil. Autrement dit: les organisations devraient divulguer leurs critères décisionnels. C'est une garantie cruciale, qui revêt encore plus d'importance dans le monde des gros volumes de données». Le fait qu'une organisation assure ou non cette transparence est un facteur très pertinent à prendre également en considération dans l'exercice de mise en balance.

[102] Concernant d'autres garanties possibles dans les situations de plus en plus courantes où les consommateurs paient au moyen de leurs données personnelles, voir la section III.3.6, et en particulier, les pages 53 et 54, sous les rubriques «Alternatives respectueuses de la protection des données aux services en ligne "gratuits"» et «Portabilité des données, "midata" et questions connexes».

dans chaque cas pour assurer la validité du consentement requis par l'article 7, point a), ou un équilibre favorable au regard de l'article 7, point f).

III.3.6. Le droit d'opposition et au-delà

a) Le droit d'opposition en vertu de l'article 14 de la directive

Les points e) et f) de l'article 7 ont ceci de particulier que, s'ils reposent principalement sur une appréciation objective des intérêts et des droits en jeu, ils font aussi intervenir l'autodétermination de la personne concernée en lui reconnaissant un droit d'opposition[103]: pour ces deux motifs, au moins, l'article 14, point a), de la directive prévoit que («sauf en cas de disposition contraire du droit national») la personne concernée peut «s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement». Il ajoute que si cette opposition est justifiée, le traitement des données doit cesser.

En principe, selon la législation actuelle, la personne concernée devra donc démontrer qu'il existe «des raisons prépondérantes et légitimes» d'arrêter de traiter ses données à caractère personnel [article 14, point a)], sauf dans le cas d'activités de prospection, où l'opposition n'a pas à être justifiée [article 14, point b)].

Il ne faut pas y voir une contradiction avec le critère de mise en balance visé à l'article 7, point f), qui est appliqué a priori: cette disposition vient plutôt compléter la mise en balance, en ce sens que, lorsque le traitement est autorisé à la suite d'une évaluation raisonnable et objective des différents droits et intérêts en jeu, la personne concernée dispose encore d'une possibilité *supplémentaire* de marquer son opposition, pour des motifs liés à sa situation particulière. Il faudra alors procéder à une nouvelle appréciation en tenant compte des arguments spécifiques avancés par la personne concernée. Cette nouvelle appréciation peut, en principe, faire encore l'objet d'une vérification par une autorité chargée de la protection des données ou par les tribunaux.

b) Au-delà de l'opposition: le rôle du refus comme garantie supplémentaire

Le groupe de travail souligne que, même si le droit reconnu par l'article 14, point a), est subordonné à la présentation d'une justification par la personne concernée, rien n'empêche le responsable du traitement de proposer une option de refus qui serait plus large, et qui n'exigerait aucune démonstration supplémentaire d'un intérêt légitime (prépondérant ou autre) de la part de la personne concernée. Ce droit inconditionnel ne devrait pas se fonder sur la situation spécifique des personnes concernées.

En effet, surtout dans les cas douteux où il est difficile de trouver un équilibre, un mécanisme bien conçu et fonctionnel permettant de refuser le traitement, sans donner nécessairement aux personnes concernées tous les éléments qui satisferaient à la condition de consentement valide

[103] Ce droit d'opposition ne doit pas être confondu avec le consentement prévu par l'article 7, point a), que le responsable du traitement des données doit obtenir pour pouvoir traiter les données.. Dans le contexte de l'article 7, point f), le responsable du traitement peut traiter les données sous réserve de certaines conditions et garanties, aussi longtemps que la personne concernée ne s'y est pas opposée. En ce sens, le droit d'opposition peut plutôt être considéré comme une forme particulière d'option de refus. Voir plus de détails dans l'avis 15/2011 du groupe de travail «Article 29» sur la définition du consentement (cité en note de bas de page 2).

visée à l'article 7, point a), pourrait jouer un rôle important pour préserver les droits et les intérêts des personnes concernées.

Pour ce faire, il est nécessaire d'adopter une approche nuancée, qui distingue entre les cas où un consentement préalable, conforme à l'article 7, point a), est requis et les cas où un mécanisme fonctionnel permettant de refuser le traitement (combiné éventuellement avec d'autres mesures supplémentaires) peut contribuer à protéger les personnes concernées au regard de l'article 7, point f).

Plus le mécanisme de l'option de refus est largement applicable et facile à exercer, plus il contribuera à faire pencher la balance en faveur du traitement et à permettre l'invocation de l'article 7, point f), comme fondement juridique.

Illustration: l'évolution de l'approche de la prospection directe

Afin d'illustrer la distinction qu'il convient d'établir entre les cas où un consentement au titre de l'article 7, point a), est requis et les cas où une option de refus pourrait servir de garantie au regard de l'article 7, point f), il est utile de prendre l'exemple de la prospection directe, pour laquelle il existe déjà une disposition spécifique prévoyant la possibilité de refuser le traitement, à l'article 14, point b), de la directive. Pour tenir compte des nouvelles avancées technologiques, cette disposition a été complétée ultérieurement par des dispositions spécifiques de la directive «vie privée et communications électroniques»[104].

Conformément à l'article 13 de la directive «vie privée et communications électroniques», pour certains types – plus intrusifs – d'activités de prospection directe (comme la prospection par courrier électronique et les automates d'appel), le consentement est de rigueur. À titre d'exception, dans le cadre d'une relation client-fournisseur existante, où un responsable du traitement cherche à promouvoir ses propres produits ou services «similaires», il est suffisant de prévoir une possibilité de refus (inconditionnelle), sans justification à fournir.

Les technologies ont évolué, nécessitant des solutions similaires, relativement simples, qui obéissent à une logique analogue pour les nouvelles pratiques de prospection.

Premièrement, la façon dont le matériel de prospection est diffusé a évolué: au lieu de simples courriers électroniques arrivant dans les boîtes aux lettres, des publicités comportementales ciblées apparaissent aussi désormais sur les écrans de smartphones et d'ordinateurs. Dans un proche avenir, la publicité pourrait être intégrée dans des objets intelligents connectés à l'internet des objets.

Deuxièmement, les publicités deviennent toujours plus spécifiquement ciblées: au lieu de se fonder sur de simples profils de clients, elles tirent parti du traçage des activités des consommateurs qui sont de plus en plus souvent conservées en ligne et hors ligne et analysées au moyen de méthodes automatisées plus élaborées[105].

[104] À propos de l'article 13 de la directive «vie privée et communications électroniques», voir aussi la section III.2.4 de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note de bas de page 9).
[105] Voir la section III.2.5 et l'annexe 2 (sur les gros volumes de données et les données ouvertes) de l'avis 3/2013 du groupe de travail «Article 29» sur la limitation de la finalité (cité précédemment en note de bas de page 9).

Du fait de ces évolutions, l'objectif de l'exercice de mise en balance est désormais différent: la question ne concerne plus la liberté d'expression commerciale, mais principalement l'intérêt économique des entreprises à mieux connaître leurs clients grâce au traçage et à la surveillance de leurs activités en ligne et hors ligne, qui devraient être mis en balance avec les droits (fondamentaux) de ces personnes au respect de leur vie privé et à la protection de leurs données à caractère personnel et avec leur intérêt à ne pas faire l'objet d'une surveillance indue.

Ce changement de modèle d'entreprise dominant et la valorisation des données à caractère personnel en tant qu'actif pour les sociétés commerciales expliquent l'exigence récente d'un consentement dans ce contexte, conformément à l'article 5, paragraphe 3, et à l'article 13 de la directive «vie privée et communications électroniques».

Il y a donc des règles spécifiques différentes, selon la forme de prospection, notamment:

- le droit inconditionnel de s'opposer au traitement à des fins de prospection (conçu pour le contexte traditionnel des envois postaux, et pour la promotion de produits similaires) conformément à l'article 14, point b), de la directive; l'article 7, point f), pourrait être invoqué comme fondement juridique dans ce cas;
- le consentement exigé en vertu de l'article 13 de la directive «vie privée et communications électroniques» pour la prospection au moyen d'automates d'appel, de télécopieurs, de messages texte et de courriers électroniques (sous réserve des exceptions prévues)[106], et l'application de fait de l'article 7, point a), de la directive sur la protection des données.
- le consentement exigé en vertu de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques» [et de l'article 7, point a), de la directive sur la protection des données] pour la publicité comportementale fondée sur des techniques de traçage comme le stockage d'informations au moyen de cookies dans l'équipement terminal des utilisateurs[107].

Si les fondements juridiques applicables sont clairs en ce qui concerne l'article 5, paragraphe 3, et l'article 13 de la directive «vie privée et communications électroniques», toutes les formes de prospection ne sont pas couvertes et il serait souhaitable de pouvoir disposer d'orientations quant aux situations qui requièrent un consentement au titre de l'article 7, point a), et aux situations dans lesquelles un équilibre est atteint au regard de l'article 7, point f), grâce notamment à la possibilité de refuser le traitement.

À cet égard, il est utile de rappeler l'avis du groupe de travail «Article 29» sur la limitation de la finalité, où il est expressément indiqué que «si une organisation souhaite spécifiquement analyser ou prédire les préférences personnelles, le comportement et les attitudes de clients individuels, qui serviront ensuite à guider des "mesures ou décisions" prises à l'égard de ces clients [...] un consentement préalable libre, spécifique, informé et indubitable devrait presque toujours être requis, faute de quoi l'utilisation ultérieure ne pourra pas être jugée compatible. Ce consentement devrait surtout être requis, par exemple, pour le traçage et le profilage à des fins de prospection directe, de publicité comportementale, de courtage en informations, de

[106] Voir aussi l'article 13, paragraphe 3, de la directive «vie privée et communications électroniques», qui laisse aux États membres le choix entre les options de consentement et de refus pour la prospection directe passant par d'autres moyens.
[107] Concernant l'application de cette disposition, voir l'avis 2/2010 du groupe de travail «Article 29» sur la publicité comportementale en ligne (WP 171).

publicités fondées sur la localisation ou d'étude de marché numérique fondée sur le traçage[108].»

Alternatives respectueuses de la protection des données aux services en ligne «gratuits»

Dans le cas où les consommateurs qui souscrivent à des services en ligne «gratuits» «paient» en fait ces services en autorisant l'utilisation de leurs données à caractère personnel, un moyen de contribuer à une évaluation favorable à l'issue de la mise en balance – ou à la conclusion que le consommateur a vraiment été libre de son choix et a donc donné un consentement valide au titre de l'article 7, point a) – consisterait, pour le responsable du traitement, à proposer aussi une autre version de ses services, où les «données à caractère personnel» ne serviraient pas à des fins de prospection.

Tant que ces autres services ne sont pas disponibles, il est plus difficile de prétendre qu'un consentement valide (donné librement) a été obtenu au titre de l'article 7, point a), du simple fait de l'utilisation des services gratuits, ou que la balance penche en faveur du responsable du traitement au regard de l'article 7, point f).

Les considérations présentées ci-dessus soulignent le rôle important que des garanties supplémentaires, et notamment un mécanisme fonctionnel permettant de refuser le traitement, peuvent jouer pour modifier le bilan provisoire. Parallèlement, elles donnent aussi à penser que dans certains cas, l'article 7, point f), ne peut pas être invoqué comme motif justifiant le traitement et que les responsables du traitement doivent obtenir un consentement valide au titre de l'article 7, point a) – ou satisfaire à quelque autre condition énoncée par la directive – pour que le traitement puisse avoir lieu.

Portabilité des données, «midata» et questions connexes

Parmi les garanties supplémentaires qui pourraient contribuer à faire pencher la balance, il convient de prêter une attention particulière à la portabilité des données et aux mesures connexes, qui peuvent se révéler de plus en plus pertinentes dans un environnement en ligne. Le groupe de travail «Article 29» rappelle son avis sur la limitation de la finalité, où il a souligné que «dans de nombreuses situations, des garanties comme le fait de permettre aux personnes concernées/consommateurs d'accéder directement à leurs données dans un format portable, convivial et lisible par machine peuvent contribuer à renforcer leur pouvoir et à rectifier le déséquilibre économique entre les grandes entreprises, d'un côté, et les personnes concernées/consommateurs, de l'autre. Cela permettrait aussi aux individus de "partager les richesses" créées par les gros volumes de données et inciterait les développeurs à proposer des fonctionnalités et des applications complémentaires à leurs utilisateurs[109]».

[108] Voir l'annexe II (sur les gros volumes de données et les données ouvertes) de l'avis (cité en note de bas de page 9, ci-dessus), page 45.

[109] «Voir des initiatives comme "midata" au Royaume-Uni, qui reposent sur le principe-clé selon lequel les données devraient être restituées aux consommateurs. Le programme "midata" est une initiative volontaire, qui devrait progressivement offrir aux consommateurs un accès renforcé à leurs données personnelles dans un format électronique portable. L'idée maîtresse est que les consommateurs devraient aussi tirer profit des gros volumes de données en accédant à leurs propres informations pour être en mesure de faire de meilleurs choix. Voir aussi les initiatives "Green button" qui permettent aux consommateurs d'accéder à des informations sur leur propre consommation énergétique.» Pour plus d'information sur des initiatives au Royaume-Uni et en France, voir http://www.midatalab.org.uk/ et http://mesinfos.fing.org/.

La disponibilité de mécanismes fonctionnels permettant aux personnes concernées d'accéder à leurs propres données, de les modifier, de les effacer, de les transférer, ou de les traiter ultérieurement d'une autre façon (ou de confier à des tiers leur traitement ultérieur) renforcera le pouvoir des personnes concernées et leur donnera la possibilité de tirer un meilleur parti des services numériques. En outre, cela peut favoriser un environnement de marché plus concurrentiel, en permettant aux clients de changer plus aisément de fournisseurs (par exemple, en matière de services bancaires en ligne ou de fournisseurs d'énergie sur un réseau électrique intelligent). Enfin, cela peut aussi contribuer au développement d'autres services à valeur ajoutée par des tiers qui pourront accéder aux données des consommateurs à la demande de ces derniers et avec leur consentement. Dans cette perspective, la portabilité des données est donc une bonne chose non seulement pour la protection des données, mais aussi pour la concurrence et la protection des consommateurs[110].

IV. Observations finales

Dans le présent avis, le groupe de travail a analysé les critères légitimant le traitement des données énoncés dans l'article 7 de la directive. Au-delà des orientations proposées pour l'interprétation et l'application pratiques de l'article 7, point f), dans le cadre juridique actuel, son objectif est de formuler des recommandations politiques destinées à aider les décideurs dans le choix des modifications qu'ils envisagent d'apporter au cadre juridique actuel en matière de protection des données. Avant de présenter ces recommandations, les principales conclusions concernant l'interprétation de l'article 7 sont résumées ci-après.

IV.1. Conclusions

Aperçu général de l'article 7

L'article 7 dispose que le traitement de données à caractère personnel ne peut être effectué que si au moins un des six motifs juridiques énumérés à cet article existe.

Le premier motif, exposé à l'article 7, point a), porte sur le consentement de la personne concernée comme fondement légitimant le traitement. Les autres motifs, en revanche, autorisent le traitement – sous réserve de garanties – dans des situations où, indépendamment du consentement, il est approprié et nécessaire de traiter les données dans un certain contexte pour servir un intérêt légitime spécifique.

Les points b), c), d), et e) spécifient chacun un contexte particulier, dans lequel le traitement des données à caractère personnel peut être considéré comme légitime. Les conditions qui s'appliquent dans chacun de ces différents contextes requièrent une attention minutieuse, car elles déterminent la portée des différents motifs légitimant le traitement. Plus particulièrement, les critères du traitement «nécessaire à l'exécution d'un contrat», «nécessaire au respect d'une obligation légale», «nécessaire à la sauvegarde de l'intérêt vital de la personne concernée» et «nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique» sont assortis d'exigences différentes, qui ont été examinées à la section III.2.

[110] À propos du droit à la portabilité des données, voir l'article 18 du règlementproposé.

Le point f) fait référence, plus généralement, à un (quelconque) intérêt légitime poursuivi par le responsable du traitement (dans n'importe quel contexte). Cette disposition générale est, cependant, expressément subordonnée à un critère supplémentaire de mise en balance, qui requiert que l'intérêt légitime poursuivi par le responsable du traitement – ou par le ou les tiers auxquels les données sont communiquées – soit comparé avec les intérêts ou les droits fondamentaux des personnes concernées.

Rôle de l'article 7, point f)

L'article 7, point f), ne doit pas être perçu comme un fondement juridique pouvant uniquement être utilisé avec parcimonie pour combler certaines lacunes «en dernier ressort» dans des situations rares et imprévues, ou comme une dernière chance si aucun autre motif ne s'applique. Il ne doit pas non plus apparaître comme une option privilégiée, et il ne s'agit pas d'encourager indûment son utilisation parce qu'il serait considéré comme moins contraignant que les autres motifs. Il s'agit plutôt d'un moyen, tout aussi valable que l'un quelconque des autres motifs permettant de légitimer le traitement des données à caractère personnel.

Une utilisation appropriée de l'article 7, point f), dans les circonstances appropriées et moyennant des garanties adéquates, permet aussi d'éviter une utilisation abusive et une invocation excessive d'autres fondements juridiques. Une évaluation appropriée de l'équilibre requis par l'article 7, point f), souvent assortie d'une possibilité de s'opposer au traitement, peut, dans d'autres cas, se substituer valablement à l'invocation inappropriée, par exemple, du motif du «consentement» ou du caractère «nécessaire à l'exécution d'un contrat». Dans cette optique, l'article 7, point f), présente des garanties complémentaires par rapport aux autres motifs prédéfinis. Il ne doit donc pas être considéré comme «le maillon faible» ou comme une porte ouverte à la légitimation de tout traitement de données qui ne relève pas d'un des autres fondements juridiques.

Intérêt légitime poursuivi par le responsable du traitement / intérêt ou droits fondamentaux de la personne concernée

La notion d'«intérêt» désigne, au sens large, l'enjeu poursuivi par le responsable du traitement, ou le bénéfice qu'il tire du traitement – ou que la société pourrait en tirer. Il peut être impérieux, manifeste ou plus controversé. Les situations auxquelles renvoie l'article 7, point f), peuvent donc aller de l'exercice de droits fondamentaux ou de la protection d'intérêts personnels ou sociaux importants à d'autres contextes moins évidents, voire problématiques.

Pour être considéré comme «légitime» et pertinent au sens de l'article 7, point f), l'intérêt doit être licite, c'est-à-dire conforme au droit applicable dans l'Union et dans le pays concerné. Il doit aussi être exprimé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée. Enfin, il doit constituer un intérêt réel et présent, c'est-à-dire qu'il ne doit pas être hypothétique.

Si le responsable du traitement, ou le tiers auquel les données doivent être communiquées, poursuit un tel intérêt légitime, il ne s'ensuit pas nécessairement que l'article 7, point f), peut être invoqué comme fondement juridique justifiant le traitement. La possibilité d'invoquer l'article 7, point f), dépendra du résultat de la mise en balance qui suit. Le traitement doit aussi être «nécessaire à la réalisation de l'intérêt légitime» poursuivi par le responsable du traitement ou – en cas de communication des données – par le tiers. Des moyens plus

respectueux de la vie privée susceptibles de servir à la même finalité devraient donc toujours être préférés.

La notion d'«intérêt» des personnes concernées est définie encore plus largement, puisqu'elle n'exige pas d'élément de «légitimité». Si le responsable du traitement ou le tiers peut poursuivre n'importe quel intérêt, pour autant qu'il ne soit pas illégitime, la personne concernée devrait aussi pouvoir s'attendre à ce que ses intérêts, quelle qu'en soit la nature, soient pris en considération et mis en balance avec ceux du responsable du traitement, pour autant qu'ils soient pertinents dans le champ d'application de la directive.

Application du critère de mise en balance

Dans son interprétation du champ d'application de l'article 7, point f), le groupe de travail entend proposer une approche équilibrée, qui garantit aux responsables du traitement des données la souplesse nécessaire dans les situations où les personnes concernées ne subissent aucune incidence indue, tout en offrant aux personnes concernées une sécurité juridique et des garanties suffisantes pour empêcher un usage abusif de cette disposition ouverte.

Pour appliquer le critère de mise en balance, il importe, tout d'abord, d'examiner la nature et la source de l'intérêt légitime, ainsi que la nécessité du traitement pour la poursuite de cet intérêt, d'une part, et l'incidence sur les personnes concernées, d'autre part. Cette appréciation initiale devrait tenir compte des mesures, en matière de transparence ou de collecte limitée des données, par exemple, que le responsable du traitement prévoit d'adopter pour se conformer à la directive.

Après une analyse et un examen attentif de tous les aspects du problème, un bilan provisoire peut être établi: une conclusion préliminaire peut être tirée afin de déterminer si l'intérêt légitime poursuivi par le responsable du traitement prévaut sur les droits et les intérêts des personnes concernées. Il peut cependant y avoir des cas où le résultat de la mise en balance n'est pas clair et où il subsiste un doute quant à la question de savoir si l'intérêt légitime du responsable du traitement (ou du tiers) prévaut et si le traitement peut se fonder sur l'article 7, point f).

C'est pourquoi il importe de procéder à une évaluation complémentaire dans le cadre de l'exercice de mise en balance. À ce stade, le responsable du traitement peut envisager d'introduire d'autres mesures, qui vont au-delà du respect des dispositions horizontales de la directive, afin de contribuer à protéger les personnes concernées. Ces mesures supplémentaires peuvent comprendre, par exemple, la mise en place d'un mécanisme fonctionnel et aisément accessible garantissant aux personnes concernées la possibilité inconditionnelle de refuser le traitement.

Facteurs-clés à prendre en considération pour appliquer le critère de mise en balance

Compte tenu de ce qui précède, les facteurs qui peuvent utilement être pris en considération lors de l'application du critère de mise en balance sont:

- la nature et la source de l'intérêt légitime, et notamment:

  - si le traitement des données est nécessaire à l'exercice d'un droit fondamental, ou

- s'il est d'intérêt public à quelque autre égard ou bénéficie d'une reconnaissance sociale, culturelle ou légale/réglementaire dans la collectivité concernée;

- l'incidence sur les personnes concernées, et notamment:

  - la nature des données, comme le fait que le traitement porte ou non sur des données qui peuvent être considérées comme sensibles ou qui ont été obtenues à partir de sources publiquement accessibles;
  - la façon dont les données sont traitées, y compris si elles ont été publiées ou rendues accessibles par quelque autre moyen à un grand nombre de personnes, ou si des volumes considérables de données à caractère personnel sont traités ou combinés avec d'autres données (par exemple, en cas d'établissement de profils, à des fins commerciales, judiciaires, ou autres);
  - les attentes raisonnables de la personne concernée, en particulier à propos de l'utilisation et de la divulgation des données dans une situation donnée;
  - le statut du responsable du traitement des données et celui de la personne concernée, y compris l'équilibre des pouvoirs entre eux, ou le fait que la personne concernée soit un enfant ou appartienne à une catégorie de population plus vulnérable.

- les garanties supplémentaires destinées à prévenir toute incidence indue sur les personnes concernées, et notamment:

  - la minimisation des données (par exemple, une limitation stricte du volume de données collectées, ou la suppression immédiate des données après utilisation);
  - les mesures techniques et organisationnelles garantissant les données ne peuvent servir à la prise de décisions ou d'autres mesures à l'endroit des individus («séparation fonctionnelle»);
  - un large recours aux techniques d'anonymisation, l'agrégation des données, les technologies renforçant la protection de la vie privée, la prise en compte du respect de la vie privée dès la conception, les analyses d'impact relatives à la vie privée et à la protection des données;
  - une transparence accrue, un droit général et inconditionnel de refuser le traitement, la portabilité des données et autres mesures connexes visant à renforcer le pouvoir des personnes concernées.

Responsabilité, transparence, droit d'opposition et au-delà

À propos de ces garanties – et de l'appréciation générale résultant de la mise en balance – trois aspects spécifiques jouent souvent un rôle crucial dans le contexte de l'article 7, point f), et requièrent donc une attention spéciale:

- l'existence de mesures supplémentaires en vue d'accroître la transparence et la responsabilité et leur nécessité éventuelle ;
- le droit de la personne concernée de s'opposer au traitement, et au-delà de cette opposition, la possibilité de refuser sans avoir à donner de justification;
- le renforcement du pouvoir des personnes concernées: portabilité des données et disponibilité de mécanismes fonctionnels permettant à la personne concernée d'accéder à ses propres données, de les modifier, de les effacer, de les transférer, ou de les traiter ultérieurement d'une autre façon (ou de confier à des tiers leur traitement ultérieur).

IV. 2. Recommandations

Le libellé actuel de l'article 7, point f), de la directive est ouvert. Cette souplesse dans sa formulation laisse une marge d'interprétation considérable et a parfois conduit – ainsi que l'expérience l'a montré – à un manque de prévisibilité et de sécurité juridique. Cependant, utilisé dans le contexte approprié, et si les critères adéquats sont appliqués, comme indiqué dans le présent avis, l'article 7, point f), a un rôle essentiel à jouer en tant que fondement juridique d'un traitement légitime des données.

Le groupe de travail soutient donc l'approche adoptée actuellement à l'article 6 de la proposition de règlement, qui maintient l'équilibre des intérêts en tant que fondement juridique séparé. D'autres orientations seraient néanmoins bienvenues pour garantir une application adéquate du critère de mise en balance.

Possibilités et moyens d'apporter des précisions

Il serait essentiel que la disposition demeure suffisamment flexible et qu'elle reflète aussi bien le point de vue du responsable du traitement des données que celui de la personne concernée, ainsi que le caractère dynamique des contextes considérés. C'est pourquoi le groupe de travail est d'avis qu'il n'est pas souhaitable de faire figurer , dans le texte du règlement proposé ou dans des actes délégués, des listes détaillées et exhaustives de situations dans lesquelles un intérêt serait, de fait, qualifié de légitime. Le groupe de travail n'est pas davantage favorable à la définition de cas où l'intérêt ou le droit d'une partie devrait *en principe* ou *par présomption* prévaloir sur l'intérêt ou le droit de l'autre partie, du simple fait de la nature de cet intérêt ou de ce droit, ou parce que certaines mesures de protection ont été prises, par exemple, parce que les données ont simplement été pseudonymisées. Cela risquerait d'être à la fois trompeur et inutilement coercitif.

Plutôt que de porter des jugements définitifs sur les mérites des différents droits et intérêts, le groupe de travail insiste sur le *rôle crucial de la mise en balance* dans l'évaluation au titre de l'article 7, point f). Il est nécessaire de conserver la flexibilité du critère, mais la façon dont il est appliqué doit être plus efficace dans la pratique et doit réellement améliorer la conformité. Cela devrait se traduire par une obligation de *responsabilité renforcée* pour les responsables du traitement des données, à qui il appartient de *démontrer* que l'intérêt et les droits de la personne concernée ne prévalent pas sur leur propre intérêt.

Orientations et responsabilité

Pour ce faire, le groupe de travail recommande, dans le règlement proposé, de formuler des orientations de la manière suivante.

1) Il serait utile d'établir et d'intégrer dans un considérant une liste non exhaustive des facteurs-clés à prendre en considération lors de l'application du critère de mise en balance, comme la nature et la source de l'intérêt légitime, l'incidence sur les personnes concernées, et les garanties supplémentaires qui peuvent être mises en place par le responsable du traitement afin de prévenir toute incidence indue sur les personnes concernées. Ces garanties peuvent comprendre, entre autres:

- une séparation fonctionnelle des données, une utilisation appropriée des techniques d'anonymisation, de chiffrement et d'autre mesures techniques et organisationnelles destinées à limiter les risques potentiels pour les personnes concernées;
- mais aussi des mesures visant à garantir aux personnes concernées une transparence accrue et une plus grande liberté de choix, comme, éventuellement, la possibilité inconditionnelle de refuser le traitement, sans frais et d'une manière qui puisse être aisément et effectivement invoquée.

2) Le groupe de travail est aussi favorable à une clarification, dans le règlement proposé, de la façon dont le responsable du traitement pourrait apporter la preuve d'un [111] renforcement de sa responsabilité.

La modification des conditions dans lesquelles les personnes concernées peuvent exercer le droit d'opposition prévu à l'article 19 du règlement proposé constitue déjà un élément important du point de vue de la responsabilité. Si la personne concernée s'oppose au traitement de ses données en vertu de l'article 7, point f), il appartiendra désormais au responsable du traitement des données, en application du règlement proposé, de démontrer que son intérêt prévaut. Le groupe de travail approuve sans réserve ce renversement de la charge de la preuve, qui contribue à une obligation renforcée de responsabilité.

Si le responsable du traitement des données ne parvient pas à démontrer à la personne concernée que son intérêt prévaut dans un cas précis, cela peut avoir des conséquences plus larges sur l'ensemble du traitement, et pas uniquement à l'égard de la personne concernée qui a manifesté son opposition. Le responsable du traitement peut être amené, le cas échéant, à remettre en question ou à réorganiser le traitement, dans l'intérêt non seulement de cette personne concernée en particulier, mais aussi de toutes les autres personnes concernées qui peuvent se trouver dans une situation similaire[112].

Cette exigence est nécessaire, mais non suffisante. Afin d'assurer dès le départ la protection des personnes concernées et d'éviter que le renversement de la charge de la preuve ne soit contourné[113], il importe de prendre des mesures *avant* que le traitement ne commence, et pas uniquement au cours des procédures d'«opposition» a posteriori.

Il est donc proposé que, dès le premier stade de toute activité de traitement, plusieurs mesures soient prises par le responsable du traitement des données. Les deux premières

[111] Une telle démonstration doit demeurer raisonnable et mettre l'accent sur le résultat plutôt que sur un processus administratif.

[112] Hormis le renversement de la charge de la preuve, le groupe de travail approuve aussi le fait que le règlement proposé n'exige plus qu'une opposition soit exprimée «pour des raisons *prépondérantes* et légitimes tenant à [l]a situation particulière [de la personne concernée]». Selon le règlement proposé, l'invocation de raisons légitimes (pas nécessairement «prépondérantes») tenant à la situation particulière de la personne concernée serait suffisante. D'ailleurs, une autre option, proposée dans le rapport final de la commission LIBE, consiste aussi à abandonner l'exigence que l'opposition se rapporte à la situation particulière de la personne concernée. Le groupe de travail est favorable à cette approche en ce sens qu'il recommande que les personnes concernées puissent tirer parti de l'une ou l'autre de ces possibilités ou des deux à la fois, le cas échéant, c'est-à-dire s'opposer au traitement du fait de leur situation particulière, ou d'une manière plus générale et, dans ce dernier cas, sans avoir à fournir une justification spécifique. Voir, en ce sens, l'amendement 114 sur l'article 19, paragraphe 1, du règlement proposé dans le rapport final de la commission LIBE.

[113] Les responsables du traitement des données, par exemple, peuvent être tentés d'éviter de démontrer au cas par cas que leur intérêt prévaut, en recourant à des formulaires de justification standard, ou à rendre fastidieux l'exercice du droit d'opposition.

mesures pourraient figurer dans un considérant du règlement proposé et la troisième dans une disposition spécifique:

- Effectuer une évaluation[114], qui comprendrait les différents stades de l'analyse présentée dans le présent avis et résumée à l'annexe 1. Le responsable du traitement devrait déterminer explicitement les intérêts en jeu qui prévalent et les raisons pour lesquelles ils prévalent sur les intérêts des personnes concernées. Cette évaluation préalable ne devrait pas être trop laborieuse et devrait rester *modulable*: elle peut se limiter aux critères essentiels si l'impact du traitement sur les personnes concernées est, à première vue, insignifiant, tandis qu'elle devrait être plus approfondie si l'équilibre paraît difficile à atteindre et requiert, par exemple, l'adoption de plusieurs garanties supplémentaires. Le cas échéant – c'est-à-dire quand une opération de traitement présente des risques spécifiques pour les droits et les libertés des personnes concernées –, il conviendrait de procéder à une analyse plus complète de l'incidence sur la vie privée et la protection des données (conformément à l'article 33 du règlement proposé), dont l'évaluation au regard de l'article 7, point f), pourrait constituer une part importante.

- Documenter cette évaluation. De même que le degré de détail dans lequel doit entrer l'évaluation est *modulable*, l'ampleur du travail de documentation devrait aussi être modulable. Cela dit, certains documents de base devraient néanmoins être disponibles dans tous les cas, sauf les plus anodins, indépendamment de l'appréciation de l'incidence du traitement sur la personne concernée. C'est sur la base de ces documents que l'évaluation du responsable du traitement peut ultérieurement être vérifiée et éventuellement contestée.

- Assurer la transparence et la visibilité de ces informations auprès des personnes concernées et d'autres parties prenantes. La transparence devrait toujours être garantie à l'égard des personnes concernées et des autorités chargées de la protection des données, mais aussi, le cas échéant, de l'opinion publique en général. Pour ce qui est des personnes concernées, le groupe de travail renvoie au projet de rapport de la

[114] Cette évaluation, comme indiqué précédemment en note de bas de page 84, ne devrait pas être confondue avec une analyse d'impact complète relative à la vie privée et à la protection des données. Il n'existe pas actuellement d'orientations globales pour les évaluations d'impact au niveau européen, bien que dans certains domaines, à savoir l'identification par radiofréquence et les compteurs intelligents, plusieurs efforts louables aient été consentis pour définir une méthodologie/un cadre (et/ou un modèle) au niveau sectoriel qui pourrait s'appliquer dans toute l'Union européenne. Voir la «proposition des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID)» et le «modèle d'analyse d'impact sur la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission». Le groupe de travail a émis plusieurs avis concernant ces deux méthodologies.
De plus, certaines initiatives ont été lancées en vue de définir une méthodologie d'analyse d'impact sur la protection des données, dont les efforts «spécifiques à un domaine» pourraient tirer profit. Voir, par exemple, le projet PIAF (A Privacy Impact Assessment Framework for data protection and privacy rights): http://www.piafproject.eu/.
Pour des orientations formulées au niveau national, voir par exemple, la méthodologie de la CNIL:
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf
et le manuel d'analyse d'impact sur la vie privée de l'ICO:
http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

commission LIBE[115], qui indiquait que le responsable du traitement devrait informer la personne concernée des raisons qui le portent à croire que ses intérêts prévalent sur l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Selon le groupe de travail, ces informations devraient être communiquées aux personnes concernées conjointement avec celles que le responsable du traitement doit fournir conformément aux articles 10 et 11 de la directive actuelle (article 11 du règlement proposé). Cela permettra à la personne concernée de soulever éventuellement des objections dans un deuxième temps et au responsable du traitement de justifier au cas par cas les intérêts qui prévalent. En outre, le responsable du traitement devrait mettre la documentation sur laquelle il a fondé son évaluation à la disposition des autorités chargées de la protection des données, à la demande de ces dernières, afin de leur permettre de procéder éventuellement à une vérification et de faire appliquer leur décision, s'il y a lieu.

Le groupe de travail recommande que ces trois mesures soient explicitement incluses dans le règlement proposé selon les modalités énoncées plus haut. Ce serait un moyen de reconnaître le rôle des fondements juridiques dans l'appréciation de la légitimité et de clarifier l'importance du critère de mise en balance dans le contexte plus large des mesures de renforcement de la responsabilité et des analyses d'impact dans le nouveau cadre juridique proposé.

Le groupe de travail estime qu'il est également souhaitable de charger le comité européen de la protection des données de formuler au besoin d'autres orientations sur la base de ce cadre. Cette approche garantirait à la fois une clarté suffisante du texte et une flexibilité suffisante dans son application.

[115] Projet de rapport sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) [COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)].

Annexe 1. Guide succinct sur les modalités d'application du critère de mise en balance visé à l'article 7, point f)

Étape 1: Évaluer quel fondement juridique peut éventuellement être retenu au titre de l'article 7, points a) à f)

Le traitement des données ne peut s'effectuer que si au moins un des six motifs – énoncés aux points a) à f) – de l'article 7 peut être retenu (des motifs différents peuvent être invoqués à différents stades de la même activité de traitement). S'il apparaît, à première vue, que l'article 7, point f), pourrait être un fondement juridique approprié, passer à l'étape 2.

Conseils pratiques:

- l'article 7, point a), s'applique uniquement si un consentement libre, informé, spécifique et indubitable a été donné; le fait qu'un individu n'ait pas marqué son opposition au traitement en vertu de l'article 14 ne doit pas être confondu avec le consentement visé à l'article 7, point a) – cependant, un mécanisme facile à utiliser et permettant de s'opposer à un traitement peut être considéré comme une garantie importante au regard de l'article 7, point f);
- l'article 7, point b), couvre le traitement nécessaire à l'exécution du contrat; le seul fait que le traitement des données soit lié au contrat ou prévu quelque part dans les clauses du contrat ne signifie pas nécessairement que ce motif puisse être retenu; le cas échéant, l'article 7, point f), peut être envisagé comme une autre option;
- l'article 7, point c), se rapporte uniquement à des obligations légales claires et spécifiques conformes aux législations de l'Union ou d'un État membre; dans le cas de lignes directrices non contraignantes (formulées, par exemple, par des organes de réglementation), ou d'une obligation légale étrangère, l'article 7, point f), doit être envisagé comme une autre option.

Étape 2: Qualifier un intérêt de «légitime» ou d'«illégitime»

Pour être considéré comme légitime, un intérêt doit remplir toutes les conditions suivantes:

- être licite (c'est-à-dire conforme au droit applicable dans l'Union et dans le pays concerné);
- être exprimé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée (c'est-à-dire suffisamment concret);
- constituer un intérêt réel et présent (c'est-à-dire ne pas être hypothétique).

Étape 3: Déterminer si le traitement est nécessaire à la réalisation de l'intérêt poursuivi

Pour remplir cette condition, examiner s'il existe d'autres moyens plus respectueux de la vie privée susceptibles d'atteindre la finalité du traitement et de servir l'intérêt légitime du responsable du traitement des données.

Étape 4: Établir un bilan provisoire en appréciant si les droits fondamentaux ou les intérêts de personnes concernées prévalent sur l'intérêt poursuivi par le responsable du traitement des données

- Tenir compte de la nature de l'intérêt poursuivi par le responsable du traitement (droit fondamental, autre type d'intérêt, intérêt public);

- évaluer le préjudice possible pour le responsable du traitement, les tiers ou la collectivité si le traitement des données n'est pas effectué;
- tenir compte de la nature des données (données sensibles au sens strict du terme ou dans un sens plus général?);
- prendre en considération le statut de la personne concernée (mineur, salarié, etc.) et celui du responsable du traitement (par exemple, si une entreprise occupe une position dominante sur le marché);
- tenir compte de la façon dont les données sont traitées (à grande échelle, extraction de données, établissement de profils, divulgation auprès d'un grand nombre de personnes ou publication);
- identifier les droits fondamentaux et/ou les intérêts des personnes concernées qui pourraient en subir les conséquences;
- prendre en considération les attentes raisonnables des personnes concernées;
- évaluer les incidences sur les personnes concernées et les comparer avec les avantages du traitement escomptés par le responsable du traitement des données.

Conseil pratique: Prendre en considération l'effet concret du traitement sur des individus en particulier – ne pas en faire un exercice abstrait ou hypothétique.

Étape 5: Établir un bilan final en tenant compte des garanties supplémentaires

Identifier et mettre en place des garanties supplémentaires appropriées résultant du devoir de vigilance et de diligence, comme:
- la minimisation des données (par exemple, une limitation stricte du volume de données collectées, ou la suppression immédiate des données après utilisation);
- les mesures techniques et organisationnelles garantissant que les données ne peuvent servir à la prise de décisions ou d'autres mesures à l'endroit des individus («séparation fonctionnelle»);
- un large recours aux techniques d'anonymisation, l'agrégation des données, les technologies renforçant la protection de la vie privée, la prise en compte du respect de la vie privée dès la conception, les analyses d'impact relatives à la vie privée et à la protection des données;
- une transparence accrue, un droit général et inconditionnel de refuser le traitement, la portabilité des données et autres mesures connexes visant à renforcer le pouvoir des personnes concernées.

Conseil pratique: L'utilisation de technologies et d'approches renforçant la protection de la vie privée peut faire pencher la balance en faveur du responsable du traitement des données, tout en protégeant les personnes concernées.

Étape 6: Démontrer le respect des dispositions applicables et garantir la transparence

- Dresser un plan des étapes 1 à 5 pour justifier le traitement avant son lancement.
- Informer les personnes concernées des raisons qui portent le responsable du traitement à penser que la balance penche en sa faveur.
- Tenir la documentation à la disposition des autorités chargées de la protection des données.

Conseil pratique: Cette étape est *modulable*; le degré de détail de l'appréciation et de la documentation doit être adapté à la nature et au contexte du traitement. Ces mesures auront plus d'ampleur quand de gros volumes d'informations concernant de nombreuses personnes sont traités, d'une façon qui pourrait avoir une incidence considérable sur ces personnes. Une analyse d'impact complète relative à la vie privée et à la protection des données (conformément à l'article 33 du règlement proposé) ne sera nécessaire que lorsqu'une opération de traitement

présente des risques spécifiques pour les droits et libertés des personnes concernées. Dans ces cas, l'évaluation au regard de l'article 7, point f), pourrait devenir une part essentielle de cette analyse d'impact plus large.

Étape 7: Et si la personne concernée exerce son droit d'opposition?

- Lorsqu'il n'existe comme garantie qu'un droit d'opposition assorti de conditions [c'est ce qui est explicitement requis en vertu de l'article 14, point a), à titre de garantie minimale]: au cas où la personne concernée s'oppose au traitement, il convient de veiller à ce qu'un mécanisme approprié et convivial ait été mis en place pour réévaluer l'équilibre en ce qui concerne cet individu et cesser de traiter ses données si la réévaluation fait apparaître que son intérêt prévaut.
- Lorsqu'un droit de refus inconditionnel a été prévu à titre de garantie supplémentaire [parce qu'il est explicitement requis au titre de l'article 14, point b), ou parce que cette garantie supplémentaire est jugée nécessaire ou utile]: au cas où la personne concernée s'oppose au traitement, il convient de veiller à ce que son choix soit respecté, sans qu'il soit nécessaire de faire d'autres démarches ou de procéder à une nouvelle évaluation.

64

Annexe 2. Exemples pratiques destinés à illustrer l'application du critère de mise en balance visé à l'article 7, point f)

Cette annexe présente des exemples de certains des contextes les plus courants où la question de l'intérêt légitime au sens de l'article 7, point f), peut se poser. Le plus souvent, nous avons regroupé sous une même rubrique au moins deux exemples liés qu'il est intéressant de comparer. Bon nombre des exemples reposent sur des situations réelles, ou des éléments de cas réels auxquels sont confrontées les autorités chargées de la protection des données dans les différents États membres. Nous avons cependant modifié parfois les faits dans une certaine mesure pour mieux illustrer comment le critère de mise en balance doit être appliqué.

Ces exemples sont fournis pour illustrer le *processus de réflexion*: la méthode à utiliser pour tenir compte des multiples facteurs du critère de mise en balance. Autrement dit, les exemples *ne sont pas* destinés à présenter une évaluation *concluante* des situations décrites. En effet, dans beaucoup de cas, en modifiant les circonstances d'une manière ou d'une autre (par exemple, si le responsable du traitement venait à adopter des garanties supplémentaires comme une anonymisation plus complète, de meilleures mesures de sécurité et davantage de transparence ou de liberté de choix pour les personnes concernées), le résultat de la mise en balance pourrait changer[116].

Cela devrait encourager les responsables du traitement à mieux respecter l'ensemble des dispositions horizontales de la directive et à prévoir, s'il y a lieu, des mesures supplémentaires fondées sur le respect de la vie privée et la protection des données dès la conception. Plus les responsables du traitement ont soin de protéger les données à caractère personnel d'une manière générale, plus ils ont des chances de satisfaire au critère de mise en balance.

Exercice du droit à la liberté d'expression ou d'information[117], notamment dans les médias et dans les arts

Exemple 1: une ONG republie les dépenses des parlementaires

Une administration publie – en vertu d'une obligation légale [article 7, point c)] – les dépenses des parlementaires; par la suite, une ONG qui se consacre à la transparence analyse les données et les republie dans une version exacte et proportionnée, mais plus informative et annotée, afin de contribuer à renforcer la transparence et la responsabilité.

En supposant que l'ONG assure le travail de republication et d'annotation de manière fidèle et proportionnée, adopte des garanties appropriées et, plus généralement, respecte les droits des individus concernés, elle devrait pouvoir invoquer l'article 7, point f), comme fondement juridique justifiant le traitement. La nature de l'intérêt légitime (un droit fondamental à la

[116] L'application correcte de l'article 7, point f), peut donner lieu à des questions d'appréciation complexes et il peut être utile, pour éclairer l'évaluation, de s'appuyer sur une législation et une jurisprudence spécifiques, sur des lignes directrices, des codes de conduite et d'autres critères formels ou informels.

[117] À propos de la liberté d'expression ou d'information, voir la page 38 de l'avis. Les dérogations éventuelles applicables en vertu du droit national pour le traitement à des fins de journalisme, conformément à l'article 9 de la directive, doivent aussi être prises en compte dans l'appréciation de ces exemples.

liberté d'expression ou d'information), l'intérêt public servi par la transparence et la responsabilité, et le fait que les informations aient déjà été publiées et se rapportent à des données à caractère personnel (relativement moins sensibles) liées aux activités menées par des individus dans l'exercice de leurs fonctions publiques[118] sont autant de facteurs qui pèsent en faveur de la légitimité du traitement. Un autre élément contribuant à l'évaluation favorable tient à ce que la publication initiale était requise par la loi et que les personnes concernées devaient donc s'attendre à voir leurs données publiées. Dans l'autre plateau de la balance, on trouve l'incidence sur les individus qui peut être considérable, à cause du jugement du public, et la mise en cause possible de l'intégrité de certains individus pouvant entraîner, par exemple, une défaite aux élections, voire dans certains cas une enquête pénale sur des activités frauduleuses. Dans l'ensemble, les facteurs ci-dessus montrent cependant que, tout bien pesé, l'intérêt poursuivi par le responsable du traitement (et l'intérêt des citoyens à qui les données sont communiquées) prévaut sur l'intérêt des personnes concernées.

Exemple 2: un conseiller municipal prend sa fille comme assistante

Un journaliste publie un article bien documenté, relatant des faits avérés, dans un journal local en ligne, qui révèle qu'un conseiller municipal n'a assisté qu'à une seule réunion du conseil sur les onze dernières et indique qu'il a peu de chances d'être réélu en raison d'un récent scandale à propos de la nomination de sa fille, âgée de dix-sept ans, comme assistante.

Une analyse semblable à celle de l'*exemple 1* s'applique également ici. En ce qui concerne les faits, il est dans l'intérêt légitime du journal en question de publier l'information. Même si des données à caractère personnel ont été révélées à propos du conseiller, le droit de ce dernier au respect de sa vie privée ne prévaut pas sur le droit fondamental à la liberté d'expression qui justifie la publication de l'article dans le journal. Cette appréciation tient au fait que le droit des personnalités publiques en matière de vie privée est relativement limité au regard de leurs activités publiques et à l'importance particulière de la liberté d'expression – surtout si la publication des informations est d'intérêt public.

Exemple 3: un délit mineur continue à apparaître parmi les premiers résultats d'une recherche en ligne

Les archives en ligne d'un journal contiennent un article déjà ancien relatif à une personne qui a, par le passé, connu une certaine célébrité au plan local en tant que capitaine d'une petite équipe de football amateur. Cet individu est identifié par son nom complet et l'article porte sur une procédure pénale relativement mineure le concernant (ivresse et trouble à l'ordre public). Le casier judiciaire de cet homme est aujourd'hui vierge et l'ancien délit pour lequel il a purgé sa peine voici plusieurs années n'y figure plus. Ce qui est gênant pour cet individu, c'est que lorsqu'une recherche sur son nom est effectuée avec les principaux moteurs de recherche en ligne, les premiers résultats affichés font apparaître le lien vers ce vieil article le concernant. Malgré une demande introduite par la personne concernée, le journal refuse de prendre des mesures techniques qui restreindraient la disponibilité générale de l'article qui lui

[118] Il ne peut être exclu que certaines dépenses révèlent des données plus sensibles, touchant à la santé, par exemple. Si tel est le cas, il conviendrait de les effacer de l'ensemble de données avant la première publication. Une bonne pratique consiste à adopter une «démarche proactive» et à offrir aux personnes concernées l'occasion d'examiner leurs données avant toute publication, en les informant clairement des possibilités et des modalités de publication.

est consacré. Par exemple, le journal n'envisage pas d'adopter des mesures techniques et organisationnelles qui viseraient – dans la mesure où la technologie le permet – à limiter l'accès aux informations à partir de moteurs de recherche externes qui se servent du nom de la personne comme critère de recherche.

C'est là un autre cas illustrant le conflit possible entre la liberté d'expression et le droit au respect de la vie privée. Cela montre aussi que, parfois, des garanties supplémentaires – comme le fait de veiller à ce que, au moins en cas d'opposition justifiée en vertu de l'article 14, point a), de la directive, la partie concernée des archives du journal ne soit plus accessible par des moteurs de recherche externes ou le format utilisé pour afficher les informations ne permette plus de recherches sur le nom – peuvent jouer un rôle essentiel pour trouver un équilibre adéquat entre les deux droits fondamentaux en cause. Cela ne fait pas obstacle à d'autres mesures éventuelles qui pourraient être prises par les moteurs de recherche ou d'autres tiers[119].

Prospection directe conventionnelle et autres formes de prospection commerciale ou de publicité

Exemple 4: un magasin d'informatique envoie à ses clients des publicités pour des produits similaires

Un magasin d'informatique obtient de ses clients leurs coordonnées de contact dans le cadre de la vente d'un produit et se sert de ces coordonnées à des fins de prospection par courrier ordinaire pour promouvoir ses propres produits similaires. Le magasin vend aussi des produits en ligne et envoie des courriers électroniques promotionnels quand une nouvelle gamme de produits entre en stock. Les clients disposent d'informations claires sur la possibilité qu'ils ont de s'y opposer, sans frais et de manière simple, quand leurs coordonnées de contact sont collectées et chaque fois qu'un message est envoyé, au cas où ils n'auraient pas refusé initialement.

La transparence du traitement, le fait que le client peut raisonnablement s'attendre à recevoir des offres pour des produits similaires en tant que client du magasin et le droit d'opposition contribuent à renforcer la légitimité du traitement et à garantir les droits des individus. Dans l'autre plateau de la balance, il ne semble pas y avoir d'incidence disproportionnée sur le droit au respect de la vie privée (dans cet exemple, nous avons supposé que le magasin d'informatique n'établit pas de profils complexes de ses clients, en se servant, par exemple, d'une analyse détaillée de ses données de consultation en ligne).

Exemple 5: une pharmacie en ligne établit des profils détaillés

Une pharmacie en ligne se livre à des activités de prospection fondées sur les achats de médicaments et autres produits faits par ses clients, y compris des produits obtenus avec une prescription médicale. Elle analyse ces informations – combinées à des données démographiques à propos de sa clientèle, par exemple l'âge et le sexe – afin d'établir un «profil de santé et de bien-être» de chaque client. Le profil utilise des données de l'historique de navigation, qui sont collectées non seulement à propos des produits achetés par les clients,

[119] Voir aussi l'affaire C-131/12 Google Spain/Agencia Española de Proteccion de Datos, actuellement pendante devant la Cour de justice de l'Union européenne.

mais aussi à propos des produits et des informations qu'ils ont consultés sur le site internet. Les profils de clients comprennent des informations ou des prévisions indiquant qu'une cliente est enceinte, qu'une autre souffre d'une maladie chronique particulière, ou serait intéressée par l'achat de compléments alimentaires, de lotion solaire ou d'autres produits de soin de la peau à certaines périodes de l'année. Les analystes de la pharmacie en ligne se servent de ces informations pour envoyer à certaines personnes des courriers électroniques leur proposant des médicaments vendus sans prescription, des compléments alimentaires et d'autres produits. Dans ce cas, la pharmacie ne peut invoquer son intérêt légitime pour justifier la création et l'utilisation de profils de ses clients à des fins de prospection. L'activité de profilage décrite pose plusieurs problèmes. Les informations sont particulièrement sensibles et peuvent révéler beaucoup de choses sur des sujets qui sont censés rester privés aux yeux de la plupart des individus[120]. L'ampleur de cette activité de profilage et la manière dont elle est effectuée (utilisation de l'historique de navigation, algorithmes prédictifs) révèlent aussi un degré élevé d'ingérence dans la vie privée. Un consentement fondé sur l'article 7, point a), et sur l'article 8, paragraphe 2, point a) (lorsqu'il s'agit de données sensibles) pourrait cependant, si besoin est, constituer une autre option.

Messages non commerciaux non sollicités, notamment à des fins de campagne politique ou de collecte de fonds pour des actions caritatives

Exemple 6: une candidate aux élections locales fait un usage ciblé de la liste électorale

Une candidate aux élections locales se sert de la liste électorale[121] pour envoyer une lettre de présentation à chaque électeur potentiel de sa circonscription dans le cadre de sa campagne pour les prochaines élections. La candidate n'utilise les données obtenues dans la liste électorale que pour envoyer sa lettre et ne conserve pas les données après la fin de la campagne.

Cette utilisation du registre local s'inscrit dans les attentes raisonnables des individus, quand elle intervient au cours de la période préélectorale: l'intérêt de la responsable du traitement est clair et légitime. L'usage limité et ciblé des informations contribue aussi à faire pencher la balance en faveur de l'intérêt légitime de la responsable du traitement. Une telle utilisation des listes électorales peut aussi être réglementée par la loi au niveau national, dans une perspective d'intérêt public, de façon à prévoir des règles spécifiques, des limitations et des garanties. Si tel est le cas, le respect de ces règles spécifiques est également requis afin de garantir la légitimité du traitement.

Exemple 7: une association sans but lucratif collecte des informations à des fins d'envois de messages ciblés

[120] Au-delà des restrictions éventuelles imposées par les lois en matière de protection des données, la publicité pour des produits soumis à prescription médicale est aussi strictement réglementée dans l'Union, et il existe certaines restrictions concernant la publicité pour les médicaments vendus sans prescription. Par ailleurs, les exigences de l'article 8 à propos des catégories particulières de données (comme les données relatives à la santé) doivent aussi être prises en considération.

[121] Il est supposé que dans l'État membre où l'exemple s'applique, une liste électorale est établie en vertu de la loi.

Une organisation philosophique qui se consacre au développement humain et social décide de mener des actions de collecte de fonds organisées sur la base du profil de ses membres. À cette fin, elle collecte des données sur les sites de réseaux sociaux au moyen d'un logiciel spécialement conçu pour cibler les individus qui ont «aimé» la page de l'organisation, «aimé» ou «partagé» les messages postés par l'organisation sur sa page, consulté régulièrement certains sujets ou re-tweeté les messages de l'organisation. Elle envoie ensuite des messages et des lettres d'information à ses membres en fonction de leurs profils. Par exemple, les personnes âgées qui ont un chien et qui ont «aimé» des articles sur les refuges pour animaux reçoivent des appels aux dons différents de ceux adressés aux familles avec enfants en bas âge; les personnes appartenant à des groupes ethniques différents reçoivent aussi des messages différents.

Le fait que des catégories particulières de données soient traitées (convictions philosophiques) requiert le respect de l'article 8, une condition qui paraît être remplie puisque le traitement est effectué dans le cadre des activités légitimes de l'organisation. Ce n'est cependant pas une condition suffisante dans ce cas: la façon dont les données sont utilisées excède les attentes raisonnables des individus. Le volume de données collectées, le manque de transparence à propos de la collecte et la réutilisation de données communiquées initialement à une fin différente contribuent à la conclusion que l'article 7, point f), ne peut pas être invoqué en l'occurrence. Le traitement ne doit donc pas être autorisé, à moins qu'un autre motif puisse être invoqué, par exemple le consentement des personnes concernées donné conformément à l'article 7, point a).

Exécution de demandes en justice, y compris le recouvrement de créances via des procédures extrajudiciaires

Exemple 8: litige à propos de la qualité de travaux de rénovation

Un client conteste la qualité de travaux de rénovation réalisés dans sa cuisine et refuse de payer la totalité du prix demandé. L'entrepreneur transmet des données pertinentes et proportionnées à son avocat pour lui permettre d'envoyer un rappel au client et de négocier un arrangement avec lui s'il continue à refuser de payer.

Dans ce cas, les démarches préliminaires accomplies par l'entrepreneur au moyen d'informations de base sur la personne concernée (par exemple, nom, adresse, référence du contrat) pour lui envoyer un rappel (directement ou, en l'occurrence, par l'intermédiaire de son avocat) peuvent encore relever du traitement nécessaire à l'exécution du contrat [article 7, point b)]. Les étapes suivantes[122], incluant l'intervention d'une société de recouvrement de créances, devraient cependant être appréciées au regard de l'article 7, point f), compte tenu, entre autres, du degré d'ingérence et de l'incidence sur la personne concernée, comme on le verra dans l'exemple suivant.

Exemple 9: un client disparaît avec une voiture achetée à crédit

[122] Selon les États membres, il existe actuellement un certain degré de variabilité quant aux mesures qui peuvent être jugées nécessaires à l'exécution d'un contrat.

Un client cesse de payer les mensualités dues pour l'achat à crédit d'une coûteuse voiture de sport et «disparaît» ensuite. Le concessionnaire fait appel à un «agent de recouvrement» tiers. L'agent de recouvrement mène une enquête intrusive «de type judiciaire», en recourant notamment à la vidéosurveillance avec camera cachée et à des écoutes téléphoniques.

Bien que l'intérêt poursuivi par le concessionnaire et par l'agent de recouvrement soit légitime, la balance ne penche pas en leur faveur à cause des méthodes intrusives utilisées pour collecter des informations, dont certaines sont explicitement interdites par la loi (écoutes téléphoniques). La conclusion serait différente si, par exemple, le concessionnaire ou l'agent de recouvrement n'avaient effectué que des vérifications limitées pour confirmer les coordonnées de contact de la personne concernée afin d'engager des poursuites en justice.

Prévention de la fraude, de l'utilisation abusive de services, ou du blanchiment d'argent

Exemple 10: vérification des données des clients avant l'ouverture d'un compte bancaire

Une institution financière suit des procédures raisonnables et proportionnées – conformément aux lignes directrices non contraignantes de l'autorité publique de surveillance financière compétente – afin de vérifier l'identité de toute personne qui souhaite ouvrir un compte. Elle conserve dans ses archives les informations utilisées pour vérifier l'identité de la personne.

L'intérêt poursuivi par le responsable du traitement est légitime et le traitement des données porte uniquement sur des informations limitées et nécessaires (pratique normale dans ce secteur d'activités, à laquelle s'attendent raisonnablement les personnes concernées, et recommandée par les autorités compétentes). Des garanties appropriées ont été mises en place pour limiter toute incidence indue et disproportionnée sur les personnes concernées. Le responsable du traitement peut donc invoquer l'article 7, point f). Sinon, et dans la mesure où les procédures utilisées sont spécifiquement requises par le droit en vigueur, l'article 7, point c), pourrait s'appliquer.

Exemple 11: échange d'informations pour lutter contre le blanchiment d'argent

Une institution financière – après avoir obtenu l'avis de l'autorité compétente chargée de la protection des données – met en place des procédures fondées sur des critères spécifiques et limités pour échanger avec d'autres filiales du même groupe des données relatives à un contournement présumé des règles de lutte contre le blanchiment d'argent, en prévoyant des limitations d'accès strictes, des mesures de sécurité et une interdiction de toute utilisation ultérieure à d'autres fins.

Pour des raisons semblables à celles exposées ci-dessus, et selon les circonstances, le traitement des données pourrait être fondé sur l'article 7, point f). Sinon, et dans la mesure où les procédures appliquées sont spécifiquement requises par le droit en vigueur, l'article 7, point c), pourrait s'appliquer.

Exemple 12: liste noire de toxicomanes agressifs

Un groupe d'hôpitaux crée une liste noire commune d'individus «agressifs» qui cherchent à se procurer des médicaments, afin de leur interdire l'accès aux locaux des hôpitaux participants.

Même si l'intérêt des responsables du traitement à assurer la sécurité des hôpitaux est légitime, il doit être mis en balance avec le droit fondamental au respect de la vie privée et avec d'autres considérations impératives comme la nécessité de ne pas priver les individus concernés d'un accès à des soins médicaux. Le fait que le traitement porte sur des données sensibles (par exemple, des données médicales relatives à une toxicomanie) corrobore aussi la conclusion que, dans ce cas, il est peu probable que le traitement puisse être justifié en vertu de l'article 7, point f)[123]. Le traitement pourrait être acceptable s'il était, par exemple, encadré par une loi prévoyant des garanties spécifiques (vérifications et contrôles, transparence, prévention des décisions automatisées) pour faire en sorte qu'il n'entraîne pas de discrimination ou de violation des droits fondamentaux des individus[124]. Dans ce dernier cas, selon que cette législation spécifique requiert ou autorise seulement le traitement, soit l'article 7, point c), soit l'article 7, point f), pourrait être invoqué comme fondement juridique.

Surveillance du personnel à des fins de sécurité ou de gestion

Exemple 13: utilisation des heures de travail des avocats à des fins de facturation et de calcul de primes

Le nombre d'heures facturables accomplies par les membres d'un cabinet d'avocats est traité à la fois à des fins d'établissement des factures et pour la détermination des primes annuelles. Le système est expliqué de manière transparente aux employés qui disposent d'un droit explicite de marquer leur désaccord avec les conclusions en ce qui concerne tant la facturation que le paiement des primes, ce qui donne alors lieu à des discussions avec la direction.

Le traitement paraît nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement et il ne semble pas qu'il existe un moyen plus respectueux de la vie privée susceptible de servir à la même finalité. L'incidence sur les employés est d'ailleurs limitée, grâce aux garanties et aux processus mis en place. L'article 7, point f), pourrait donc constituer un fondement juridique approprié dans ce cas. Il pourrait aussi être soutenu que le traitement effectué à l'une de ces fins ou aux deux est nécessaire à l'exécution du contrat.

[123] Les exigences de l'article 8 à propos des catégories particulières de données (comme les données de santé) doivent aussi être prises en considération.

[124] Voir le document de travail sur les listes noires (WP 65), adopté le 3 octobre 2002.

Exemple 14: surveillance électronique de l'utilisation de l'internet[125]

Un employeur surveille l'utilisation de l'internet par les salariés durant les heures de travail pour s'assurer qu'ils ne font pas un usage personnel excessif de l'équipement informatique de la société. Les données collectées comprennent les fichiers temporaires et les cookies créés sur les ordinateurs des salariés, l'historique des sites visités et des téléchargements effectués durant les heures de travail. Les données sont traitées sans consultation préalable des personnes concernées ni des représentants syndicaux/du comité d'entreprise. Les informations fournies aux individus concernés à propos de ces pratiques sont insuffisantes.

Le volume et la nature des données collectées représentent une ingérence considérable dans la vie privée des salariés. En plus des questions de proportionnalité, la transparence des pratiques, étroitement liée aux attentes raisonnables des personnes concernées, est aussi un facteur important à prendre en considération. Même si l'employeur a un intérêt légitime à limiter le temps consacré par les salariés à visiter des sites internet qui ne sont pas directement pertinents pour leur travail, les méthodes utilisées ne satisfont pas au critère de mise en balance prévu par l'article 7, point f). L'employeur devrait recourir à des méthodes moins intrusives (par exemple, limiter l'accessibilité de certains sites), qu'il conviendrait, pour se conformer aux meilleures pratiques, de discuter et d'approuver conjointement avec les représentants du personnel et de communiquer aux salariés de façon transparente.

Mécanismes de dénonciation des dysfonctionnements

Exemple 15: mécanisme de dénonciation des dysfonctionnements répondant à des obligations légales étrangères

Une filiale européenne d'un groupe américain met en place un mécanisme limité de dénonciation des dysfonctionnements pour signaler les infractions graves dans le domaine de la comptabilité et des finances. Les entités du groupe sont soumises à un code de bonne gouvernance qui préconise un renforcement des procédures de contrôle interne et de gestion des risques. Du fait de ses activités internationales, la filiale européenne est tenue de fournir des données financières fiables aux autres membres du groupe aux États-Unis. Le mécanisme est conçu pour être conforme au droit américain et aux lignes directrices formulées par les autorités nationales chargées de la protection des données dans l'Union.

Parmi les garanties prévues, des séances de formation ainsi que d'autres moyens servent à donner des orientations claires aux salariés sur les circonstances dans lesquelles il convient d'utiliser le mécanisme. Le personnel est mis en garde contre tout abus – par exemple, des allégations fausses ou sans fondement à l'encontre de collègues. Il est aussi expliqué aux salariés qu'ils peuvent, à leur convenance, utiliser le mécanisme de façon anonyme ou en s'identifiant. Dans ce dernier cas, ils sont avisés des circonstances dans lesquelles les informations qui les identifient seront transmises à leur employeur ou à d'autres agences.

Si le droit européen ou la législation d'un État membre de l'Union exigeait la mise en place du mécanisme, le traitement pourrait se fonder sur l'article 7, point c). Cependant, les

[125] Quelques États membres estiment qu'un contrôle électronique limité peut être «nécessaire à l'exécution d'un contrat» et peut donc tirer son fondement juridique de l'article 7, point b), plutôt que de l'article 7, point f).

obligations légales étrangères ne sont pas considérées comme une obligation légale au sens de l'article 7, point c), et ne peuvent donc pas servir à légitimer le traitement en vertu de l'article 7, point c). Le traitement pourrait néanmoins se fonder sur l'article 7, point f), par exemple, s'il existe un intérêt légitime à garantir la stabilité des marchés financiers ou à lutter contre la corruption, et pour autant que le mécanisme comporte des garanties suffisantes, conformément aux orientations des autorités de réglementation compétentes dans l'Union.

Exemple 16: mécanisme interne de dénonciation des dysfonctionnements dépourvu de procédures cohérentes

Une société de services financiers décide d'instaurer un mécanisme de dénonciation des dysfonctionnements parce qu'elle soupçonne l'existence de pratiques répandues de détournement et de corruption parmi son personnel et souhaite encourager les salariés à se surveiller mutuellement. Dans un souci d'économie, la société décide d'intégrer le mécanisme à son fonctionnement interne, en confiant sa gestion aux membres de son service de ressources humaines. Pour inciter les salariés à faire usage du mécanisme, elle offre une gratification en espèces «en toute discrétion» à ceux dont la contribution permet de repérer des conduites inappropriées et de recouvrer des fonds.

La société a sans doute un intérêt légitime à détecter et prévenir le vol et la corruption. Cependant, son mécanisme de dénonciation des dysfonctionnements est si mal conçu et dépourvu de garanties que l'intérêt et le droit au respect de la vie privée des salariés prévalent – en particulier de ceux qui pourraient être victimes de fausses accusations formulées dans le seul but d'un gain financier. Le fait que le mécanisme soit géré en interne plutôt que de manière indépendante pose un autre problème, tout comme le manque de formation et d'orientations concernant l'utilisation du mécanisme.

Sécurité physique, sécurité des systèmes et réseaux informatiques

Exemple 17: contrôles biométriques dans un laboratoire de recherche

Un laboratoire de recherche scientifique travaillant sur des virus mortels utilise un système d'accès biométrique en raison du risque élevé pour la santé publique au cas où ces virus viendraient à sortir des installations. Des garanties appropriées sont appliquées, notamment la conservation des données biométriques sur des cartes personnelles que les salariés gardent en leur possession plutôt que dans un système centralisé.

Même si les données sont sensibles, au sens large du terme, leur traitement est motivé par des raisons d'intérêt public. Ces considérations, ajoutées au fait que les risques d'abus sont réduits par le recours à des garanties appropriées, font de l'article 7, point f), une base juridique adéquate justifiant le traitement.

Exemple 18: caméras cachées servant à identifier les visiteurs et les salariés qui fument

Une société utilise des caméras cachées pour identifier les visiteurs et les salariés qui fument dans des locaux du bâtiment où ce n'est pas autorisé.

Bien que le responsable du traitement ait un intérêt légitime à veiller au respect de l'interdiction de fumer, les moyens utilisés à cet effet sont, d'une manière générale,

disproportionnés et inutilement intrusifs. Il existe des méthodes plus respectueuses de la vie privée et plus transparentes (comme les détecteurs de fumée et les panneaux d'interdiction visibles). Le traitement n'est donc pas conforme à l'article 6, qui requiert que les données soient «non excessives» au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. De même, il ne satisfera probablement pas au critère de mise en balance visé à l'article 7.

Recherche scientifique

Exemple 19: recherches relatives aux effets du divorce et du chômage des parents sur la réussite scolaire des enfants

Dans le cadre d'un programme lancé par le gouvernement et autorisé par un comité d'éthique compétent, des recherches sont menées sur la relation entre le divorce, le chômage des parents et la réussite scolaire des enfants. Sans faire partie des «catégories particulières de données», l'objet de ces recherches tient néanmoins à des questions qui, pour de nombreuses familles, seraient considérées comme personnelles et très intimes. Les recherches permettront de mettre en place une assistance pédagogique spéciale ciblant des enfants qui seraient exposés, sinon, à des risques d'absentéisme, de mauvais résultats scolaires et, parvenus à l'âge adulte, de chômage et de criminalité. La législation de l'État membre concerné autorise explicitement le traitement des données à caractère personnel (à l'exception des catégories particulières de données) à des fins de recherches, pour autant que ces travaux soient nécessaires à la réalisation d'un intérêt public important et menés dans le respect de garanties adéquates, qui sont décrites en détail dans des dispositions d'exécution. Ce cadre juridique inclut des exigences spécifiques, mais aussi une structure de responsabilité qui permet l'évaluation au cas par cas de l'admissibilité des recherches (si elles sont effectuées sans le consentement des individus concernés) et des mesures à appliquer en particulier pour protéger les personnes concernées.

Le chercheur dirige un centre de recherche sûr auquel sont transmises les informations pertinentes, dans des conditions sécurisées, par le registre de population, les tribunaux, les services d'aide à l'emploi et les écoles. Le centre de recherche procède alors au «hachage» des identités individuelles pour que les enregistrements relatifs aux divorces, au chômage et aux résultats scolaires puissent être liés sans révéler les identités «civiles» des individus – par exemple, leurs noms et leurs adresses. Toutes les données originales sont ensuite définitivement supprimées. D'autres mesures sont prises pour assurer la séparation fonctionnelle (c'est-à-dire garantir que les données serviront uniquement à des fins de recherche) et réduire le risque de ré-identification éventuelle.

Les membres du personnel qui travaillent au centre de recherche reçoivent une formation rigoureuse en matière de sécurité et sont personnellement responsables – voire passibles de poursuites pénales – pour tout manquement à la sécurité qui leur serait imputable. Des mesures techniques et organisationnelles sont prises, par exemple, pour garantir que les employés qui se servent de clés USB ne peuvent pas faire sortir des données à caractère personnel du centre.

Le centre de recherche a un intérêt légitime à effectuer ces travaux, qui présentent un grand intérêt public. Lesdits travaux sont aussi dans l'intérêt légitime des administrations de l'emploi, de l'éducation et d'autres organismes participant au programme, qui seront mieux à même de planifier et dispenser des services à ceux qui en ont le plus besoin. Les aspects du

programme touchant à la vie privée ont été bien conçus et les garanties mises en place font que ni l'intérêt ni le droit au respect de la vie privée des parents ou des enfants dont les données ont servi de base aux recherches ne prévalent sur l'intérêt légitime des organisations qui mènent ces travaux.

Exemple 20: étude sur l'obésité

Une université souhaite mener des recherches sur les niveaux d'obésité infantile dans plusieurs villes et collectivités rurales. Malgré les difficultés auxquelles elle se heurte généralement pour obtenir des écoles et autres institutions un accès aux données pertinentes, elle parvient à convaincre quelques dizaines d'enseignants à suivre pendant un certain temps les enfants de leurs classes qui paraissent obèses et à leur poser des questions à propos de leurs habitudes alimentaires, de leurs niveaux d'activité physique, du temps qu'ils consacrent à jouer à des jeux vidéo, etc. Ces enseignants consignent aussi les noms et adresses des enfants interrogés pour leur faire envoyer un coupon permettant de télécharger gratuitement de la musique en ligne en guise de remerciement pour leur participation. Les chercheurs constituent ensuite une base de données sur les enfants, en mettant en corrélation les niveaux d'obésité avec l'activité physique et d'autres facteurs. Les exemplaires papier des questionnaires complétés – sous une forme qui permet encore d'identifier les enfants – sont conservés dans les archives de l'université pendant une durée indéterminée, sans mesures de sécurité adéquates. Des photocopies de tous les questionnaires sont envoyées sur demande à tout étudiant de la faculté de médecine ou d'universités partenaires dans le monde entier qui manifeste son intérêt en vue d'une utilisation ultérieure des données de recherche.

Bien que l'université ait un intérêt légitime à effectuer ces recherches, la façon dont celles-ci sont conçues signifie que, à plusieurs égards, les intérêts des enfants et leurs droits au respect de la vie privée l'emportent sur cet intérêt légitime. Hormis la méthodologie, qui manque de rigueur scientifique, le problème vient en particulier de l'absence d'approche renforçant la protection de la vie privée dans la conception des recherches et de la facilité d'accès aux données à caractère personnel collectées. À aucun moment, les données des enfants ne sont codées ou anonymisées et aucune autre mesure n'a été prise pour en garantir la sécurité ou assurer une séparation fonctionnelle. Il n'a pas non plus été obtenu de consentement valide au regard de l'article 7, point a), et de l'article 8, paragraphe 2, point a), et rien n'indique qu'on ait expliqué aux enfants ou à leurs parents à quoi allaient servir leurs données à caractère personnel ou avec qui elles seraient partagées.

Obligation légale étrangère

Exemple 21: respect des exigences du droit fiscal en vigueur dans un pays tiers

Des banques de l'Union collectent et transfèrent certaines données de leurs clients aux fins du respect des obligations en matière de fiscalité qui s'appliquent à leurs clients dans un pays tiers. La collecte et le transfert de ces données sont prévus dans les conditions et garanties convenues entre l'Union et le pays étranger dans le cadre d'un accord international et s'effectuent conformément aux termes de cet accord.

Si une obligation étrangère n'est pas, en soi, considérée comme une base légitimant le traitement au titre de l'article 7, point c), elle peut le devenir dès lors qu'elle est confirmée par un accord international. Dans ce dernier cas, le traitement pourrait être jugé nécessaire au respect d'une obligation légale intégrée au cadre juridique intérieur par l'accord international.

Cependant, s'il n'existe pas d'accord de ce type, la collecte et le transfert devront faire l'objet d'une évaluation au regard des exigences de l'article 7, point f), et ne pourront être considérés comme admissibles que si des garanties adéquates sont mises en place, comme celles approuvées par l'autorité compétente chargée de la protection des données (voir aussi l'*exemple 15*, ci-dessus).

Exemple 22: transfert de données sur des dissidents

Une entreprise de l'Union transfère des données relatives à des résidents étrangers à la demande d'un régime autoritaire dans un pays tiers qui souhaite accéder aux données de dissidents (par exemple, les données relatives à leurs échanges de courriers électroniques, le contenu de ces courriers, l'historique de navigation ou des messages privés échangés sur les réseaux sociaux).

Dans ce cas, à la différence de l'exemple précédent, il n'existe aucun accord international qui autoriserait l'application de l'article 7, point c), comme fondement juridique. En outre, plusieurs éléments plaident contre une invocation de l'article 7, point f), pour justifier le traitement. Bien que le responsable du traitement puisse avoir un intérêt économique à se plier aux demandes d'un gouvernement étranger (à défaut de quoi il pourrait faire l'objet d'un traitement moins favorable de la part de l'administration du pays tiers par rapport à d'autres entreprises), la légitimité et la proportionnalité du transfert sont hautement contestables au regard du cadre des droits fondamentaux de l'Union. L'impact potentiellement gigantesque sur les individus concernés (par exemple, discrimination, emprisonnement, condamnation à mort) fait aussi pencher fortement la balance en faveur des intérêts et des droits des personnes concernées.

Réutilisation de données publiquement disponibles

Exemple 23: classement de personnalités politiques[126]

Une ONG qui se consacre à la transparence se sert de données publiquement disponibles concernant des élus (promesses faites à l'époque de leur élection et participation effective aux scrutins de l'assemblée où ils siègent) pour les classer selon le respect de leurs engagements.

Même si l'incidence sur les personnalités politiques concernées peut être considérable, le fait que le traitement se fonde sur des informations publiques et se rapporte à leurs responsabilités publiques, ajouté à une finalité évidente de renforcement de la transparence et de la responsabilité, fait pencher la balance en faveur de l'intérêt du responsable du traitement[127].

Enfants et autres personnes vulnérables

Exemple 24: site internet d'information à l'intention des adolescents

[126] Voir aussi, pour comparaison, l'*exemple 7* ci-dessus.

[127] Comme dans les *exemples 1 et 2*, nous avons supposé que la publication est exacte et proportionnée. L'absence de garanties et d'autres facteurs peuvent modifier l'équilibre des intérêts selon les circonstances.

Le site internet d'une ONG qui dispense des conseils aux adolescents sur des questions comme la drogue, la grossesse non désirée et la consommation d'alcool collecte des données via son propre serveur à propos des visiteurs du site. Ces données sont immédiatement anonymisées et transformées en statistiques générales sur les sections les plus populaires du site auprès des visiteurs selon les différentes régions géographiques du pays.

L'article 7, point f), pourrait servir de fondement juridique, même si des données concernant des individus vulnérables sont concernées, dès lors que le traitement est effectué dans l'intérêt public et que des garanties strictes ont été mises en place (les données sont immédiatement rendues anonymes et utilisées seulement pour la production de statistiques), ce qui contribue à faire pencher la balance en faveur du responsable du traitement.

Solutions de prise en compte du respect de la vie privée dès la conception utilisées comme garantie supplémentaire

Exemple 25: accès aux numéros de téléphone mobile des utilisateurs et non-utilisateurs d'une application: «comparer et oublier»

Les données à caractère personnel d'individus sont traitées pour vérifier s'ils ont déjà indubitablement donné leur consentement dans le passé (système «comparer et oublier» mis en place à titre de garantie).

Le développeur d'une application est tenu d'obtenir le consentement indubitable des personnes concernées pour traiter leurs données à caractère personnel: c'est le cas, par exemple, s'il souhaite accéder à tout le carnet d'adresses électroniques des utilisateurs de l'application, y compris les numéros de téléphone mobiles de contacts qui n'utilisent pas l'application. Pour ce faire, il peut d'abord vérifier si les détenteurs des numéros de téléphone mobile figurant dans le carnet d'adresses des utilisateurs de l'application ont déjà indubitablement donné leur consentement [conformément à l'article 7, point a)] pour le traitement de leurs données.

Pour ce traitement initial limité (à savoir, un accès en lecture à court terme à tout le carnet d'adresses de l'utilisateur d'une application), le développeur peut invoquer l'article 7, point f), comme fondement juridique, sous réserve de garanties appropriées. Ces garanties devraient inclure des mesures techniques et organisationnelles pour faire en sorte que cet accès serve uniquement à aider l'utilisateur à identifier quels sont, parmi ses contacts, ceux qui sont déjà des utilisateurs et qui ont donc déjà indubitablement donné leur consentement pour que la société collecte et traite leurs numéros de téléphone à cet effet. Les numéros de téléphone mobile des non-utilisateurs ne peuvent être utilisés et collectés que dans le but strictement limité de vérifier s'ils ont déjà indubitablement donné leur consentement et devraient être effacés immédiatement après.

Combinaison d'informations personnelles recueillies par des services internet

Exemple 26: combinaison d'informations personnelles recueillies par différents services internet

La politique de confidentialité d'une société proposant divers services sur l'internet, dont un moteur de recherche, le partage de vidéos et un réseau social, contient une clause qui l'autorise à «combiner toutes les informations personnelles» collectées à propos de chacun de

ses utilisateurs pour les différents services qu'ils utilisent, sans déterminer aucune période de conservation des données. Selon cette société, le but est de «garantir la meilleure qualité de service possible».

La société met certains outils à la disposition de différentes catégories d'utilisateurs pour leur permettre d'exercer leurs droits (par exemple, désactiver les publicités ciblées, s'opposer à l'ajout d'un type de cookies spécifique).

Cependant, les outils disponibles ne permettent pas aux utilisateurs d'exercer un contrôle effectif sur le traitement de leurs données: les utilisateurs ne peuvent pas contrôler les combinaisons spécifiques de leurs données collectées par différents services et ils ne peuvent pas s'opposer à la combinaison des données les concernant. Dans l'ensemble, il existe un déséquilibre entre l'intérêt légitime de la société et la protection des droits fondamentaux des utilisateurs, de telle sorte que l'article 7, point f), ne devrait pas pouvoir servir de fondement juridique justifiant le traitement. L'article 7, point a), constituerait un fondement plus approprié, pour autant que les conditions d'un consentement valide soient remplies.

78

Lignes directrices relatives à la portabilité des données (WP242)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

16/FR
WP 242 rev.01

Lignes directrices relatives au droit à la portabilité des données

Adoptées le 13 décembre 2016
Version révisée et adoptée le 5 avril 2017

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et état de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO59 05/35.

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

TABLE DES MATIÈRES

Synthèse

L'article 20 du règlement général sur la protection des données crée un nouveau droit à la portabilité des données, qui est étroitement lié au droit d'accès aux données, tout en différant de celui-ci à de nombreux égards. Il confère aux personnes concernées le droit de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable du traitement. Ce nouveau droit a pour objectif de responsabiliser les personnes concernées et de leur permettre de contrôler davantage les données à caractère personnel les concernant.

Dans la mesure où il permet la transmission directe des données à caractère personnel d'un responsable du traitement à un autre, le droit à la portabilité des données constitue également un instrument important qui facilitera la libre circulation des données à caractère personnel dans l'Union et qui stimulera la concurrence entre les responsables du traitement. Il facilitera le passage d'un prestataire de services à un autre et encouragera dès lors la mise au point de nouveaux services dans le contexte de la stratégie pour un marché unique numérique.

Le présent avis fournit des orientations sur la manière d'interpréter et de mettre en œuvre le droit à la portabilité des données, tel qu'il a été introduit par le règlement général sur la protection des données. Il a pour objet d'examiner la question du droit à la portabilité des données et son champ d'application. Il précise les conditions dans lesquelles ce nouveau droit s'applique compte tenu de la base juridique du traitement des données (soit le consentement de la personne concernée, soit la nécessité d'exécuter un contrat) et du fait que ce droit est limité aux données à caractère personnel fournies par la personne concernée. Le présent avis fournit également des exemples et des critères concrets pour expliquer les circonstances dans lesquelles ce droit s'applique. À cet égard, le groupe de travail «Article 29» considère que le droit à la portabilité des données couvre les données fournies sciemment et activement par la personne concernée, ainsi que les données à caractère personnel générées par son activité. Ce nouveau droit ne peut être remis en cause et limité aux informations à caractère personnel que la personne concernée communique directement, par exemple sur un formulaire en ligne.

À titre de bonne pratique, les responsables du traitement devraient commencer à élaborer les moyens qui contribueront à répondre aux demandes de portabilité des données, comme des outils de téléchargement et des interfaces de programme d'application. Ils devraient garantir que les données à caractère personnel sont transmises dans un format structuré, couramment utilisé et lisible par machine et doivent être encouragés à garantir l'interopérabilité du format de données fourni dans le cadre de l'exercice d'une demande de portabilité des données.

Le présent avis aide également les responsables du traitement à comprendre clairement leurs obligations respectives et recommande des bonnes pratiques et des outils visant à soutenir le respect du droit à la portabilité des données. Enfin, il recommande que les parties prenantes du secteur et les associations professionnelles travaillent de concert sur une série commune de normes et de formats interopérables afin de satisfaire aux exigences liées au droit à la portabilité des données.

I. Introduction

L'article 20 du règlement général sur la protection des données (RGPD) introduit un nouveau droit à la portabilité des données. Ce droit permet aux personnes concernées de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre sans obstacle à un autre responsable du traitement. Ce droit, qui s'applique sous réserve de certaines conditions, encourage le choix et le contrôle de l'utilisateur, ainsi que sa responsabilisation.

Les personnes exerçant leur droit d'accès au titre de la directive 95/46/CE relative à la protection des données étaient limitées par le format choisi par le responsable du traitement lors de la fourniture des informations demandées. **Le nouveau droit à la portabilité des données vise à responsabiliser les personnes concernées au sujet de leurs données à caractère personnel, car il facilite leur capacité à déplacer, à copier ou à transmettre facilement des données à caractère personnel d'un environnement informatique vers un autre** (qu'il s'agisse de leur propre système, du système de tiers de confiance ou de celui de nouveaux responsables du traitement).

En affirmant les droits et le contrôle personnels des particuliers sur les données à caractère personnel les concernant, la portabilité des données représente également une occasion de «rééquilibrer» la relation entre les personnes concernées et les responsables du traitement[1].

Si le droit à la portabilité des données à caractère personnel peut également favoriser la concurrence entre les services (en facilitant le passage d'un service à l'autre), le RGPD réglemente les données à caractère personnel et non la concurrence. En particulier, l'article 20 ne limite pas les données portables à celles qui sont nécessaires ou utiles pour le changement de services[2].

Bien que la portabilité des données soit un nouveau droit, d'autres types de portabilité existent déjà ou sont en cours de discussion dans d'autres domaines de la législation (par exemple, dans le contexte de la résiliation d'un contrat, de l'itinérance des services de communication et de l'accès transfrontière aux services[3]). Certaines synergies, voire des avantages pour les particuliers, peuvent découler de ces différents types de portabilité si ces services sont fournis dans le cadre d'une approche combinée, même si les analogies doivent être traitées avec prudence.

Le présent avis fournit des orientations aux responsables du traitement afin qu'ils puissent mettre à jour leurs pratiques, leurs processus et leurs stratégies, et clarifie la signification de la portabilité des données afin de permettre aux personnes concernées d'exercer efficacement leur nouveau droit.

[1] L'objectif premier de la portabilité des données est de renforcer le contrôle des particuliers sur les données à caractère personnel les concernant et de veiller à ce qu'ils jouent un rôle actif dans l'écosystème des données.
[2] Par exemple, ce droit peut permettre aux banques de proposer des services complémentaires, sous le contrôle de l'utilisateur, en utilisant des données à caractère personnel initialement recueillies dans le cadre d'un service d'approvisionnement en énergie.
[3] Voir le programme de la Commission européenne pour un marché unique numérique: https://ec.europa.eu/digital-agenda/en/digital-single-market, en particulier le premier pilier stratégique intitulé «Améliorer l'accès aux biens et services numériques».

II. Quels sont les principaux éléments de la portabilité des données?

À son article 20, paragraphe 1, le règlement général sur la protection des données définit le droit à la portabilité des données comme suit:

> *Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle […]*

- Le droit de recevoir des données à caractère personnel

Premièrement, la portabilité des données est un **droit des personnes concernées à recevoir un sous-ensemble de données à caractère personnel** les concernant traitées par un responsable du traitement et à les sauvegarder en vue d'un usage personnel ultérieur. Cette sauvegarde peut se faire sur un dispositif privé ou un nuage privé, sans que les données soient nécessairement transmises à un autre responsable du traitement.

À cet égard, la portabilité des données complète le droit d'accès. Une particularité de la portabilité des données réside dans le fait qu'elle offre aux personnes concernées un moyen aisé de gérer et de réutiliser elles-mêmes les données à caractère personnel les concernant. Ces données doivent être reçues «*dans un format structuré, couramment utilisé et lisible par machine*». Par exemple, une personne concernée pourrait vouloir extraire sa liste de chansons actuelle (ou un historique des titres écoutés) d'un service de diffusion en flux de musique afin de voir le nombre de fois qu'elle a écouté certaines chansons ou de décider quelle musique elle souhaite acheter ou écouter sur une autre plate-forme. De la même manière, elle pourrait aussi souhaiter extraire la liste de ses contacts de son application de messagerie, par exemple, pour établir une liste de mariage ou obtenir des informations sur des achats effectués en utilisant différentes cartes de fidélité, ou pour évaluer son empreinte carbone[4].

- Le droit de transmettre les données à caractère personnel d'un responsable du traitement à un autre responsable du traitement

Deuxièmement, l'article 20, paragraphe 1, confère aux personnes concernées le **droit de transmettre les données à caractère personnel d'un responsable du traitement à un autre responsable du traitement** sans que le premier «y fasse obstacle». Les données peuvent aussi être transmises directement d'un responsable du traitement à un autre à la demande de la personne concernée, lorsque cela est techniquement possible (article 20, paragraphe 2). À cet égard, le considérant 68 énonce qu'[i]l y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données[5], mais sans créer, pour les responsables du traitement, d'obligation

[4] Dans ces cas, le traitement des données effectué par la personne concernée peut relever des activités domestiques lorsque le traitement est entièrement effectué sous le seul contrôle de la personne concernée ou être réalisé par une autre partie, au nom de la personne concernée. Dans ce dernier cas, l'autre partie doit être considérée comme le responsable du traitement, y compris aux seules fins de la conservation des données à caractère personnel, et doit respecter les principes et obligations énoncés dans le règlement général.
[5] Voir également la section V.

d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles[6]. Le règlement général sur la protection des données interdit toutefois aux responsables du traitement d'entraver la transmission.

En substance, cet aspect de la portabilité des données habilite les personnes concernées non seulement à obtenir et à réutiliser les données qu'elles ont fournies, mais aussi à les transmettre à un autre prestataire de services (dans le même secteur d'activité ou dans un autre). En plus de responsabiliser le consommateur en empêchant un «verrouillage» des données, le droit à la portabilité des données devrait renforcer les possibilités d'innovation et de partage des données à caractère personnel entre les responsables du traitement de manière sûre et sécurisée, sous le contrôle de la personne concernée[7]. La portabilité des données peut encourager le partage contrôlé et limité par les utilisateurs de données à caractère personnel entre organisations et, partant, enrichir les services et les expériences clients[8]. La portabilité des données peut faciliter la transmission et la réutilisation de données à caractère personnel concernant les utilisateurs entre les différents services qui les intéressent.

[6] Une attention particulière doit par conséquent être accordée au format des données transmises pour garantir que les données peuvent être réutilisées, avec un minimum d'effort, par la personne concernée ou un autre responsable du traitement. Voir également la section V.

[7] Voir plusieurs applications expérimentales en Europe, par exemple MiData au Royaume-Uni ou MesInfos / SelfData par FING en France.

[8] Les industries appartenant aux mouvements du «Quantified Self» et de l'«Internet of Things» ont démontré l'avantage (et les risques) découlant de la mise en relation des données à caractère personnel provenant de différents aspects de la vie d'une personne, comme la forme physique, l'activité sportive et l'absorption de calories, afin de fournir une image plus complète de la vie d'une personne en un seul fichier.

- **Responsabilité**

La portabilité des données garantit le droit de recevoir des données à caractère personnel et de les traiter selon les souhaits de la personne concernée[9].

Les responsables du traitement qui répondent à des demandes de portabilité des données, dans les conditions établies à l'article 20, ne sont pas responsables du traitement effectué par la personne concernée ou par une autre société qui reçoit les données à caractère personnel. Ils agissent au nom de la personne concernée, y compris lorsque les données à caractère personnel sont directement transmises à un autre responsable du traitement. À cet égard, le responsable des données n'est pas responsable de la conformité du responsable du traitement destinataire avec la législation relative à la protection des données, étant donné que ce n'est pas le responsable du traitement émetteur qui choisit le destinataire. En même temps, le responsable du traitement devrait fixer des garanties pour s'assurer qu'il agit réellement au nom de la personne concernée. Il peut par exemple mettre en place des procédures pour s'assurer que le type de données à caractère personnel transmises est effectivement celui que la personne concernée souhaite transmettre. À cet effet, il est possible d'obtenir la confirmation de la personne concernée avant la transmission ou plus tôt, lorsque le consentement original au traitement est donné ou lors de la finalisation du contrat.

Les responsables du traitement répondant à une demande de portabilité des données n'ont aucune obligation particulière de contrôler et de vérifier la qualité des données avant de les transmettre. Bien entendu, ces données doivent déjà être exactes et tenues à jour, conformément aux principes énoncés à l'article 5, paragraphe 1, du règlement général sur la protection des données. La portabilité des données n'oblige par ailleurs pas le responsable du traitement à conserver des données à caractère personnel plus longtemps que nécessaire ou au-delà d'une période de conservation spécifiée[10]. Il est important de noter qu'il n'existe aucune exigence supplémentaire concernant la conservation des données au-delà des périodes de conservation applicables par ailleurs, simplement pour pouvoir répondre de manière positive à toute éventuelle demande future de portabilité des données.

Lorsque les données à caractère personnel demandées sont traitées par un sous-traitant, le contrat conclu en vertu de l'article 28 du règlement général sur la protection des données doit inclure l'obligation d'aider «le responsable du traitement, par des mesures techniques et organisationnelles appropriées, [à] donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits». Le responsable du traitement devrait donc mettre en œuvre des procédures spécifiques en coopération avec ses sous-traitants pour répondre aux demandes de portabilité des données. En cas de responsabilité conjointe, le contrat devrait clairement répartir les responsabilités entre chaque responsable du traitement en ce qui concerne le traitement des demandes de portabilité des données.

Par ailleurs, un responsable du traitement destinataire [11] est chargé de garantir que les données portables fournies sont pertinentes et ne sont pas excessives au regard du nouveau traitement

[9] Le droit à la portabilité des données ne se limite pas aux données à caractère personnel qui sont utiles et pertinentes pour des services similaires fournis par des concurrents du responsable du traitement.
[10] Dans l'exemple ci-dessus, si le responsable du traitement des données ne conserve aucune liste des chansons écoutées par un utilisateur, ces données à caractère personnel ne peuvent être incluses dans une demande de portabilité des données.
[11] C'est-à-dire le responsable du traitement qui reçoit les données à caractère personnel à la suite d'une demande de portabilité des données introduite par la personne concernée auprès d'un autre responsable du traitement.

des données. Par exemple, dans le cas d'une demande de portabilité des données auprès d'un service de messagerie par laquelle la personne concernée souhaite récupérer des courriers électroniques et les envoyer vers une plate-forme d'archivage sécurisée, le nouveau responsable du traitement ne doit pas traiter les coordonnées des correspondants de la personne concernée. Si ces informations ne sont pas pertinentes au regard de la finalité du nouveau traitement, elles ne doivent pas être conservées ni traitées. Dans tous les cas, les responsables du traitement destinataires ne sont pas tenus d'accepter de traiter les données à caractère personnel transmises à la suite d'une demande de portabilité des données. De la même manière, lorsqu'une personne concernée demande à transmettre les détails de ses transactions bancaires à un service qui l'aide à gérer son budget, le responsable du traitement destinataire ne doit pas accepter toutes les données ni conserver tous les détails des transactions une fois qu'elles ont été caractérisées aux fins du nouveau service. En d'autres termes, les données acceptées et conservées devraient se limiter à celles qui sont nécessaires et pertinentes au service fourni par le responsable du traitement destinataire.

Une organisation «destinataire» devient un nouveau responsable du traitement pour ces données à caractère personnel et doit respecter les principes énoncés à l'article 5 du règlement général sur la protection des données. Par conséquent, le «nouveau» responsable du traitement destinataire doit indiquer clairement et directement la finalité du nouveau traitement avant toute demande de transmission des données portables, conformément aux exigences en matière de transparence établies à l'article 14[12]. Comme pour tout traitement de données effectué sous sa responsabilité, le responsable du traitement doit appliquer les principes énoncés à l'article 5, tels que la licéité, la loyauté et la transparence, la limitation des finalités, la minimisation des données, l'exactitude, l'intégrité et la confidentialité, la limitation de la conservation et la responsabilité[13].

Les responsables du traitement détenant des données à caractère personnel doivent être prêts à faciliter l'exercice du droit à la portabilité des données par leurs personnes concernées. Les responsables du traitement peuvent également choisir d'accepter des données provenant d'une personne concernée, mais ils n'y sont pas tenus.

- **Portabilité des données au regard des autres droits des personnes concernées**

Lorsqu'une personne exerce son droit à la portabilité des données, elle le fait sans porter atteinte à aucun autre droit (comme c'est le cas pour tout autre droit prévu par le règlement général sur la protection des données). Une personne concernée peut continuer à utiliser le service du responsable du traitement et à en bénéficier même après une opération de portabilité des données. La portabilité des données ne déclenche pas automatiquement l'effacement des données[14] des systèmes du responsable du traitement et n'a pas d'incidence sur la période de conservation initiale qui s'applique aux données transmises. La personne

[12] En outre, le nouveau responsable du traitement ne doit pas traiter de données à caractère personnel qui ne sont pas pertinentes et le traitement doit être limité à ce qui est nécessaire au regard des nouvelles finalités, même si les données à caractère personnel font partie d'une série de données plus globale transmise au moyen d'un processus de portabilité. Les données à caractère personnel qui ne sont pas nécessaires pour réaliser la finalité du nouveau traitement doivent être supprimées dans les meilleurs délais.

[13] Une fois reçues par le responsable du traitement, les données à caractère personnel envoyées dans le cadre du droit à la portabilité des données peuvent être considérées comme ayant été «fournies» par la personne concernée et être retransmises conformément à ce droit, dans la mesure où les autres conditions applicables à celui-ci (c'est-à-dire la base juridique du traitement, etc.) sont remplies.

[14] Comme indiqué à l'article 17 du règlement général sur la protection des données.

concernée peut exercer ses droits aussi longtemps que le responsable du traitement continue de traiter les données.

De la même manière, si la personne concernée souhaite exercer son droit à l'effacement de ses données («droit à l'oubli» établi à l'article 17), la portabilité des données ne peut être utilisée par un responsable du traitement comme moyen de reporter ou de refuser cet effacement.

Si une personne concernée venait à découvrir que des données à caractère personnel demandées dans le cadre du droit à la portabilité des données ne répondent pas totalement à sa demande, toute autre demande de données à caractère personnel au titre du droit d'accès doit être accueillie complètement, conformément à l'article 15 du règlement général sur la protection des données.

Par ailleurs, lorsqu'un acte législatif spécifique de l'Union ou d'un État membre dans un autre domaine prévoit également une certaine forme de portabilité des données concernées, les conditions établies par ces législations spécifiques doivent aussi être prises en considération lorsqu'il est donné suite à une demande de portabilité des données au titre du règlement général sur la protection des données. S'il ressort clairement de la demande formulée par la personne concernée que son intention n'est pas d'exercer ses droits au titre du règlement général sur la protection des données mais plutôt au titre de la législation sectorielle uniquement, alors, les dispositions du règlement général sur la protection des données relatives à la portabilité des données ne s'appliquent pas à cette demande[15]. Si, en revanche, la demande concerne la portabilité au titre du règlement général sur la protection des données, l'existence de cette législation spécifique est sans préjudice de l'application générale du principe de portabilité des données à tout responsable du traitement, comme le prévoit ledit règlement. Il convient plutôt d'évaluer, au cas par cas, comment cette législation spécifique peut, éventuellement, affecter le droit à la portabilité des données.

III. Quand la portabilité des données s'applique-t-elle?

- Quelles sont les opérations de traitement couvertes par le droit à la portabilité des données?

Le respect du règlement général sur la protection des données exige des responsables du traitement qu'ils se fondent sur une base juridique claire pour le traitement des données à caractère personnel.

Conformément à l'article 20, paragraphe 1, point a), du règlement général sur la protection des données, **pour relever du champ d'application de la portabilité des données**, les opérations de traitement doivent être fondées:

[15] Par exemple, si, par sa demande, la personne concernée cherche spécifiquement à donner accès à l'historique de son compte bancaire à un prestataire de services d'information sur les comptes aux fins énoncées dans la directive sur les services de paiement 2 (DSP2), cet accès doit être octroyé conformément aux dispositions de cette directive.

- sur le consentement de la personne concernée [en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), s'agissant de catégories particulières de données à caractère personnel];

- ou sur un contrat auquel la personne concernée est partie en application de l'article 6, paragraphe 1, point b).

Les titres de livres achetés par une personne sur une librairie en ligne ou les chansons écoutées via un service de diffusion en flux de musique sont des exemples de données à caractère personnel qui relèvent généralement du champ d'application de la portabilité des données, parce qu'elles sont traitées sur la base de l'exécution d'un contrat auquel la personne concernée est partie.

Le règlement général sur la protection des données n'établit aucun droit général à la portabilité des données dans les cas où le traitement des données à caractère personnel ne se fonde pas sur le consentement ou sur un contrat[16]. Par exemple, les établissements financiers n'ont pas l'obligation de donner suite à une demande de portabilité des données concernant les données à caractère personnel traitées dans le cadre de leurs obligations en matière de prévention et de détection du blanchiment d'argent et d'autres formes de criminalité financière. De même, la portabilité des données ne couvre pas les coordonnées professionnelles traitées dans le cadre d'une relation d'entreprise à entreprise lorsque le traitement n'est fondé ni sur le consentement de la personne concernée ni sur un contrat auquel cette personne est partie.

S'agissant des données des employés, le droit à la portabilité des données ne s'applique généralement que si le traitement se fonde sur un contrat auquel la personne concernée est partie. Dans de nombreux cas, le consentement ne sera pas considéré comme ayant été donné librement dans ce contexte, en raison du déséquilibre des pouvoirs entre l'employeur et l'employé[17]. Certains traitements relevant des ressources humaines se fondent plutôt sur la base juridique de l'intérêt légitime, ou sont nécessaires au respect d'obligations juridiques spécifiques dans le domaine de l'emploi. Dans la pratique, le droit à la portabilité des données dans le domaine des ressources humaines concernera incontestablement certaines opérations de traitement (tels que les services de paiement et d'indemnisation ou le recrutement interne), mais dans de nombreuses autres situations, une approche au cas par cas sera nécessaire pour déterminer si toutes les conditions régissant le droit à la portabilité des données sont remplies.

[16] Voir le considérant 68 et l'article 20, paragraphe 3, du règlement général sur la protection des données. L'article 20, paragraphe 3, et le considérant 68 disposent que la portabilité des données ne s'applique pas si le traitement des données est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou si un responsable du traitement exerce ses missions publiques ou respecte une obligation légale. Dès lors, les responsables du traitement ne sont pas obligés de prévoir la portabilité dans ces cas. Toutefois, une bonne pratique consiste à mettre au point des processus visant à répondre automatiquement à des demandes de portabilité, en suivant les principes régissant le droit à la portabilité des données. Un exemple serait un service public fournissant un service de téléchargement facile des précédentes déclarations des revenus des particuliers. Concernant la portabilité des données en tant que bonne pratique dans le cas d'un traitement fondé sur la base juridique de la nécessité d'un intérêt légitime et de régimes volontaires existants, voir les pages 53 et 54 de l'avis 6/2014 du groupe de travail «Article 29» concernant les intérêts légitimes (WP 217).

[17] Comme le groupe de travail «Article 29» l'a souligné dans son avis 8/2001 du 13 septembre 2001 (WP 48).

Enfin, le droit à la portabilité des données s'applique uniquement si le traitement des données «est effectué à l'aide de procédés automatisés» et, par conséquent, ne couvre pas la plupart des dossiers papier.

- **Quelles sont les données à caractère personnel à inclure?**

Conformément à l'article 20, paragraphe 1, les personnes concernées ont le droit de recevoir les données:
- à caractère personnel les concernant et
- qu'elles ont *fournies* à un responsable du traitement.

L'article 20, paragraphe 4, dispose également que le respect de ce droit ne porte pas atteinte aux droits et libertés de tiers.

Première condition: données à caractère personnel relatives à la personne concernée

Seules les données à caractère personnel peuvent faire l'objet d'une demande de portabilité. Par conséquent, toute donnée anonyme[18] ou ne se rapportant pas la personne concernée est exclue du champ d'application. Toutefois, les données pseudonymisées qui peuvent clairement être liées à la personne concernée (par exemple, lorsque la personne concernée fournit l'identifiant correspondant, voir l'article 11, paragraphe 2) relèvent du champ d'application.

Dans de nombreuses circonstances, les responsables du traitement traiteront des informations qui contiennent les données à caractère personnel de plusieurs personnes concernées. Dans un tel cas, les responsables du traitement ne devraient pas interpréter de manière trop restrictive l'expression «données à caractère personnel les concernant [relatives à la personne concernée]». À titre d'exemple, les registres des services de téléphonie, de messagerie interpersonnelle ou de VoIP peuvent inclure (dans l'historique du compte de l'abonné) les coordonnées de tiers concernés par des appels entrants et sortants. Même si les registres contiennent dès lors des données à caractère personnel relatives à plusieurs personnes, les abonnés devraient pouvoir recevoir ceux-ci en réponse à leurs demandes de portabilité des données, étant donné que les registres se rapportent (également) à la personne concernée. Toutefois, lorsque ces registres sont ensuite transmis à un nouveau responsable du traitement, ce dernier ne doit pas les traiter pour une finalité qui porterait atteinte aux droits et libertés de tiers (voir ci-dessous: troisième condition).

Deuxième condition: données fournies par la personne concernée

La deuxième condition restreint le champ d'application aux données «fournies» par la personne concernée.

Il existe de nombreux exemples de données à caractère personnel qui sont sciemment et activement «fournies» par la personne concernée, comme les données relatives à un compte (par exemple, adresse postale, nom d'utilisateur, âge) transmises via des formulaires en ligne. Néanmoins, les données «fournies» par la personne concernée peuvent également découler de l'observation de l'activité de cette dernière. Par conséquent, le groupe de travail «Article 29»

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

considère que pour donner tout son effet à ce nouveau droit, il convient que le terme «fournies» couvre également les données personnelles qui sont observées dans le cadre des activités des utilisateurs, telles que les données brutes traitées par un compteur intelligent ou d'autres types d'objets connectés[19], les journaux d'activités, l'historique d'utilisation d'un site web ou des activités de recherche.

Cette dernière catégorie de données n'inclut pas les données qui sont générées par le responsable du traitement (au moyen des données observées ou directement fournies comme intrants), telles qu'un profil d'utilisateur créé par l'analyse des données brutes collectées à partir d'un compteur intelligent.

Une distinction peut être opérée entre différentes catégories de données, en fonction de leur origine, afin de déterminer si elles sont couvertes par le droit à la portabilité des données. Les catégories suivantes peuvent être qualifiées de données «fournies par la personne concernée»:

- **les données activement et sciemment fournies par la personne concernée** (par exemple, adresse postale, nom d'utilisateur, âge, etc.);
- **les données observées fournies par la personne concernée grâce à l'utilisation du service ou du dispositif**. Ces données peuvent inclure, par exemple, l'historique de recherche, les données relatives au trafic et les données de localisation d'une personne. Elles peuvent aussi inclure d'autres données brutes comme le rythme cardiaque enregistré par un dispositif portable.

En revanche, les données déduites et les données dérivées sont créées par le responsable du traitement sur la base des données «fournies par la personne concernée». Par exemple, le résultat d'une appréciation relative à la santé d'un utilisateur ou un profil créé dans le contexte des règlementations relatives à la gestion des risques et de la réglementation financière (par ex., pour attribuer une cote de solvabilité ou respecter les règles en matière de lutte contre le blanchiment d'argent) ne peuvent pas être considérés en soi comme ayant été «fournis» par la personne concernée. Bien que ces données puissent faire partie d'un profil conservé par un responsable du traitement et soient déduites ou dérivées d'une analyse des données fournies par la personne concernée (par ses actions, par exemple), ces données ne seront généralement pas considérées comme étant «fournies par la personne concernée» et ne relèveront dès lors pas du champ d'application de ce nouveau droit[20].

En général, compte tenu des objectifs stratégiques du droit à la portabilité des données, l'expression «fournies par la personne concernée» doit être interprétée au sens large, et devrait exclure les «données déduites» et les «données dérivées», qui incluent les données à caractère personnel qui sont créées par un prestataire de services (par exemple, des résultats algorithmiques). Un responsable du traitement peut exclure ces données déduites, mais doit

[19] En ayant la possibilité d'extraire les données résultant de l'observation de son activité, la personne concernée pourra également disposer d'un meilleur aperçu des choix de mise en œuvre posés par le responsable du traitement en ce qui concerne la portée des données observées et sera plus à même de choisir les données qu'elle est prête à fournir pour obtenir un service similaire, de même qu'elle saura dans quelle mesure son droit à la vie privée est respecté.

[20] Néanmoins, la personne concernée peut continuer à exercer son «droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel», ainsi que son droit d'accès à des informations concernant «l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée», conformément à l'article 15 du règlement général sur la protection des données (qui fait référence au droit d'accès).

inclure toutes les autres données à caractère personnel fournies par la personne concernée via les moyens techniques mis à disposition par le responsable du traitement[21].

Par conséquent, l'expression «fournies par» englobe les données à caractère personnel qui se rapportent à l'activité de la personne concernée ou qui résultent de l'observation du comportement d'une personne, mais exclut les données résultant d'une analyse subséquente de ce comportement. En revanche, les données à caractère personnel qui ont été créées par le responsable du traitement dans le cadre du traitement des données, par exemple, par un processus de personnalisation ou de recommandation, par catégorisation ou profilage des utilisateurs, sont des données qui sont dérivées ou déduites des données à caractère personnel fournies par la personne concernée et elles ne sont pas couvertes par le droit à la portabilité des données.

Troisième condition: le droit à la portabilité des données ne doit pas porter atteinte aux droits et libertés de tiers

En ce qui concerne les données à caractère personnel relatives à d'autres personnes concernées:

La troisième condition vise à empêcher l'extraction et la transmission de données contenant les données à caractère personnel d'autres personnes concernées (non consentantes) à un nouveau responsable du traitement dans le cas où ces données sont susceptibles d'être traitées d'une manière qui porterait atteinte aux droits et aux libertés des autres personnes concernées (article 20, paragraphe 4, du règlement général sur la protection des données)[22].

Une telle atteinte interviendrait, par exemple, si la transmission de données d'un responsable du traitement à un autre empêchait des tiers d'exercer leurs droits en tant que personnes concernées en vertu du règlement général sur la protection des données (comme le droit à l'information, le droit d'accès, etc.).

La personne concernée qui initie la transmission des données la concernant à un autre responsable du traitement soit donne son consentement au nouveau responsable du traitement aux fins du traitement de ses données, soit conclut un contrat avec ce dernier. Lorsque des données à caractère personnel de tiers sont comprises dans l'ensemble de données, une autre base juridique doit être définie pour le traitement. Par exemple, un intérêt légitime peut être poursuivi par le responsable du traitement au titre de l'article 6, paragraphe 1, point f), en particulier lorsque l'objectif du responsable du traitement est de fournir à la personne concernée un service qui permet à cette dernière de traiter des données à caractère personnel dans le cadre d'une activité purement personnelle ou domestique. L'opération de traitement initiée par la personne concernée dans le cadre d'une activité personnelle qui concerne et

[21] Sont incluses toutes les données observées au sujet de la personne concernée durant les activités pour lesquelles les données sont collectées, comme l'historique des transactions ou le protocole des accès. Les données collectées au moyen du suivi et de l'enregistrement de la personne concernée (comme une application enregistrant le rythme cardiaque ou une technologie utilisée pour suivre le comportement de navigation sur le web) doivent également être considérées comme étant «fournies par» la personne concernée, même si les données ne sont pas activement ou sciemment transmises.

[22] Le considérant 68 dispose que «[l]orsque, dans un ensemble de données à caractère personnel, plusieurs personnes sont concernées, le droit de recevoir les données à caractère personnel devrait s'entendre sans préjudice des droits et libertés des autres personnes concernées conformément au présent règlement».

affecte potentiellement des tiers reste de sa responsabilité dans la mesure où ce traitement n'est, en aucune manière, décidé par le responsable du traitement.

Par exemple, un service de messagerie peut permettre la création d'un répertoire de contacts, d'amis, de parents, de membres de la famille et de connaissances plus éloignées d'une personne concernée. Dans la mesure où ces données concernent la personne identifiable qui souhaite exercer son droit à la portabilité des données (et sont créées par celle-ci), les responsables du traitement doivent transmettre à cette personne concernée l'ensemble du répertoire des courriers électroniques entrants et sortants.

De même, le compte bancaire d'une personne concernée peut contenir des données à caractère personnel relatives aux transactions non seulement du titulaire du compte, mais aussi d'autres personnes (par exemple en cas de virement d'argent au titulaire du compte). Il est peu probable que les droits et libertés de ces tiers soient compromis par la transmission des informations concernant le compte bancaire au titulaire du compte dans le cadre d'une demande de portabilité, pour autant que, dans les deux exemples, les données soient utilisées à la même fin (c'est-à-dire, une adresse de contact utilisée uniquement par la personne concernée ou l'historique du compte bancaire de la personne concernée).

À l'inverse, les droits et libertés des tiers ne seront pas respectés si le nouveau responsable du traitement utilise les données à caractère personnel à d'autres fins, par exemple, si le responsable du traitement destinataire des données utilise les données à caractère personnel d'autres personnes figurant dans le carnet d'adresses de la personne concernée à des fins de marketing.

Par conséquent, afin d'éviter qu'il soit porté atteinte aux tiers concernés, le traitement de ces données à caractère personnel par un autre responsable du traitement est permis uniquement dans la mesure où les données sont conservées sous le seul contrôle de l'utilisateur demandeur et sont gérées uniquement à des fins purement personnelles ou domestiques. Un «nouveau» responsable du traitement destinataire (auquel les données peuvent être transmises à la demande de l'utilisateur) ne peut pas utiliser les données de tiers qui lui sont transmises à des fins qui lui sont propres, par exemple pour proposer des produits et services de marketing à ces autres tierces personnes concernées. Par exemple, ces informations ne doivent pas être utilisées pour enrichir le profil de la tierce personne concernée et reconstruire son environnement social, sans qu'elle en soit informée et qu'elle y ait consenti[23]. Elles ne peuvent pas non plus être utilisées pour extraire des informations concernant ces tiers et créer des profils spécifiques, même si le responsable du traitement est déjà en possession de leurs données à caractère personnel. Dans le cas contraire, ce traitement est susceptible d'être illicite et abusif, en particulier si les tiers concernés ne sont pas informés et ne peuvent exercer leurs droits en tant que personnes concernées.

Par ailleurs, il est de bonne pratique pour tous les responsables du traitement (qu'il s'agisse de la partie émettrice ou destinataire des données) de mettre en œuvre des outils permettant aux personnes concernées de choisir les données qu'elles souhaitent recevoir et transmettre et d'exclure, le cas échéant, les données d'autres personnes. Cette manière de procéder

[23] Un service de réseaux sociaux ne doit pas enrichir le profil de ses membres en utilisant des données à caractère personnel transmises par une personne concernée dans le cadre de son droit à la portabilité des données sans respecter le principe de transparence et veiller à ce que ce traitement spécifique repose sur une base juridique appropriée.

contribuera à réduire les risques pour les tiers dont les données à caractère personnel pourraient être concernées par la portabilité.

Par ailleurs, les responsables du traitement devraient mettre en place des mécanismes de consentement applicables à d'autres personnes concernées, afin de faciliter la transmission de données dans les cas où ces parties veulent donner leur consentement, par exemple si celles-ci veulent également transférer leurs données à un autre responsable du traitement. Cette situation peut se produire, par exemple, dans le cas des réseaux sociaux, mais il appartient aux responsables du traitement de décider de la meilleure pratique à suivre.

En ce qui concerne les données couvertes par la propriété intellectuelle et le secret des affaires:
Les droits et libertés d'autrui sont mentionnés à l'article 20, paragraphe 4. Bien qu'elle ne soit pas directement liée à la portabilité, cette notion peut s'entendre comme incluant le «secret des affaires ou [...] la propriété intellectuelle, notamment [le] droit d'auteur protégeant le logiciel». Toutefois, s'il convient de prendre en considération ces droits avant de répondre à une demande de portabilité des données, «ces considérations ne devraient pas aboutir à refuser toute communication d'informations à la personne concernée». En outre, le responsable du traitement ne doit pas rejeter une demande de portabilité des données sur la base d'une violation d'un autre droit contractuel (par exemple, une dette en suspens ou un litige commercial avec la personne concernée).

Le droit à la portabilité des données n'est pas un droit permettant à une personne d'abuser des informations d'une manière qui pourrait être qualifiée de déloyale ou qui constituerait une violation des droits de propriété intellectuelle.

Toutefois, un risque commercial potentiel ne saurait, en soi, motiver un refus de répondre à la demande de portabilité et les responsables du traitement peuvent transmettre les données à caractère personnel fournies par les personnes concernées sous une forme qui ne divulgue pas des informations couvertes par le secret des affaires ou par des droits de propriété intellectuelle.

IV. De quelle manière les règles générales régissant l'exercice des droits de la personne concernée s'appliquent-elles à la portabilité des données?

- **Quelles sont les informations préalables à fournir à la personne concernée?**

Afin de respecter le nouveau droit à la portabilité des données, les responsables du traitement doivent informer les personnes concernées de l'existence de ce nouveau droit. Lorsque les données à caractère personnel concernées sont collectées directement auprès de la personne concernée, cette information doit avoir lieu «au moment où les données en question sont obtenues». Si les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, le responsable du traitement doit fournir les informations requises par l'article 13, paragraphe 2, point b), et l'article 14, paragraphe 2, point c).

«Lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée», l'article 14, paragraphe 3, exige que les informations soient fournies dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas

un mois, au moment de la première communication avec la personne concernée ou lorsque les données à caractère personnel sont communiquées à des tiers[24].

Lorsqu'ils fournissent les informations requises, les responsables du traitement doivent veiller à opérer une distinction entre le droit à la portabilité des données et les autres droits. Par conséquent, le groupe de travail «Article 29» recommande en particulier que les responsables du traitement expliquent clairement la différence entre les types de données qu'une personne concernée peut recevoir en exerçant son droit d'accès et son droit à la portabilité.

En outre, le groupe de travail recommande que les responsables du traitement incluent toujours des informations concernant le droit à la portabilité des données avant toute clôture de compte par une personne concernée. Cette mesure permet aux utilisateurs de faire le point sur leurs données à caractère personnel et de les transférer facilement vers leur propre dispositif ou tout autre prestataire avant la résiliation d'un contrat.

Enfin, en tant que meilleure pratique pour les responsables du traitement «destinataires», le groupe de travail «Article 29» recommande que les personnes concernées reçoivent des informations complètes sur la nature des données à caractère personnel qui sont pertinentes aux fins de l'exécution des services considérés. Outre qu'elle renforce le caractère loyal du traitement, cette pratique permet aux utilisateurs de limiter les risques pour les tiers, ainsi que toute autre duplication inutile de données à caractère personnel, même lorsqu'aucune autre personne n'est concernée.

- **De quelle manière le responsable du traitement peut-il identifier la personne concernée avant de répondre à sa demande?**

Le règlement général sur la protection des données ne contient aucune prescription normative concernant la manière d'authentifier la personne concernée. Néanmoins, l'article 12, paragraphe 2, dudit règlement dispose que le responsable du traitement ne peut pas refuser de donner suite à la demande de la personne concernée d'exercer ses droits (y compris le droit à la portabilité des données), à moins qu'il ne traite des données à caractère personnel pour une finalité qui n'exige pas l'identification d'une personne concernée et qu'il puisse démontrer qu'il n'est pas en mesure d'identifier la personne concernée. Toutefois, conformément à l'article 11, paragraphe 2, en pareils cas, la personne concernée peut fournir des informations complémentaires qui permettent de l'identifier. Par ailleurs, l'article 12, paragraphe 6, dispose que lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne concernée, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée. Lorsqu'une personne concernée fournit des informations complémentaires permettant de l'identifier, le responsable du traitement ne peut refuser de donner suite à la demande. Lorsque les informations et données collectées en ligne sont liées à des pseudonymes ou à des identifiants uniques, les responsables du traitement peuvent appliquer des procédures appropriées permettant à une personne de présenter une demande de portabilité des données et de recevoir des données la concernant. En tout état de cause, les responsables du traitement doivent appliquer une procédure d'authentification afin d'établir avec certitude l'identité de la

[24] L'article 12 exige que le responsable du traitement procède à «toute communication […] d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant.»

personne concernée demandant ses données à caractère personnel ou, plus généralement, exerçant les droits conférés par le règlement général sur la protection des données.

Ces procédures existent déjà souvent. À l'heure actuelle, les personnes concernées sont souvent déjà authentifiées par le responsable du traitement avant la conclusion d'un contrat ou la collecte de leur consentement au traitement. Par conséquent, les données à caractère personnel utilisées pour enregistrer la personne concernée par le traitement peuvent également être utilisées comme preuves pour l'authentification de cette personne aux fins de la portabilité[25].

Si, en pareils cas, l'identification préalable des personnes concernées peut nécessiter une demande de preuve de leur identité légale, cette vérification peut ne pas être pertinente pour évaluer le lien entre les données et la personne concernée, étant donné que ce lien est sans rapport avec l'identité officielle ou légale. Fondamentalement, la possibilité, pour le responsable du traitement, de demander à la personne concernée des informations complémentaires destinées à vérifier son identité ne peut donner lieu à des exigences excessives ni à la collecte de données à caractère personnel qui ne sont pas pertinentes ni nécessaires au renforcement du lien entre la personne et les données à caractère personnel demandées.

Dans de nombreux cas, de telles procédures d'authentification sont déjà en place. Par exemple, les noms d'utilisateur et les mots de passe sont souvent utilisés pour permettre à des personnes d'accéder à leurs données contenues dans leurs comptes de messagerie, leurs comptes sur des réseaux sociaux et les comptes utilisés pour différents services, que certaines personnes choisissent d'utiliser sans révéler leurs identité et nom complets.

Si le volume des données demandées par la personne concernée rend la transmission via l'internet problématique, au lieu de prévoir éventuellement une prolongation de délai de maximum trois mois afin de répondre à cette demande[26], le responsable du traitement pourrait également devoir envisager d'autres moyens de transmettre les données, notamment en utilisant la diffusion en flux ou le stockage sur un CD, un DVD ou d'autres supports physiques ou en autorisant que les données à caractère personnel soient transmises directement à un autre responsable du traitement (conformément à l'article 20, paragraphe 2, du règlement général sur la protection des données, lorsque cela est techniquement possible).

- **Quel est le délai imparti pour répondre à une demande de portabilité?**

L'article 12, paragraphe 3, requiert que le responsable du traitement fournisse à la personne concernée «des informations sur les mesures prises» «dans les meilleurs délais» et en tout état de cause «dans un délai d'un mois à compter de la réception de la demande». Ce délai d'un mois peut être prolongé à un maximum de trois mois pour les affaires complexes, à condition que la personne concernée ait été informée des motifs de cette prolongation dans un délai d'un mois à compter de la réception de la demande initiale.

Les responsables du traitement fournissant des services informatiques sont susceptibles d'être mieux équipés pour pouvoir répondre à des demandes dans un délai très court. Afin de

[25] Par exemple, lorsque le traitement des données est lié à un compte d'utilisateur, la communication de l'identifiant et du mot de passe correspondant à ce compte peut suffire à identifier la personne concernée.
[26] Article 12, paragraphe 3: «Le responsable du traitement fournit des informations sur les mesures prises à la suite d'une demande».

répondre aux attentes de l'utilisateur, une bonne pratique consiste à définir le délai dans lequel une réponse peut d'ordinaire être donnée à une demande de portabilité de données et à communiquer cette information aux personnes concernées.

Le responsable du traitement qui ne donne pas suite à une demande de portabilité informe la personne concernée, conformément à l'article 12, paragraphe 4, «des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel», dans un délai maximal d'un mois à compter de la réception de la demande.

Les responsables du traitement doivent respecter l'obligation de répondre à la demande dans les conditions prescrites, même s'il s'agit de signifier un refus. En d'autres termes, le responsable du traitement est tenu de répondre à une demande de portabilité des données.

- **Dans quels cas une demande de portabilité des données peut-elle être rejetée ou subordonnée au paiement de frais?**

L'article 12 interdit au responsable du traitement d'exiger un paiement pour fournir les données à caractère personnel, à moins qu'il puisse démontrer que les demandes sont manifestement infondées ou excessives, «notamment en raison de leur caractère répétitif». Pour les services de la société de l'information spécialisés dans le traitement automatisé de données à caractère personnel, la mise en œuvre de systèmes automatisés, tels que des interfaces de programme d'application (API)[27], peut faciliter les échanges avec les personnes concernées et donc alléger la charge potentielle découlant de demandes répétées. Par conséquent, les cas dans lesquels le responsable du traitement peut justifier un refus de fournir les informations demandées devraient être très rares, même lorsqu'il est question de demandes multiples de portabilité des données.

En outre, le coût global des processus créés pour répondre aux demandes de portabilité des données ne devrait pas être pris en considération pour déterminer le caractère excessif d'une demande. En effet, l'article 12 du règlement général sur la protection des données se concentre sur les demandes introduites par une personne concernée et non sur le nombre total de demandes reçues par le responsable du traitement. En conséquence, les coûts totaux liés à la mise en œuvre du système ne devraient pas être imputés aux personnes concernées ni invoqués pour justifier un refus de répondre à des demandes de portabilité.

V. De quelle manière les données portables doivent-elles être fournies?

- **Quels sont les moyens que le responsable du traitement est censé mettre en œuvre pour fournir les données?**

L'article 20, paragraphe 1, du règlement général sur la protection des données dispose que les personnes concernées ont le droit de transmettre les données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle.

[27] Le terme «interface de programme d'application» (API) désigne les interfaces d'applications ou les services web mis à disposition par les responsables du traitement de sorte que d'autres systèmes ou applications puissent se mettre en relation avec leurs systèmes et travailler avec ceux-ci.

Il peut s'agir d'entraves juridiques, techniques ou financières mises en place par le responsable du traitement pour empêcher ou ralentir l'accès aux données, leur transmission ou leur réutilisation par la personne concernée ou par un autre responsable du traitement, par exemple, des frais demandés pour la fourniture des données; un manque d'interopérabilité ou l'absence d'accès à un format de données ou à une interface de programme d'application ou le format fourni; des délais ou une complexité excessifs pour extraire l'intégralité de l'ensemble de données; l'obscurcissement délibéré de l'ensemble de données; ou encore une normalisation sectorielle ou des exigences en matière d'accréditation spécifiques et abusives ou excessives[28].

L'article 20, paragraphe 2, fait également obligation aux responsables du traitement de transmettre directement les données portables à d'autres responsables du traitement «lorsque cela est techniquement possible».

La possibilité technique de la transmission de responsable du traitement à responsable du traitement, sous le contrôle de la personne concernée, doit être évaluée au cas par cas. Le considérant 68 précise les limites de ce qui est «techniquement possible», indiquant que ce droit «ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles».

Les responsables du traitement sont censés transmettre les données à caractère personnel dans un format interopérable, bien que cela n'oblige pas les autres responsables du traitement à prendre en charge ces formats. La transmission directe d'un responsable du traitement à un autre peut par conséquent avoir lieu lorsque la communication entre deux systèmes est possible, de manière sécurisée[29], et lorsque le système récepteur est techniquement en mesure de recevoir les données entrantes. Si des entraves techniques empêchent la transmission directe, le responsable du traitement doit expliquer celles-ci à la personne concernée, car, dans le cas contraire, sa décision sera considérée comme semblable, dans ses effets, à un refus de donner suite à la demande formulée par la personne concernée (article 12, paragraphe 4).

Du point de vue technique, les responsables du traitement devraient envisager et évaluer deux modes différents et complémentaires pour mettre les données portables à la disposition des personnes concernées ou d'autres responsables du traitement:

- une transmission directe de l'intégralité de l'ensemble de données portables (ou plusieurs extraits de parties de l'ensemble global de données);
- un outil automatisé permettant l'extraction des données pertinentes.

Le deuxième mode de transmission peut être privilégié par les responsables du traitement dans les cas impliquant des ensembles de données volumineux et complexes, étant donné qu'il permet l'extraction de toute partie de l'ensemble de données pertinente pour la personne concernée dans le cadre de sa demande, peut contribuer à réduire le risque au minimum et

[28] Certaines entraves légitimes peuvent survenir, par exemple celles qui sont liées aux droits et libertés de tiers visés à l'article 20, paragraphe 4, ou celles qui ont trait à la sécurité des propres systèmes des responsables du traitement. Il incombe au responsable du traitement de justifier en quoi ces entraves sont justifiées et pourquoi il ne s'agit pas d'obstacles au sens de l'article 20, paragraphe 1.
[29] Par une communication authentifiée présentant le niveau de chiffrement des données nécessaire.

permet éventuellement l'utilisation de mécanismes de synchronisation[30] (par exemple, dans le contexte d'une communication régulière entre responsables du traitement). Il peut s'agir d'une meilleure manière d'assurer la conformité pour le «nouveau» responsable du traitement et constituerait une bonne pratique en ce qui concerne la réduction des risques liés à la confidentialité de la part du responsable du traitement initial.

Ces deux manières différentes et éventuellement complémentaires de fournir les données portables pertinentes pourraient être mises en œuvre par la mise à disposition des données au moyen, par exemple, de messages sécurisés, d'un serveur SFTP, d'une interface de programme d'application web ou d'un portail web sécurisés. Les personnes concernées devraient avoir la possibilité d'utiliser un entrepôt de données personnelles, un système de gestion des informations personnelles[31] ou d'autres types de services de tiers de confiance pour conserver et stocker leurs données à caractère personnel et accorder aux responsables du traitement l'autorisation d'accéder aux données personnelles et de les traiter en tant que de besoin.

- **Quel est le format de données attendu?**

Le règlement général sur la protection des données exige du responsable du traitement qu'il fournisse les données à caractère personnel demandées par la personne concernée dans un format qui permet leur réutilisation. Plus spécifiquement, l'article 20, paragraphe 1, du règlement général sur la protection des données dispose que les données à caractère personnel doivent être fournies «dans un format structuré, couramment utilisé et lisible par machine». Le considérant 68 précise que ce format doit être interopérable, un terme qui est défini[32] comme suit dans l'Union:

> *la capacité de diverses organisations hétérogènes à interagir en vue d'atteindre des objectifs communs, mutuellement avantageux et convenus, impliquant le partage d'informations et de connaissances entre elles, selon les processus d'entreprise qu'elles prennent en charge, par l'échange de données entre leurs systèmes TIC respectifs.*

Les qualificatifs «structuré», «couramment utilisé» et «lisible par machine» constituent une série d'exigences minimales qui devraient faciliter l'interopérabilité du format de données fourni par le responsable du traitement. En ce sens, les termes «structuré, couramment utilisé et lisible par machine» donnent des précisions sur les moyens, tandis que l'interopérabilité est le résultat escompté.

Le considérant 21 de la directive 2013/37/UE[33] [34]définit le format «lisible par machine» comme suit:

[30] Les mécanismes de synchronisation contribuent au respect de l'obligation générale établie à l'article 5 du règlement général sur la protection des données, qui dispose que les données à caractère personnel «doivent être [...] exactes et, si nécessaire, tenues à jour».
[31] Pour les systèmes de gestion des informations personnelles (PIMS), voir, par exemple, l'avis 9/2016 du CEPD, à l'adresse:https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_fr.pdf
[32] Article 2 de la décision nº 922/2009/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant des solutions d'interopérabilité pour les administrations publiques européennes (ISA), JO L 260 du 3.10.2009, p. 20.
[33] Modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public.

> *un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d'un fait et sa structure interne. Les données encodées présentes dans des fichiers qui sont structurés dans un format lisible par machine sont des données lisibles par machine. Les formats lisibles par machine peuvent être ouverts ou propriétaires; il peut s'agir de normes formelles ou non. Les documents encodés dans un format de fichier qui limite le traitement automatique, en raison du fait que les données ne peuvent pas, ou ne peuvent pas facilement, être extraites de ces documents, ne devraient pas être considérés comme des documents dans des formats lisibles par machine. Les États membres devraient, le cas échéant, encourager l'utilisation de formats ouverts, lisibles par machine.*

Compte tenu de la grande variété de types de données potentiels qui pourraient être traités par un responsable du traitement, le règlement général sur la protection des données n'impose pas de recommandations spécifiques quant au format des données à caractère personnel à fournir. Le format le plus approprié différera d'un secteur à l'autre et des formats adéquats peuvent déjà exister, et doivent toujours être choisis de manière à pouvoir être interprétés et offrir à la personne concernée un degré élevé de portabilité. Dès lors, les formats qui sont soumis à des contraintes de licences onéreuses ne sont pas considérés comme relevant d'une approche adéquate.

Le considérant 68 précise que «*[l]e droit de la personne concernée de transmettre ou de recevoir des données à caractère personnel la concernant ne devrait pas créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles*». **Dès lors, la portabilité vise à produire des systèmes interopérables, et non des systèmes compatibles**[35].

Les données à caractère personnel devraient être fournies dans des formats dont le niveau d'abstraction par rapport à tout format interne ou propriétaire est élevé. En tant que telle, la portabilité des données suppose un traitement des données supplémentaire par les responsables du traitement, afin d'extraire les données des plates-formes et de filtrer les données à caractère personnel hors du champ d'application de la portabilité, comme les données déduites ou les données liées à la sécurité des systèmes. Ainsi, les responsables du traitement sont encouragés à recenser préalablement les données qui relèvent du champ d'application de la portabilité dans leurs propres systèmes. Ce traitement de données supplémentaire sera considéré comme accessoire au traitement des données principal parce qu'il n'est pas effectué pour réaliser une nouvelle finalité définie par le responsable du traitement.

Lorsqu'aucun format n'est d'usage courant dans un secteur ou un contexte donné, **les responsables du traitement devraient fournir les données à caractère personnel au moyen de formats ouverts communément utilisés (par exemple XML, JSON, CSV, etc.), assortis de métadonnées** utiles **au meilleur niveau de granularité possible,** tout en maintenant un niveau d'abstraction élevé. À cet effet, il convient d'utiliser des métadonnées

[34] Le glossaire de l'UE (http://eur-lex.europa.eu/eli-register/glossary.html) fournit davantage de précisions quant aux attentes liées aux notions utilisées dans les présentes lignes directrices, telles que *lisible par machine, interopérabilité*, *format ouvert*, *norme* ou *métadonnées*.

[35] La norme ISO/IEC 2382-01 définit l'interopérabilité comme suit: «La possibilité de communiquer, d'exécuter des programmes, ou de transférer des données entre diverses unités fonctionnelles d'une façon qui n'exige que peu, voire aucune connaissance des caractéristiques particulières de ces unités de la part de l'utilisateur».

appropriées afin de décrire précisément la signification des informations échangées. Ces métadonnées devraient être suffisantes pour rendre possibles la fonction et la réutilisation des données, sans, bien entendu, violer le secret des affaires. Il est par conséquent peu probable qu'une version PDF d'une boîte de messagerie électronique fournie à une personne soit suffisamment structurée ou descriptive pour permettre la réutilisation aisée des données de la boîte de messagerie. Les données contenues dans les courriers électroniques devraient plutôt être fournies dans un format qui préserve toutes les métadonnées, afin de permettre une réutilisation efficace des données. À cet effet, lorsqu'il sélectionne un format de données dans lequel fournir les données à caractère personnel, le responsable du traitement doit examiner en quoi ce format pourrait affecter ou entraver le droit de la personne à réutiliser les données. Dans les cas où un responsable du traitement est en mesure de fournir à la personne concernée des choix quant au format de données à caractère personnel qu'elle préfère, il doit expliquer clairement l'incidence de ce choix. Toutefois, le traitement de métadonnées supplémentaires uniquement parce qu'elles pourraient être nécessaires ou souhaitées dans le cadre d'une demande de portabilité des données ne constitue pas un motif légitime pour ce traitement.

Le groupe de travail «Article 29» encourage la coopération entre les parties prenantes de l'industrie et les associations professionnelles afin qu'elles travaillent de concert sur une série commune de normes et de formats interopérables en vue de satisfaire aux exigences liées au droit à la portabilité des données. Ce défi a également été relevé par le cadre d'interopérabilité européen (EIF, European Interoperability Framework), qui a défini une approche commune de l'interopérabilité pour les organisations souhaitant collaborer en vue de la fourniture de services publics. Au sein de son champ d'application, le cadre définit un ensemble d'éléments communs tels que le vocabulaire, les concepts, les principes, les politiques, les lignes directrices, les recommandations, les normes, les spécifications et les pratiques[36].

- **Comment traiter une collecte de données à caractère personnel de grande ampleur ou complexe?**

Le règlement général sur la protection des données n'explique pas comment relever le défi d'une collecte de données de grande ampleur, d'une structure de données complexe ou d'autres problèmes techniques susceptibles de créer des difficultés pour les responsables du traitement ou les personnes concernées.

Toutefois, dans tous les cas, il est capital que la personne soit en mesure de comprendre pleinement la définition, le schéma et la structure des données à caractère personnel qui pourraient être fournies par le responsable du traitement. Par exemple, les données pourraient d'abord être fournies dans un format résumé au moyen de tableaux permettant à la personne concernée de transmettre des sous-ensembles de données à caractère personnel plutôt que l'intégralité de celles-ci. Le responsable du traitement doit fournir un aperçu «d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples» (voir l'article 12, paragraphe 1, du règlement général sur la protection des données), de manière à ce que la personne concernée dispose toujours d'informations claires quant aux données à télécharger ou à transmettre à un autre responsable du traitement en relation avec une finalité donnée. Par exemple, les personnes concernées doivent être en mesure d'utiliser des applications logicielles afin d'identifier, de reconnaître et de traiter facilement des données spécifiques.

[36] Source: http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

Comme indiqué ci-dessus, une manière pratique permettant à un responsable du traitement de répondre à des demandes de portabilité des données pourrait consister à offrir une API dûment sécurisée et documentée. Les personnes concernées pourraient ainsi introduire auprès du responsable du traitement des demandes de données à caractère personnel via leur propre logiciel ou le logiciel d'un tiers ou accorder à d'autres (y compris un autre responsable du traitement) la permission de le faire en leur nom, comme précisé à l'article 20, paragraphe 2, du règlement général sur la protection des données. En accordant l'accès à des données par l'intermédiaire d'une interface de programme d'application accessible depuis l'extérieur, il pourrait également être possible de proposer un système d'accès plus sophistiqué permettant aux personnes d'introduire des demandes de données ultérieures, sous la forme soit d'un téléchargement complet, soit d'une fonction delta contenant uniquement les modifications apportées depuis le dernier téléchargement, sans que ces demandes supplémentaires soient onéreuses pour le responsable du traitement.

- **De quelle manière les données portables peuvent-elles être sécurisées?**

En général, conformément à l'article 5, paragraphe 1, point f), du règlement général sur la protection des données, les responsables du traitement doivent garantir la «sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées».

Toutefois, la transmission des données à caractère personnel à la personne concernée peut aussi poser des problèmes de sécurité:

Comment les responsables du traitement peuvent-ils garantir la fourniture sécurisée de données à caractère personnel à la bonne personne?

La portabilité des données étant destinée à extraire des données à caractère personnel du système d'information du responsable du traitement, la transmission peut devenir une source de risque possible pour ces données (en particulier, un risque de violation des données pendant la transmission). Il incombe au responsable du traitement de prendre toutes les mesures de sécurité qui s'imposent afin de garantir non seulement la transmission sécurisée des données à caractère personnel (par exemple, en utilisant le chiffrement de bout en bout ou le cryptage de données) au bon destinataire (par exemple, en utilisant des informations d'authentification fortes), mais aussi de maintenir la protection des données à caractère personnel qui restent dans ses systèmes, ainsi que d'établir des procédures transparentes pour remédier aux éventuelles violations des données[37]. Pour ce faire, il doit évaluer les éventuels risques spécifiques liés à la portabilité des données et prendre les mesures d'atténuation des risques appropriées.

Les mesures d'atténuation des risques précitées pourraient inclure: si la personne concernée doit déjà s'authentifier, l'utilisation d'informations d'authentification supplémentaires, telles qu'un secret partagé ou un autre élément d'authentification comme un mot de passe à usage unique; la suspension ou le gel de la transmission, s'il existe une suspicion de compromission du compte; en cas de transmission directe d'un responsable du traitement à un autre, il convient d'utiliser une authentification par mandat, telle que l'authentification par jeton.

[37] Conformément à la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

De telles mesures de sécurité ne doivent pas être obstructives par nature et ne doivent pas empêcher les utilisateurs d'exercer leurs droits, notamment en imposant des coûts supplémentaires.

Comment aider les utilisateurs à sécuriser le stockage de leurs données à caractère personnel dans leur propre système?

En récupérant leurs données à caractère personnel d'un service en ligne, les utilisateurs courent toujours le risque de stocker ces données dans des systèmes moins sécurisés que celui fourni par le service. Il incombe à la personne concernée demandant les données de définir les bonnes mesures pour sécuriser les données à caractère personnel dans son propre système. Toutefois, la personne concernée doit être informée de ce risque afin de prendre les mesures nécessaires pour protéger les informations qu'elle a reçues. Comme exemple de bonne pratique, les responsables du traitement pourraient aussi recommander des formats, outils de chiffrement ou autres mesures de sécurité appropriés pour aider les personnes concernées à atteindre cet objectif.

* * *

Fait à Bruxelles, le 13 décembre 2016

Pour le groupe de travail,
La présidente
Isabelle FALQUE-PIERROTIN

Version révisée et adoptée le 5 avril 2017

Pour le groupe de travail
La présidente
Isabelle FALQUE-PIERROTIN

24

Lignes directrices concernant les délégués à la protection des données (DPD) (WP243)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

16/FR
WP 243 rev.01

Lignes directrices concernant les délégués à la protection des données (DPD)

Adoptées le 13 décembre 2016

Version révisée et adoptée le 5 avril 2017

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et état de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO59 03/068.

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

Table des matières

1 Introduction

Le règlement général sur la protection des données (RGPD)[1], qui devrait prendre effet le 25 mai 2018, fournit un cadre de conformité modernisé, fondé sur la responsabilité, en matière de protection des données en Europe. Les délégués à la protection des données (DPD) seront au cœur de ce nouveau cadre juridique pour de nombreux organismes, pour faciliter la conformité avec les dispositions du RGPD.

En vertu du RGPD, certains responsables du traitement et sous-traitants ont l'obligation de désigner un DPD[2]. Cette obligation s'appliquera à l'ensemble des autorités et organismes publics (indépendamment de la nature des données qu'ils traitent), ainsi qu'à d'autres organismes dont les activités de base consistent en un suivi systématique à grande échelle de personnes ou en un traitement à grande échelle de catégories particulières de données à caractère personnel.

Même lorsque le RGPD n'exige pas spécifiquement la désignation d'un DPD, les organismes peuvent parfois juger utile d'en désigner un sur une base volontaire. Le groupe de travail «Article 29» sur la protection des données («G29») encourage ces efforts déployés sur une base volontaire.

La notion de DPD n'est pas nouvelle. Bien que la directive 95/46/CE[3] ne contraigne aucun organisme à désigner un DPD, la pratique consistant à désigner un DPD s'est néanmoins installée dans plusieurs États membres au fil des ans.

Avant l'adoption du RGPD, le G29 avait fait valoir que le DPD était l'une des pierres angulaires du régime de responsabilité et que la désignation d'un DPD pouvait faciliter le respect des règles et, en outre, devenir un avantage concurrentiel pour les entreprises[4]. Outre qu'ils favorisent le respect des règles grâce à la mise en œuvre d'outils de responsabilité (comme la facilitation d'analyses d'impact relatives à la protection des données et la facilitation ou la réalisation d'audits relatifs à la protection des données), les DPD agissent comme intermédiaires entre les acteurs concernés (par exemple, les autorités de contrôle, les personnes concernées et les entités économiques au sein d'un organisme).

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016,). Le règlement général présente de l'intérêt pour l'EEE et s'y appliquera après son intégration dans l'accord sur l'EEE.

[2] La désignation d'un DPD est également obligatoire pour les autorités compétentes en vertu de l'article 32 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89), ainsi que de la législation de transposition nationale. Bien que les présentes lignes directrices portent essentiellement sur les DPD désignés en vertu du RGPD, elles sont également pertinentes pour les DPD désignés en vertu de la directive 2016/680, en ce qui concerne les dispositions similaires des deux actes.

[3] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

[4] Voir http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_fr.pdf

Les DPD ne sont pas personnellement responsables en cas de non-respect du RGPD. Ce dernier établit clairement que c'est le responsable du traitement ou le sous-traitant qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément à ses dispositions (article 24, paragraphe 1). Le respect de la protection des données relève de la responsabilité du responsable du traitement ou du sous-traitant.

Le responsable du traitement ou le sous-traitant jouent également un rôle essentiel pour permettre l'exécution efficace des missions du DPD. La désignation d'un DPD est une première étape, mais celui-ci doit aussi disposer d'une autonomie et de ressources suffisantes pour s'acquitter efficacement de ses missions.

Le RGPD reconnaît le DPD en tant qu'acteur clé dans le nouveau système de gouvernance des données et établit les conditions relatives à sa désignation, à sa fonction et à ses missions. L'objectif des présentes lignes directrices est de préciser les dispositions pertinentes du RGPD afin d'aider les responsables du traitement et les sous-traitants à respecter la législation, mais aussi d'assister les DPD dans leur rôle. Les présentes lignes directrices formulent également des recommandations en matière de bonnes pratiques, en s'appuyant sur l'expérience acquise dans certains États membres de l'Union. Le G29 assurera le suivi de la mise en œuvre des présentes lignes directrices et pourrait les compléter avec des précisions supplémentaires si nécessaire.

2 Désignation d'un DPD

2.1. Désignation obligatoire

L'article 37, paragraphe 1, du RGPD requiert la désignation d'un DPD dans trois cas spécifiques[5]:

a) lorsque le traitement est effectué par une autorité publique ou un organisme public[6];
b) lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou
c) lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données[7] ou[8] de données à caractère personnel relatives à des condamnations pénales et à des infractions[9].

Dans les points ci-après, le G29 donne des orientations en ce qui concerne les critères et la terminologie figurant à l'article 37, paragraphe 1.

[5] Il est à noter que, conformément à l'article 37, paragraphe 4, le droit de l'Union ou des États membres peut exiger la désignation de DPD dans d'autres situations également.
[6] À l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle. Voir article 32 de la directive (UE) 2016/680.
[7] Conformément à l'article 9, ces catégories incluent les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale; est également visé le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
[8] L'article 37, paragraphe 1, point c), utilise le terme «*et*». Voir le point 2.1.5 ci-dessous pour des explications concernant l'utilisation du terme «*ou*» au lieu du terme «*et*».
[9] Article 10.

À moins qu'il soit évident qu'un organisme n'est pas tenu de désigner un DPD, le G29 recommande que les responsables du traitement et les sous-traitants documentent l'analyse interne effectuée afin de déterminer si, oui ou non, il y a lieu de désigner un DPD, afin qu'ils soient en mesure de démontrer que les facteurs pertinents ont été correctement pris en considération[10]. Cette analyse fait partie de la documentation requise au titre du principe de responsabilité. Elle peut être exigée par l'autorité de contrôle et doit être tenue à jour le cas échéant, par exemple si les responsables du traitement ou les sous-traitants exercent de nouvelles activités ou s'ils proposent de nouveaux services susceptibles de correspondre aux cas énumérés à l'article 37, paragraphe 1.

Lorsqu'un organisme désigne un DPD sur une base volontaire, les conditions prévues aux articles 37 à 39 s'appliquent à la désignation, à la fonction et aux missions de celui-ci comme si la désignation avait été obligatoire.

Rien n'empêche un organisme qui n'est pas tenu légalement de désigner un DPD et ne souhaite pas en désigner sur une base volontaire d'employer du personnel ou des consultants extérieurs chargés de missions liées à la protection des données à caractère personnel. En pareil cas, il importe de veiller à ce qu'il n'y ait pas de confusion quant à leur titre, leur statut, leur fonction et leurs missions. Ainsi, il convient d'indiquer clairement, dans toute communication au sein de l'entreprise ainsi qu'avec les autorités chargées de la protection des données, les personnes concernées et le public au sens large, que cette personne ou ce consultant ne porte pas le titre de délégué à la protection des données (DPD). [11]

Le DPD, que sa désignation soit obligatoire ou volontaire, est désigné pour toutes les opérations de traitement effectuées par le responsable du traitement ou le sous-traitant.

2.1.1 «UNE AUTORITE PUBLIQUE OU UN ORGANISME PUBLIC»

Le RGPD ne définit pas ce qu'il convient d'entendre par «*une autorité publique ou un organisme public*». Le G29 considère que cette notion doit être définie en fonction du droit national. En conséquence, les autorités publiques et les organismes publics incluent les autorités nationales, régionales et locales, mais, au regard des législations nationales applicables, cette notion englobe aussi généralement une série d'autres organismes de droit public[12]. En pareils cas, la désignation d'un DPD est obligatoire.

Les autorités publiques et les organismes publics ne sont pas les seuls à pouvoir effectuer des missions de service public ou exercer l'autorité publique[13]; d'autres personnes physiques ou morales de droit public ou privé peuvent également le faire, dans des domaines variant en fonction de la réglementation nationale de chaque État membre, tels que les services de transports publics, l'approvisionnement en eau et en énergie, les infrastructures routières, la radiodiffusion publique, le logement social ou les organes disciplinaires pour les professions réglementées.

Dans ces cas, les personnes concernées peuvent se trouver dans une situation très similaire à celle dans laquelle leurs données sont traitées par une autorité publique ou un organisme public. En particulier,

[10] Voir l'article 24, paragraphe 1.

[11] Cela vaut également pour les responsables de la protection de la vie privée (*chief privacy officers*) ou les autres professionnels chargés des questions de confidentialité qui sont déjà employés dans certaines entreprises et qui, s'ils ne respectent pas les critères établis par le RGPD, notamment pour ce qui est des ressources disponibles ou des garanties d'indépendance, ne peuvent être considérés ni désignés comme DPD.

les données peuvent être traitées à des fins similaires, et les particuliers n'ont souvent guère ou pas le choix quant au traitement même des données les concernant ou aux modalités de ce traitement et peuvent donc requérir la protection supplémentaire que peut apporter la désignation d'un DPD.

Bien qu'il n'y ait pas d'obligation dans ce cas, le G29 recommande, à titre de bonne pratique, que les organismes privés chargés d'effectuer des missions de service public ou exerçant l'autorité publique désignent un DPD. Les activités de ce DPD couvrent l'ensemble des opérations de traitement effectuées, y compris celles qui ne sont pas liées à la réalisation d'une mission de service public ou à l'exercice d'une charge officielle (par exemple, la gestion d'une base de données des employés).

2.1.2 «ACTIVITES DE BASE»

L'article 37, paragraphe 1, points b) et c), du RGPD fait référence aux «*activités de base du responsable du traitement ou du sous-traitant*». Le considérant 97 précise que «*les activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire*». Les «activités de base» peuvent être considérées comme les opérations essentielles nécessaires pour atteindre les objectifs du responsable du traitement ou du sous-traitant.

Toutefois, les «activités de base» ne doivent pas être interprétées comme excluant les activités pour lesquelles le traitement de données fait partie intégrante de l'activité du responsable du traitement ou du sous-traitant. Par exemple, l'activité de base d'un hôpital est de fournir des soins de santé. Toutefois, un hôpital ne peut fournir de soins de santé de manière sûre et efficace sans traiter des données concernant la santé, telles que les dossiers médicaux des patients. Par conséquent, le traitement de ces données doit être considéré comme l'une des activités de base de tout hôpital, et les hôpitaux doivent donc désigner un DPD.

On peut aussi citer l'exemple d'une société de sécurité privée qui assure la surveillance d'un certain nombre de centres commerciaux privés et d'espaces publics. L'activité de base de la société est la surveillance, qui est elle-même indissociablement liée au traitement de données à caractère personnel. Par conséquent, cette société doit également désigner un DPD.

En revanche, tous les organismes exercent certaines activités comme la rémunération de leurs employés ou les activités d'assistance informatique classiques. Ces activités constituent des exemples de fonctions de soutien nécessaires à l'activité de base ou principale de l'organisme. Bien que ces activités soient nécessaires ou essentielles, elles sont généralement considérées comme des fonctions auxiliaires plutôt que comme l'activité de base.

2.1.3 «À GRANDE ECHELLE»

L'article 37, paragraphe 1, points b) et c), exige que le traitement des données à caractère personnel soit effectué à grande échelle pour que la désignation d'un DPD soit obligatoire. Si le RGPD ne définit

[12] Voir, par exemple, les définitions de l'«*organisme du secteur public*» et de l'«*organisme de droit public*» énoncées respectivement à l'article 2, point 1), et à l'article 2, point 2), de la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public (JO L 345 du 31.12.2003, p. 90).
[13] Article 6, paragraphe 1, point e).

pas la notion de traitement à «grande échelle», le considérant 91 fournit toutefois certaines orientations[14].

En effet, il n'est pas possible de donner un chiffre précis, que ce soit pour la quantité de données traitées ou le nombre d'individus concernés, qui soit applicable dans toutes les situations. Cela n'exclut toutefois pas la possibilité qu'au fil du temps, une pratique courante puisse émerger, permettant de déterminer en des termes plus spécifiques ou quantitatifs ce qui constitue un traitement «*à grande échelle*» pour certains types d'activités de traitement courantes. Le G29 prévoit également de contribuer à cette évolution, en partageant et faisant connaître des exemples de seuils pertinents pour la désignation d'un DPD.

En tout état de cause, le G29 recommande que les facteurs suivants, en particulier, soient pris en considération pour déterminer si le traitement est mis en œuvre à grande échelle:

- le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée;
- le volume de données et/ou le spectre des données traitées;
- la durée, ou la permanence, des activités de traitement des données;
- l'étendue géographique de l'activité de traitement.

[14] Selon ce considérant, les «*opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées et qui sont susceptibles d'engendrer un risque élevé*» devraient être incluses en particulier. Par ailleurs, le considérant indique spécifiquement que le «*traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel*». Il importe de souligner que, si le considérant donne des exemples extrêmes dans un sens comme dans l'autre (le traitement par un médecin exerçant à titre individuel par rapport au traitement des données d'un pays entier ou dans l'ensemble de l'Europe), il existe une large zone grise entre ces deux extrêmes. En outre, il convient de garder à l'esprit que ce considérant concerne les analyses d'impact relatives à la protection des données, ce qui signifie que certains éléments pourraient être spécifiques à ce contexte et ne pas nécessairement s'appliquer exactement de la même manière à la désignation de DPD.

Exemples de traitement à grande échelle:

- traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités;
- traitement des données de voyage des passagers utilisant un moyen de transport public urbain (par exemple, suivi par les titres de transport);
- traitement des données de géolocalisation en temps réel des clients d'une chaîne internationale de restauration rapide à des fins statistiques par un sous-traitant spécialisé dans la fourniture de ces services;
- traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités;
- traitement des données à caractère personnel par un moteur de recherche à des fins de publicité comportementale;
- traitement des données (contenu, trafic, localisation) par des fournisseurs de services de téléphonie ou internet.

Exemples ne constituant pas un traitement à grande échelle:

- traitement, par un médecin exerçant à titre individuel, des données de ses patients;
- traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

2.1.4 «SUIVI REGULIER ET SYSTEMATIQUE»

La notion de suivi régulier et systématique des personnes concernées n'est pas définie dans le RGPD, mais celle de «*suivi du comportement des personnes concernées*» est mentionnée au considérant 24[15] et inclut clairement toutes les formes de suivi et de profilage sur l'internet, y compris à des fins de publicité comportementale.

Toutefois, la notion de suivi n'est pas limitée à l'environnement en ligne et le suivi en ligne ne doit être considéré que comme un exemple de suivi du comportement des personnes concernées[16].

Le G29 interprète le terme «régulier» comme recouvrant une ou plusieurs des significations suivantes:

- continu ou se produisant à intervalles réguliers au cours d'une période donnée;
- récurrent ou se répétant à des moments fixes;
- ayant lieu de manière constante ou périodique.

Le G29 interprète le terme «systématique» comme recouvrant une ou plusieurs des significations suivantes:

[15] *«Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.»*

[16] Il est à noter que le considérant 24 porte en particulier sur l'application extraterritoriale du RGPD. En outre, il existe également une différence entre l'expression «*le suivi du comportement de ces personnes*» [article 3, paragraphe 2, point b)], et l'expression «*un suivi régulier et systématique [...] des personnes concernées*» [article 37, paragraphe 1, point b)], qui pourrait donc être considéré comme une notion différente.

- se produisant conformément à un système;
- préétabli, organisé ou méthodique;
- ayant lieu dans le cadre d'un programme général de collecte de données;
- effectué dans le cadre d'une stratégie.

Exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées: exploitation d'un réseau de télécommunications; fourniture de services de télécommunications; reciblage par courrier électronique; activités de marketing fondées sur les données; profilage et notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent); géolocalisation, par exemple, par des applications mobiles; programmes de fidélité; publicité comportementale; surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables; systèmes de télévision en circuit fermé; dispositifs connectés tels que les voitures et compteurs intelligents, la domotique, etc.

2.1.5 CATEGORIES PARTICULIERES DE DONNEES ET DONNEES RELATIVES A DES CONDAMNATIONS PENALES ET A DES INFRACTIONS

L'article 37, paragraphe 1, point c), concerne le traitement de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. Bien que cette disposition utilise le terme «et», il n'existe aucune raison de principe qui voudrait que les deux critères doivent être appliqués simultanément. Il convient donc de lire le texte comme voulant dire «ou».

2.2. DPD du sous-traitant

L'article 37 s'applique à la fois aux responsables du traitement[17] et aux sous-traitants[18] en ce qui concerne la désignation d'un DPD. En fonction de la personne qui remplit les critères de désignation obligatoire, dans certains cas, seul le responsable du traitement ou le sous-traitant est tenu de désigner un DPD, dans d'autres, le responsable de traitement et le sous-traitant sont tenus de désigner chacun un DPD (les deux DPD devant alors collaborer entre eux).

Il est important de souligner que, même si le responsable du traitement remplit les critères de désignation obligatoire, son sous-traitant n'est pas nécessairement tenu de désigner un DPD. Il peut toutefois s'agir d'une bonne pratique.

Exemples:

- Une petite entreprise familiale active dans le secteur de la distribution d'appareils électroménagers dans une seule ville recourt aux services d'un sous-traitant dont l'activité de base consiste à fournir des services d'analyse de sites internet et d'assistance à la publicité et

[17] Le responsable du traitement est défini à l'article 4, point 7), comme la personne ou l'organisme qui détermine les finalités et les moyens du traitement.

[18] Le sous-traitant est défini à l'article 4, point 8), comme la personne ou l'organisme qui traite des données pour le compte du responsable du traitement.

au marketing ciblés. Les activités de l'entreprise familiale et ses clients n'entraînent pas de traitement de données à «grande échelle», compte tenu du faible nombre de clients et des activités relativement limitées. Toutefois, prises globalement, les activités du sous-traitant, qui dispose d'un grand nombre de clients comme cette petite entreprise, consistent en un traitement à grande échelle. Le sous-traitant doit donc désigner un DPD en vertu de l'article 37, paragraphe 1, point b), tandis que l'entreprise familiale elle-même n'est pas soumise à l'obligation de désigner un DPD.

- Une entreprise de taille moyenne spécialisée dans la fabrication de carrelage sous-traite ses services de médecine du travail à un sous-traitant externe, qui dispose d'un grand nombre de clients similaires. Le sous-traitant doit désigner un DPD en vertu de l'article 37, paragraphe 1, point c), dans la mesure où le traitement s'effectue à grande échelle. En revanche, le fabricant n'est pas nécessairement tenu de désigner un DPD.

Le DPD désigné par un sous-traitant supervise également les activités menées par l'organisme sous-traitant lorsque celui-ci agit lui-même en qualité de responsable du traitement (par exemple, ressources humaines, informatique, logistique).

2.3. Désignation d'un DPD unique pour plusieurs organismes

L'article 37, paragraphe 2, autorise un groupe d'entreprises à désigner un seul DPD à condition qu'il soit «*facilement joignable à partir de chaque lieu d'établissement*». La notion de joignabilité renvoie aux missions du DPD en tant que point de contact pour les personnes concernées[19], pour l'autorité de contrôle[20], mais également en interne au sein de l'organisme, compte tenu du fait que l'une des missions du DPD consiste à «*informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement*»[21].

Afin de veiller à ce que le DPD, qu'il soit interne ou externe, soit joignable, il est important de s'assurer que ses coordonnées sont mises à disposition conformément aux exigences du RGPD[22].

Il doit être en mesure, avec l'aide d'une équipe si nécessaire, de communiquer efficacement avec les personnes concernées[23] et de coopérer[24] avec les autorités de contrôle compétentes, ce qui implique

[19] Article 38, paragraphe 4: «*Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement*».

[20] Article 39, paragraphe 1, point e): «*faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet*».

[21] Article 39, paragraphe 1, point a).

[22] Voir à cet égard le point 2.6 ci-dessous.

[23] Article 12, paragraphe 1: *«Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant».*

[24] Article 39, paragraphe 1, point d): *«coopérer avec l'autorité de contrôle».*

également que cette communication s'effectue dans la ou les langues utilisées par les autorités de contrôle et les personnes concernées en question. La disponibilité d'un DPD (qu'il se trouve physiquement dans le même lieu que les employés ou qu'il soit joignable à travers un service d'assistance téléphonique ou d'autres moyens de communication sécurisés) est essentielle pour que les personnes concernées puissent prendre contact avec lui.

En vertu de l'article 37, paragraphe 3, un seul délégué à la protection des données peut être désigné pour plusieurs autorités publiques ou organismes publics, compte tenu de leur structure organisationnelle et de leur taille. Les mêmes considérations en matière de ressources et de communication s'appliquent. Étant donné que le DPD est chargé d'une série de missions, le responsable du traitement ou le sous-traitant doit s'assurer qu'un seul DPD peut, avec l'aide d'une équipe si nécessaire, s'acquitter efficacement de ces missions en dépit du fait qu'il soit désigné par plusieurs autorités publiques et organismes publics.

2.4. Joignabilité et localisation du DPD

Conformément à la section 4 du RGPD, la joignabilité du DPD doit être effective.

Afin de garantir que le DPD soit joignable, le G29 recommande que celui-ci se trouve dans l'Union européenne, que le responsable du traitement ou le sous-traitant soit ou non établi dans l'Union.

Toutefois, il ne peut être exclu que, dans certaines situations où le responsable du traitement ou le sous-traitant ne possède pas d'établissement dans l'Union européenne[25], le DPD puisse mener ses activités de manière plus efficace s'il se trouve en dehors de l'Union.

2.5. Expertise et compétences du DPD

L'article 37, paragraphe 5, dispose que le DPD «*est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39*». Le considérant 97 indique que le niveau de connaissances spécialisées requis devrait être déterminé en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées.

- **Niveau d'expertise**

Le niveau d'expertise requis n'est pas strictement défini, mais il doit être proportionné à la sensibilité, à la complexité et au volume des données traitées par un organisme. Par exemple, lorsqu'une opération de traitement de données est particulièrement complexe, ou lorsqu'une grande quantité de données sensibles est concernée, il est possible que le DPD doive disposer d'un niveau plus élevé d'expertise et de soutien. Il existe également une différence selon que l'organisme transfère systématiquement des données à caractère personnel hors de l'Union européenne ou, au contraire, que les transferts de ce

[25] Voir l'article 3 du RGPD concernant le champ d'application territorial.

type sont occasionnels. Il convient donc de choisir le DPD soigneusement, en prenant dûment en considération les questions relatives à la protection des données qui se posent au sein de l'organisme.

- **Qualités professionnelles**

Bien que l'article 37, paragraphe 5, ne précise pas les qualités professionnelles à prendre en considération lors de la désignation du DPD, il est nécessaire que les DPD disposent d'une expertise dans le domaine des législations et pratiques nationales et européennes en matière de protection des données, ainsi que d'une connaissance approfondie du RGPD. Il est également utile que les autorités de contrôle encouragent la formation adéquate et régulière des DPD.

La connaissance du secteur d'activité et de l'organisme du responsable du traitement est utile. Le DPD devrait également disposer d'une bonne compréhension des opérations de traitement effectuées, ainsi que des systèmes d'information et des besoins du responsable du traitement en matière de protection et de sécurité des données.

Dans le cas d'une autorité publique ou d'un organisme public, le DPD devrait également avoir une bonne connaissance des règles et procédures administratives de l'organisme.

- **Aptitude à exercer ses missions**

L'aptitude à exercer les missions qui incombent au DPD doit être interprétée tant au regard des qualités personnelles et connaissances du DPD que de sa fonction au sein de l'organisme. Parmi les qualités personnelles figurent par exemple l'intégrité et un haut niveau de déontologie; la préoccupation première du DPD doit être de permettre le respect du RGPD. Le DPD joue un rôle clé dans la promotion d'une culture de la protection des données au sein de l'organisme et contribue à mettre en œuvre des éléments essentiels du RGPD, tels que les principes relatifs au traitement des données[26], les droits des personnes concernées[27], la protection des données dès la conception et la protection des données par défaut[28], le registre des activités de traitement[29], la sécurité du traitement[30] ainsi que la notification et la communication des violations de données[31].

- **DPD sur la base d'un contrat de service**

La fonction du DPD peut aussi être exercée sur la base d'un contrat de service conclu avec une personne ou un organisme indépendant de l'organisme du responsable du traitement ou du sous-traitant. Dans ce cas, il est essentiel que chaque membre de l'organisme exerçant les fonctions de DPD remplisse l'ensemble des exigences applicables établies à la section 4 du RGPD (par exemple, il est essentiel qu'aucun des membres de l'organisme n'ait de conflit d'intérêts). Il est tout aussi important que chaque membre soit protégé par les dispositions du RGPD (par exemple, pas de résiliation abusive du contrat de service pour les activités de DPD pas plus que de licenciement abusif d'un membre de l'organisme exerçant les missions du DPD). Dans le même temps, les compétences et les atouts

[26] Chapitre II.
[27] Chapitre III.
[28] Article 25.
[29] Article 30.
[30] Article 32.
[31] Articles 33 et 34.

individuels peuvent être combinés de sorte que plusieurs personnes, travaillant en équipe, puissent mieux servir leurs clients.

Dans un souci de clarté juridique et de bonne organisation, et afin d'éviter les conflits d'intérêts pour les membres de l'équipe, il est recommandé de prévoir une répartition claire des tâches au sein de l'équipe chargée de la fonction de DPD et de désigner, pour chaque client, une seule personne comme personne de contact principale «responsable» de ce client. En règle générale, il serait également utile de préciser ces points dans le contrat de service.

2.6. Publication et communication des coordonnées du DPD

L'article 37, paragraphe 7, du RGPD dispose que le responsable du traitement ou le sous-traitant:

- publie les coordonnées du DPD et
- communique ces coordonnées à l'autorité de contrôle compétente.

Ces exigences visent à garantir que les personnes concernées (tant à l'intérieur qu'à l'extérieur de l'organisme) et les autorités de contrôle puissent aisément et directement prendre contact avec le DPD sans devoir s'adresser à un autre service de l'organisme. La confidentialité est également un aspect important: les employés pourraient par exemple hésiter à se plaindre auprès du DPD si la confidentialité de leurs communications n'est pas garantie
Le DPD est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres (article 38, paragraphe 5).

Les coordonnées du DPD doivent contenir des informations permettant aux personnes concernées et aux autorités de contrôle de joindre celui-ci facilement (une adresse postale, un numéro de téléphone spécifique et/ou une adresse de courrier électronique spécifique). Le cas échéant, aux fins de la communication avec le public, d'autres moyens de communication pourraient également être prévus, par exemple, une assistance par téléphone spécifique, ou un formulaire de contact spécifique adressé au DPD sur le site web de l'organisme.

L'article 37, paragraphe 7, n'exige pas que les coordonnées publiées incluent le nom du DPD. Si la publication du nom du DPD peut constituer une bonne pratique, il appartient au responsable du traitement, ou au sous-traitant, et au DPD de décider si elle est nécessaire ou utile dans les circonstances particulières du cas considéré[32].

Toutefois, la communication du nom du DPD à l'autorité de contrôle est essentielle pour que le DPD puisse faire office de point de contact entre l'organisme et l'autorité de contrôle [article 39, paragraphe 1, point e)].

À titre de bonne pratique, le G29 recommande également que tout organisme communique le nom et les coordonnées du DPD à ses employés. Par exemple, le nom et les coordonnées du DPD pourraient

[32] Il est à noter qu'à la différence de l'article 37, paragraphe 7, l'article 33, paragraphe 3, point b), qui décrit les informations à communiquer à l'autorité de contrôle et à la personne concernée en cas de violation de données à caractère personnel, exige explicitement la communication du nom du DPD (et pas uniquement de ses coordonnées).

être publiés en interne sur l'intranet, dans le répertoire téléphonique et dans les organigrammes de l'organisme.

3 Fonction du DPD

3.1. Association du DPD à toutes les questions relatives à la protection des données à caractère personnel

L'article 38 du RGPD dispose que le responsable du traitement et le sous-traitant doivent veiller à ce que le DPD «*soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel*».

Il est essentiel que le DPD, ou son équipe, soit associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données. En ce qui concerne les analyses d'impact relatives à la protection des données, le RGPD prévoit expressément la participation du DPD à un stade précoce et précise que le responsable du traitement doit demander conseil au DPD lorsqu'il effectue une analyse de ce type[33]. L'information et la consultation du DPD dès le début permettront de faciliter le respect du RGPD et d'encourager une approche fondée sur la protection des données dès la conception; il devrait donc s'agir d'une procédure habituelle au sein de la gouvernance de l'organisme. En outre, il importe que le DPD soit considéré comme un interlocuteur au sein de l'organisme et qu'il soit membre des groupes de travail consacrés aux activités de traitement de données au sein de l'organisme.

Par conséquent, l'organisme devrait veiller, par exemple, à ce que:

- le DPD soit invité à participer régulièrement aux réunions de l'encadrement supérieur et intermédiaire;
- sa présence soit recommandée lorsque des décisions ayant des implications en matière de protection des données sont prises. Toutes les informations pertinentes doivent être transmises au DPD en temps utile afin de lui permettre de fournir un avis adéquat;
- l'avis du DPD soit toujours dûment pris en considération. En cas de désaccord, le G29 recommande, à titre de bonne pratique, de consigner les raisons pour lesquelles l'avis du DPD n'a pas été suivi;
- le DPD soit immédiatement consulté lorsqu'une violation de données ou un autre incident se produit.

Le cas échéant, le responsable du traitement ou le sous-traitant pourrait élaborer des lignes directrices ou des programmes en matière de protection des données indiquant les cas dans lesquels le DPD doit être consulté.

[33] Article 35, paragraphe 2.

3.2. Ressources nécessaires

L'article 38, paragraphe 2, du RGPD exige que l'organisme aide son DPD *en fournissant les ressources nécessaires pour exercer [ses] missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées*. Les aspects suivants, en particulier, doivent être pris en considération:

- soutien actif de la fonction du DPD par l'encadrement supérieur (par exemple, au niveau du conseil d'administration);
- temps suffisant pour que les DPD puissent accomplir leurs tâches. Cet aspect est particulièrement important lorsqu'un DPD interne est désigné à temps partiel ou lorsque le DPD externe est chargé de la protection des données en plus d'autres tâches. Autrement, des conflits de priorités pourraient conduire à ce que les tâches du DPD soient négligées. Il est primordial que le DPD puisse consacrer suffisamment de temps à ses missions. Il est de bonne pratique de fixer un pourcentage de temps consacré à la fonction de DPD lorsque cette fonction n'est pas occupée à temps plein. Il est également de bonne pratique de déterminer le temps nécessaire à l'exécution de la fonction et le niveau de priorité approprié pour les tâches du DPD, et que le DPD (ou l'organisme) établisse un plan de travail;
- soutien adéquat du point de vue des ressources financières, des infrastructures (locaux, installations, équipements) et du personnel, le cas échéant;
- communication officielle de la désignation du DPD à l'ensemble du personnel afin de veiller à ce que l'existence et la fonction de celui-ci soient connues au sein de l'organisme;
- accès nécessaire à d'autres services, tels que les ressources humaines, le service juridique, l'informatique, la sécurité, etc., de manière à ce que les DPD puissent recevoir le soutien, les contributions et les informations essentiels de ces autres services;
- formation continue. Les DPD doivent avoir la possibilité de maintenir leurs connaissances à jour en ce qui concerne les évolutions dans le domaine de la protection des données. L'objectif devrait être d'augmenter constamment le niveau d'expertise des DPD et ceux-ci devraient être encouragés à participer à des cours de formation sur la protection des données ainsi qu'à d'autres formes de développement professionnel, telles que la participation à des forums sur la protection de la vie privée, des ateliers, etc.;
- compte tenu de la taille et de la structure de l'organisme, il est possible qu'il faille mettre en place une équipe de DPD (un DPD et son personnel). En pareils cas, la structure interne de l'équipe ainsi que les tâches et responsabilités de chacun de ses membres doivent être clairement établies. De même, lorsque la fonction du DPD est exercée par un prestataire de services externe, une équipe de personnes travaillant pour le compte de cette entité peut exercer, dans les faits, les missions du DPD en tant que groupe, sous la responsabilité d'une personne de contact principale désignée pour le client.

D'une manière générale, plus les opérations de traitement sont complexes ou sensibles, plus les ressources octroyées au DPD devront être importantes. La fonction de protection des données doit être effective et dotée de ressources adéquates au regard du traitement de données réalisé.

3.3. Instructions et exercice de «leurs fonctions et missions en toute indépendance»

L'article 38, paragraphe 3, prévoit certaines garanties de base destinées à faire en sorte que les DPD soient en mesure d'exercer leurs missions avec un degré suffisant d'autonomie au sein de leur

organisme. En particulier, les responsables du traitement/sous-traitants doivent veiller à ce que le DPD «*ne reçoive aucune instruction en ce qui concerne l'exercice des missions*». Le considérant 97 indique en outre que les DPD, «*qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance*».

Cela signifie que, dans l'exercice de leurs missions au titre de l'article 39, les DPD ne doivent pas recevoir d'instructions sur la façon de traiter une affaire, par exemple, quel résultat devrait être obtenu, comment enquêter sur une plainte ou s'il y a lieu de consulter l'autorité de contrôle. En outre, ils ne peuvent être tenus d'adopter un certain point de vue sur une question liée à la législation en matière de protection des données, par exemple, une interprétation particulière du droit.

L'autonomie des DPD ne signifie cependant pas qu'ils disposent de pouvoirs de décision allant au-delà des missions leur incombant conformément à l'article 39.

Le responsable du traitement ou le sous-traitant reste responsable du respect de la législation sur la protection des données et doit être en mesure de démontrer ce respect[34]. Si le responsable du traitement ou le sous-traitant prend des décisions qui sont incompatibles avec le RGPD et l'avis du DPD, ce dernier devrait avoir la possibilité d'indiquer clairement son avis divergent au niveau le plus élevé de la direction et aux décideurs. À cet égard, l'article 38, paragraphe 3, dispose que le DPD «*fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant*». Une telle reddition de compte directe garantit que l'encadrement supérieur (par ex., le conseil d'administration) a connaissance des avis et recommandations du DPD qui s'inscrivent dans le cadre de la mission de ce dernier consistant à informer et à conseiller le responsable du traitement ou le sous-traitant. L'élaboration d'un rapport annuel sur les activités du DPD destiné au niveau le plus élevé de la direction constitue un autre exemple de reddition de compte directe.

3.4. Licenciement ou sanction pour l'exercice des missions du DPD

L'article 38, paragraphe 3, dispose que le DPD ne devrait pas être «*relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions*».

Cette exigence renforce l'autonomie des DPD et contribue à garantir que ceux-ci agissent en toute indépendance et bénéficient d'une protection suffisante dans l'exercice de leurs missions relatives à la protection des données.

Le RGPD n'interdit les sanctions que si elles sont imposées au DPD à la suite de l'exercice de ses missions de DPD. Par exemple, si un DPD considère qu'un traitement particulier est susceptible d'engendrer un risque élevé et conseille au responsable du traitement ou au sous-traitant de procéder à une analyse d'impact relative à la protection des données, mais que le responsable du traitement ou le sous-traitant n'est pas d'accord avec l'évaluation du DPD, ce dernier ne peut être relevé de ses fonctions pour avoir formulé cet avis.

Les sanctions peuvent prendre des formes diverses et peuvent être directes ou indirectes. Il peut s'agir, par exemple, d'absence de promotion ou de retard dans la promotion, de freins à l'avancement de carrière ou du refus de l'octroi d'avantages dont bénéficient d'autres travailleurs. Il n'est pas

[34] Article 5, paragraphe 2.

nécessaire que ces sanctions soient effectivement mises en œuvre, une simple menace suffit pour autant qu'elle soit utilisée pour sanctionner le DPD pour des motifs liés à ses activités de DPD.

Dans le cadre d'une gestion normale, et comme c'est le cas pour tout autre employé ou sous-traitant conformément au droit des contrats ou au droit du travail et au droit pénal applicables au niveau national, et selon les conditions qui y sont fixées, un DPD pourra toujours être licencié légitimement pour des motifs autres que l'exercice de ses missions de DPD (par exemple, en cas de vol, de harcèlement physique, moral ou sexuel ou d'autres fautes graves similaires).

Dans ce contexte, il convient de noter que le RGPD ne précise pas comment et quand un DPD peut être licencié ou remplacé par une autre personne. Toutefois, plus le contrat d'un DPD est stable et plus il existe de garanties contre le licenciement abusif, plus il est probable que le DPD pourra agir en toute indépendance. Par conséquent, le G29 encourage les efforts déployés par les organismes à cet effet.

3.5. Conflits d'intérêts

L'article 38, paragraphe 6, autorise les DPD à «*exécuter d'autres missions et tâches*». Il exige toutefois que l'organisme veille à ce que «*ces missions et tâches n'entraînent pas de conflit d'intérêts*».

L'absence de conflit d'intérêts est étroitement liée à l'obligation d'agir en toute indépendance. Bien que les DPD soient autorisés à exercer d'autres fonctions, un DPD ne peut se voir confier d'autres missions et tâches qu'à condition que celles-ci ne donnent pas lieu à un conflit d'intérêts. Cela signifie en particulier que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. En raison de la structure organisationnelle spécifique de chaque organisme, cet aspect doit être étudié au cas par cas.

En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. En outre, il peut également y avoir conflit d'intérêts, par exemple, si un DPD externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.

En fonction des activités, de la taille et de la structure de l'organisme, il peut être de bonne pratique pour les responsables du traitement ou les sous-traitants:

- de recenser les fonctions qui seraient incompatibles avec celle de DPD;
- d'établir des règles internes à cet effet, afin d'éviter les conflits d'intérêts;
- d'inclure une explication plus générale concernant les conflits d'intérêts;
- de déclarer que leur DPD n'a pas de conflit d'intérêts en ce qui concerne sa fonction de DPD, dans le but de mieux faire connaître cette exigence;
- de prévoir des garanties dans le règlement intérieur de l'organisme, et de veiller à ce que l'avis de vacance pour la fonction de DPD ou le contrat de service soit suffisamment précis et

détaillé pour éviter tout conflit d'intérêts. Dans ce contexte, il convient également de garder à l'esprit que les conflits d'intérêts peuvent prendre différentes formes selon que le DPD est recruté en interne ou à l'extérieur.

4 Missions du DPD

4.1. Contrôle du respect du RGPD

L'article 39, paragraphe 1, point b), confie au DPD, entre autres missions, la tâche de contrôler le respect du RGPD. Le considérant 97 précise en outre que le DPD «*devrait aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement*».

Dans le cadre de ces tâches de contrôle du respect du RGPD, les DPD peuvent notamment:

- recueillir des informations permettant de recenser les activités de traitement;
- analyser et vérifier la conformité des activités de traitement;
- informer et conseiller le responsable du traitement ou le sous-traitant et formuler des recommandations à son intention.

Le contrôle du respect du RGPD ne signifie pas que le DPD est personnellement responsable en cas de non-respect de celui-ci. Le RGPD établit clairement que c'est le responsable du traitement, et non le DPD, qui est tenu de mettre «*en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement*» (article 24, paragraphe 1). Le respect de la protection des données relève de la responsabilité sociale du responsable du traitement des données, et non du DPD.

4.2. Rôle du DPD dans les analyses d'impact relatives à la protection des données

Conformément à l'article 35, paragraphe 1, il incombe au responsable du traitement, et non au DPD, d'effectuer, si nécessaire, une analyse d'impact relative à la protection des données. Toutefois, le DPD peut jouer un rôle d'assistance du responsable du traitement très important et très utile. Conformément au principe de protection des données dès la conception, l'article 35, paragraphe 2, exige expressément que le responsable du traitement «*demande conseil*» au DPD lorsqu'il réalise une analyse d'impact relative à la protection des données. L'article 39, paragraphe 1, point c), donne pour sa part mission au DPD de «*dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35*».

Le G29 recommande que le responsable du traitement demande conseil au DPD sur les questions suivantes notamment[35]:

- la question de savoir s'il convient ou non de procéder à une analyse d'impact relative à la protection des données;
- la méthodologie à suivre lors de la réalisation d'une analyse d'impact relative à la protection des données;

[35] L'article 39, paragraphe 1, énumère les missions du DPD et indique que ces missions sont «*au moins*» les suivantes. Par conséquent, rien ne s'oppose à ce que le responsable du traitement confie au DPD des missions autres que celles qui sont expressément mentionnées à l'article 39, paragraphe 1, ou précise ces missions de manière plus détaillée.

- la question de savoir s'il convient d'effectuer l'analyse d'impact relative à la protection des données en interne ou de la sous-traiter;
- les mesures (y compris des mesures techniques et organisationnelles) à appliquer pour atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées;
- la question de savoir si l'analyse d'impact relative à la protection des données a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes au RGPD.

Si le responsable du traitement est en désaccord avec l'avis fourni par le DPD, la documentation de l'analyse d'impact relative à la protection des données devrait expressément justifier, par écrit, la raison pour laquelle l'avis n'a pas été pris en considération[36]

Le G29 recommande en outre que le responsable du traitement décrive clairement, par exemple dans le contrat du DPD, mais aussi dans les informations fournies aux employés et à l'encadrement (ainsi qu'à d'autres parties prenantes, le cas échéant), les missions précises du DPD et leur champ d'application, notamment en ce qui concerne la réalisation des analyses d'impact relatives à la protection des données.

4.3. Coopérer avec l'autorité de contrôle et faire office de point de contact

Conformément à l'article 39, paragraphe 1, points d) et e), le DPD devrait: «*coopérer avec l'autorité de contrôle*» et «*faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet*».

Ces missions ont trait au rôle de «facilitateur» du DPD mentionné dans l'introduction des présentes lignes directrices. Le DPD fait office de point de contact pour faciliter l'accès de l'autorité de contrôle aux documents et informations nécessaires à l'exécution des missions mentionnées à l'article 57, ainsi qu'à l'exercice de ses pouvoirs d'enquête, de ses pouvoirs d'adopter des mesures correctrices, de ses pouvoirs d'autorisation et de ses pouvoirs consultatifs visés à l'article 58. Comme cela a déjà été mentionné, le DPD est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres (article 38, paragraphe 5). Toutefois, l'obligation de secret professionnel/confidentialité n'interdit pas au DPD de prendre contact avec l'autorité de contrôle pour solliciter son avis. L'article 39, paragraphe 1, point e), dispose que le DPD peut mener des consultations auprès de l'autorité de contrôle sur tout autre sujet, le cas échéant.

[36] L'article 24, paragraphe 1, dispose que, «*[c]ompte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer* ***et être en mesure de démontrer*** *que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire*».

4.4. Approche fondée sur les risques

L'article 39, paragraphe 2, requiert que le DPD tienne «*dûment compte [...] du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement*».

Cet article rappelle un principe général de bon sens, qui peut s'appliquer à de nombreux aspects du travail quotidien d'un DPD. En substance, il exige des DPD qu'ils établissent des priorités dans leurs activités et concentrent leurs efforts sur les questions qui représentent un risque élevé en matière de protection des données. Cela ne signifie pas qu'ils doivent négliger la vérification de la conformité des opérations de traitement présentant un niveau de risque inférieur, mais plutôt qu'ils doivent se concentrer, en premier lieu, sur les secteurs présentant un risque élevé.

Cette approche sélective et pragmatique devrait aider les DPD à conseiller le responsable du traitement sur la méthode à utiliser lors de la réalisation d'une analyse d'impact sur la protection des données, sur les domaines qui devraient être soumis à un audit interne ou externe en matière de protection des données, sur les activités de formation à proposer au personnel ou aux membres de l'encadrement responsables des activités de traitement des données et sur les opérations de traitement auxquelles il devrait consacrer une part plus importante de son temps et de ses ressources.

4.5. Rôle du DPD dans la tenue du registre

En vertu de l'article 30, paragraphes 1 et 2, c'est le responsable du traitement ou le sous-traitant, et non le DPD, qui doit tenir «*un registre des activités de traitement effectuées sous [sa] responsabilité*» ou «*un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement*».

Dans la pratique, les DPD dressent souvent des inventaires et tiennent un registre des opérations de traitement sur la base des informations qui leur ont été fournies par les différents services dans leur organisme responsables du traitement de données à caractère personnel. Cette pratique a été inscrite dans de nombreuses législations nationales ainsi que dans les règles en matière de protection des données applicables aux institutions et organes de l'Union européenne[37].

L'article 39, paragraphe 1, établit une liste des missions que le DPD doit au moins se voir confier. Par conséquent, rien ne s'oppose à ce que le responsable du traitement ou le sous-traitant confie au DPD la mission de tenir le registre des opérations de traitement effectuées sous la responsabilité du responsable du traitement ou du sous-traitant. Ce registre doit être considéré comme l'un des outils permettant au DPD d'exercer ses missions de contrôle du respect du RGPD ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant.

En tout état de cause, le registre qui doit être tenu au titre de l'article 30 doit aussi être considéré comme un outil permettant au responsable du traitement et à l'autorité de contrôle de disposer, sur demande, d'une vue d'ensemble de toutes les activités de traitement de données à caractère personnel effectuées par un organisme. Il s'agit donc d'une condition préalable nécessaire au respect du RGPD et, à ce titre, d'une mesure de responsabilisation efficace.

[37] Article 24, paragraphe 1, point d), du règlement (CE) nº 45/2001.

23

5 ANNEXE – LIGNES DIRECTRICES CONCERNANT LES DPD: CE QU'IL FAUT SAVOIR

L'objectif de la présente annexe est de répondre, dans un format simplifié et facile à lire, à certaines des principales questions que peuvent se poser les organismes au sujet des nouvelles exigences prévues par le règlement général sur la protection des données (RGPD) en matière de désignation d'un DPD.

Désignation du DPD

1 Quels sont les organismes tenus de désigner un DPD

La désignation d'un DPD est obligatoire:

- si le traitement est effectué par une autorité publique ou un organisme public, quelles que soient les données qui sont traitées;
- si les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes concernées;
- si les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

Il est à noter que le droit de l'Union ou des États membres peut exiger la désignation de DPD dans d'autres situations également. Enfin, même si la désignation d'un DPD n'est pas obligatoire, les organismes peuvent parfois estimer utile d'en désigner un sur une base volontaire. Le groupe de travail «Article 29» sur la protection des données («G29») encourage ces efforts déployés sur une base volontaire. Lorsqu'un organisme désigne un DPD sur une base volontaire, les mêmes conditions s'appliquent à la désignation, à la fonction et aux missions de celui-ci que si la désignation avait été obligatoire.

Sources: article 37, paragraphe 1, du RGPD

2 Qu'entend-on par «activités de base»?

Les «activités de base» peuvent être considérées comme les opérations essentielles pour atteindre les objectifs du responsable du traitement ou du sous-traitant. Elles comprennent également toutes les activités pour lesquelles le traitement de données fait partie intégrante de l'activité du responsable du traitement ou du sous-traitant. Par exemple, le traitement des données concernant la santé telles que les dossiers médicaux des patients doit être considéré comme l'une des activités de base des hôpitaux, et ces derniers doivent donc désigner un DPD.

En revanche, tous les organismes exercent certaines activités de soutien comme la rémunération de leurs employés ou les activités d'assistance informatique classiques. Ces activités constituent des exemples de fonctions de soutien nécessaires à l'activité de base ou principale de l'organisme. Bien que ces activités soient nécessaires ou essentielles, elles sont généralement considérées comme des fonctions auxiliaires plutôt que comme l'activité de base.

Sources: article 37, paragraphe 1, points b) et c), du RGPD

3 Qu'entend-on par «à grande échelle»?

Le RGPD ne définit pas la notion de traitement «à grande échelle». Le G29 recommande que les facteurs suivants, en particulier, soient pris en considération pour déterminer si le traitement est mis en œuvre à grande échelle:

- le nombre de personnes concernées, soit en valeur absolue, soit en valeur relative par rapport à la population concernée;
- le volume de données et/ou le spectre des données traitées;
- la durée, ou la permanence, des activités de traitement des données;
- l'étendue géographique de l'activité de traitement.

Exemples de traitement à grande échelle:

- traitement des données de patients par un hôpital dans le cadre du déroulement normal de ses activités;
- traitement des données de voyage des passagers utilisant un moyen de transport public urbain (par exemple, suivi par les titres de transport);
- traitement des données de géolocalisation en temps réel des clients d'une chaîne internationale de restauration rapide à des fins statistiques par un sous-traitant spécialisé dans ces activités;
- traitement des données de clients par une compagnie d'assurance ou une banque dans le cadre du déroulement normal de ses activités;
- traitement des données à caractère personnel par un moteur de recherche à des fins de publicité comportementale;
- traitement des données (contenu, trafic, localisation) par des fournisseurs de services de téléphonie ou internet.

Exemples ne constituant pas un traitement à grande échelle:

- traitement, par un médecin exerçant à titre individuel, des données de ses patients;
- traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions par un avocat exerçant à titre individuel.

Sources: article 37, paragraphe 1, points b) et c), du RGPD

4 Qu'entend-on par «suivi régulier et systématique»

La notion de suivi régulier et systématique des personnes concernées n'est pas définie dans le RGPD, mais inclut clairement toutes les formes de suivi et de profilage sur l'internet, y compris à des fins de publicité comportementale. La notion de suivi ne se limite toutefois pas à l'environnement en ligne.

Exemples d'activités pouvant constituer un suivi régulier et systématique des personnes concernées: exploitation d'un réseau de télécommunications; fourniture de services de télécommunications; reciblage par courrier électronique; activités de marketing fondées sur les données; profilage et notation à des fins d'évaluation des risques (par exemple, aux fins de l'évaluation du risque de crédit, de l'établissement des primes d'assurance, de la prévention de la fraude ou de la détection du blanchiment d'argent); géolocalisation, par exemple, par des applications mobiles; programmes de fidélité; publicité comportementale; surveillance des données sur le bien-être, la santé et la condition physique au moyen de dispositifs portables; systèmes de télévision en circuit fermé; dispositifs connectés tels que les voitures et compteurs intelligents, la domotique, etc.

Le G29 interprète le terme «régulier» comme recouvrant une ou plusieurs des significations suivantes:

- continu ou se produisant à intervalles réguliers au cours d'une période donnée;
- récurrent ou se répétant à des moments fixes;
- ayant lieu de manière constante ou périodique.

Le G29 interprète le terme «systématique» comme recouvrant une ou plusieurs des significations suivantes:

- se produisant conformément à un système;
- préétabli, organisé ou méthodique;
- ayant lieu dans le cadre d'un programme général de collecte de données;
- effectué dans le cadre d'une stratégie.

Sources: article 37, paragraphe 1, point b), du RGPD

5 Des organismes peuvent-ils désigner un DPD conjointement? Dans l'affirmative, à quelles conditions?

Oui. Un groupe d'entreprises peut désigner un seul DPD à condition qu'il soit «*facilement joignable à partir de chaque lieu d'établissement*». La notion de joignabilité renvoie aux missions du DPD en tant que point de contact pour les personnes concernées, pour l'autorité de contrôle et également en interne au sein de l'organisme. Afin de veiller à ce que le DPD, qu'il soit interne ou externe, soit joignable, il est important de s'assurer que ses coordonnées sont mises à disposition. Le DPD, avec l'aide d'une équipe si nécessaire, doit être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec les autorités de contrôle compétentes, ce qui implique que cette communication s'effectue dans la ou les langues utilisées par les autorités de contrôle et les personnes concernées en question. La disponibilité d'un DPD (qu'il se trouve physiquement dans le même lieu que les employés ou qu'il soit joignable à travers un service d'assistance téléphonique ou d'autres moyens de communication sécurisés) est essentielle pour que les personnes concernées puissent prendre contact avec lui.

Un seul délégué à la protection des données peut être désigné pour plusieurs autorités publiques ou organismes publics, compte tenu de leur structure organisationnelle et de leur taille. Les mêmes considérations en matière de ressources et de communication s'appliquent. Étant donné que le DPD est chargé d'une série de missions, le responsable du traitement ou le sous-traitant doit s'assurer qu'un seul DPD peut, avec l'aide d'une équipe si nécessaire, s'acquitter efficacement de ces missions en dépit du fait qu'il soit désigné par plusieurs autorités publiques et organismes publics.

Sources: article 37, paragraphes 2 et 3, du RGPD

6 Où le DPD doit-il se trouver?

Afin de garantir que le DPD soit joignable, le G29 recommande que celui-ci se trouve dans l'Union européenne, que le responsable du traitement ou le sous-traitant soit ou non établi dans l'Union. Toutefois, il ne peut être exclu que, dans certaines situations où le responsable du traitement ou le sous-traitant ne possède pas d'établissement dans l'Union européenne, le DPD puisse mener ses activités de manière plus efficace s'il se trouve en dehors de l'Union.

7 Est-il possible de désigner un DPD externe?

Oui. Le DPD peut être un membre du personnel du responsable du traitement ou du sous-traitant (DPD interne) ou exercer ses missions sur la base d'un contrat de service, ce qui signifie que le DPD peut être une personne externe et, dans ce cas, sa fonction peut être exercée sur la base d'un contrat de service conclu avec une personne ou un organisme.

Lorsque la fonction du DPD est exercée par un prestataire de services externe, une équipe de personnes travaillant pour le compte de cette entité peut, dans les faits, exercer les missions du DPD en tant que groupe, sous la responsabilité d'une personne de contact principale responsable du client. Dans ce cas, il est essentiel que chaque membre de l'organisme externe exerçant les fonctions de DPD remplisse l'ensemble des exigences applicables établies dans le RGPD.

Dans un souci de clarté juridique et de bonne organisation, et afin de prévenir les conflits d'intérêts pour les membres de l'équipe, les lignes directrices recommandent de prévoir, dans le contrat de service, une répartition claire des tâches au sein de l'équipe externe chargée de la fonction de DPD et de désigner une seule personne comme personne de contact principale «responsable» du client.

Sources: article 37, paragraphe 6, du RGPD

8 Quelles sont les qualités professionnelles que le DPD doit posséder?

Le DPD est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions.

Le niveau de connaissances spécialisées requis devrait être déterminé en fonction des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées. Par exemple, lorsqu'une opération de traitement de données est particulièrement complexe, ou lorsqu'une grande quantité de données sensibles est concernée, il est possible que le DPD doive disposer d'un niveau plus élevé d'expertise et de soutien.

Les compétences et l'expertise nécessaires sont notamment les suivantes:

- expertise relative aux législations nationale et européenne en matière de protection des données, y compris une connaissance approfondie du RGPD;
- compréhension des opérations de traitement effectuées;
- compréhension des technologies de l'information et de la sécurité des données;
- connaissance du secteur d'activité et de l'organisme;
- capacité à promouvoir une culture de protection des données au sein de l'organisme.

Sources: article 37, paragraphe 5, du RGPD

Fonction du DPD

9 Quelles ressources le responsable du traitement ou le sous-traitant doit-il mettre à la disposition du DPD?

Le DPD doit disposer des ressources nécessaires à l'exécution de ses missions.

En fonction de la nature des opérations et activités de traitement et de la taille de l'organisme, les ressources suivantes devraient être fournies au DPD:

- soutien actif de la fonction du DPD par l'encadrement supérieur;
- temps suffisant pour que les DPD puissent accomplir leurs missions;
- soutien adéquat du point de vue des ressources financières, des infrastructures (locaux, installations, équipements) et du personnel, le cas échéant;
- communication officielle de la désignation du DPD à l'ensemble du personnel;
- accès à d'autres services au sein de l'organisme de manière à ce que les DPD puissent recevoir le soutien, les contributions et les informations essentiels de ces autres services;
- formation continue.

Sources: article 38, paragraphe 2, du RGPD

10 Quelles sont les garanties permettant au DPD d'exercer ses missions en toute indépendance? Qu'entend-on par «conflit d'intérêts»?

Il existe plusieurs garanties permettant au DPD d'agir en toute indépendance:

- absence d'instruction de la part des responsables du traitement ou des sous-traitants en ce qui concerne l'exercice des missions du DPD;
- interdiction pour le responsable du traitement de licencier ou de sanctionner le DPD pour l'exercice de ses missions;
- absence de conflit d'intérêts avec d'autres missions et tâches possibles.

Les autres missions et tâches d'un DPD ne doivent pas donner lieu à un conflit d'intérêts. Cela signifie tout d'abord que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. En raison de la structure organisationnelle spécifique de chaque organisme, cet aspect doit être étudié au cas par cas.

En règle générale, parmi les fonctions susceptibles de donner lieu à un conflit d'intérêts au sein de l'organisme peuvent figurer les fonctions d'encadrement supérieur (par exemple, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique), mais aussi d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. En outre, il peut également y avoir conflit d'intérêts, par exemple, si un DPD externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.

Sources: article 38, paragraphes 3 et 6, du RGPD

Missions du DPD

11 Qu'entend-on par «surveillance du respect des règles»?

Dans le cadre de ces tâches de contrôle du respect du RGPD, les DPD peuvent notamment:

- recueillir des informations permettant de recenser les activités de traitement;
- analyser et vérifier la conformité des activités de traitement;
- informer et conseiller le responsable du traitement ou le sous-traitant et formuler des recommandations à son intention.

Sources: article 39, paragraphe 1, point b), du RGPD

12 Le DPD est-il personnellement responsable en cas de non-respect des exigences en matière de protection des données?

Non, le DPD n'est pas personnellement responsable en cas de non-respect des exigences en matière de protection des données. C'est le responsable du traitement ou le sous-traitant qui est tenu de s'assurer et doit être en mesure de démontrer que le traitement est effectué conformément au RGPD. Le respect de la protection des données relève de la responsabilité du responsable du traitement ou du sous-traitant.

13 Quel est le rôle du DPD en ce qui concerne l'analyse d'impact relative à la protection des données et le registre des activités de traitement?

En ce qui concerne l'analyse d'impact relative à la protection des données, le responsable du traitement ou le sous-traitant devrait solliciter l'avis du DPD sur les questions suivantes notamment:

- la question de savoir s'il convient ou non de procéder à une analyse d'impact relative à la protection des données;
- la méthodologie à suivre lors de la réalisation d'une analyse d'impact relative à la protection des données;
- la question de savoir s'il convient d'effectuer l'analyse d'impact relative à la protection des données en interne ou de la sous-traiter;
- les mesures (y compris des mesures techniques et organisationnelles) à appliquer pour atténuer les risques éventuels pesant sur les droits et les intérêts des personnes concernées;
- la question de savoir si l'analyse d'impact relative à la protection des données a été correctement réalisée et si ses conclusions (opportunité ou non de procéder au traitement et garanties à mettre en place) sont conformes aux exigences en matière de protection des données.

En ce qui concerne le registre des activités de traitement, c'est le responsable du traitement ou le sous-traitant, et non le DPD, qui est tenu de tenir un registre de ces opérations. Toutefois, rien ne s'oppose à ce que le responsable du traitement ou le sous-traitant confie au DPD la mission de tenir le registre des opérations de traitement effectuées sous la responsabilité du responsable du traitement ou du sous-traitant. Ce registre doit être considéré comme l'un des outils permettant au DPD d'exercer ses missions de contrôle du respect des règles ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant.

Sources: article 39, paragraphe 1, point c), et article 30 du RGPD

Fait à Bruxelles, le 13 décembre 2016

Pour le groupe de travail,
La présidente

Isabelle FALQUE-PIERROTIN

Version révisée et adoptée le 5 avril 2017

Pour le groupe de travail
La présidente

Isabelle FALQUE-PIERROTIN

30

Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant (WP244)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

16/FR
WP 244 rev.01

Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant

Adoptées le 13 décembre 2016
Version révisée et adoptée le 5 avril 2017

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et état de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO59 05/35.

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

Table des matières

1. Désignation d'une autorité de contrôle chef de file: notions principales

1.1. «Traitement transfrontalier de données à caractère personnel»

Il n'est pertinent de désigner une autorité de contrôle chef de file que lorsque le traitement transfrontalier de données à caractère personnel est effectué par un responsable du traitement ou un sous-traitant. L'article 4, point 23), du règlement général sur la protection des données (ci-après le «règlement général») définit le «traitement transfrontalier» comme suit:

- *un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres; ou*

- *un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres*.

Cela signifie que, si une organisation a des établissements en France et en Roumanie, par exemple, et si le traitement de données à caractère personnel a lieu dans le cadre de l'activité de ceux-ci, ce traitement constituera un traitement transfrontalier.

L'organisation peut aussi exercer une activité de traitement dans le seul cadre de son établissement situé en France. Toutefois, si cette activité affecte sensiblement, ou est susceptible d'affecter sensiblement, des personnes concernées en France et en Roumanie, elle sera également considérée comme un traitement transfrontalier.

1.1.1. Libellé «*substantially affects*» dans la version anglaise («affecte sensiblement»)

Le règlement général ne définit ni l'adverbe «*substantially*» («sensiblement») ni la forme verbale «*affects*» («affecte»). Ce libellé traduit l'intention de garantir que toutes les activités de traitement, *quel que soit leur effet*, qui ont lieu dans le cadre d'un seul établissement ne relèvent pas de la définition de «traitement transfrontalier».

Les significations les plus courantes du terme anglais «*substantial*» sont les suivantes: de grande dimension ou en quantité importante; assez important, assez grand ou d'une valeur indéniable, de grande importance; solide; de poids, important.

La signification la plus pertinente du verbe «*affect*» est «influencer» ou «avoir un effet important sur». Le substantif «*effect*» qui correspond au verbe «*affect*», signifie, entre autres, «résultat» ou «conséquence». Ces définitions suggèrent que, pour qu'un traitement de données *affecte* une personne, il faut qu'il ait une quelconque incidence sur cette dernière. Ainsi, un traitement qui n'a pas d'incidence significative sur les personnes ne relève pas de la seconde partie de la définition de «traitement transfrontalier». En revanche, il relève de la première partie de la définition s'il a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres.

Un traitement peut relever de la seconde partie de la définition non seulement s'il a une incidence sensible réelle, mais également s'il est susceptible d'avoir une telle incidence. Il convient d'observer que l'expression «susceptible de» ne signifie pas qu'il existe une lointaine possibilité d'incidence sensible. L'incidence sensible doit être plus probable qu'improbable. En revanche, cela signifie également qu'il n'est pas nécessaire que les personnes soient réellement affectées: la probabilité qu'elles soient sensiblement affectées suffit à faire entrer le traitement en cause dans le champ de la définition de «traitement transfrontalier».

Le fait qu'une opération de traitement de données puisse donner lieu au traitement d'un certain nombre – voire d'un grand nombre – de données à caractère personnel de personnes résidant dans un certain nombre d'États membres ne signifie pas nécessairement que ce traitement a ou est susceptible d'avoir une incidence significative. Un traitement qui n'a pas d'incidence sensible ne constitue pas un traitement transfrontalier au sens de la seconde partie de la définition, et ce quel que soit le nombre de personnes qu'il affecte.

Les autorités de contrôle interpréteront l'expression «affecte sensiblement» au cas par cas. Il sera tenu compte du contexte du traitement, du type de données, des finalités du traitement et de facteurs tels que le fait que le traitement:

- provoque ou est susceptible de provoquer un dommage, une perte ou des difficultés pour les personnes concernées;
- affecte ou est susceptible d'affecter réellement les personnes concernées en limitant leurs droits ou en les privant d'une possibilité;
- affecte ou est susceptible d'affecter la santé, le bien-être ou la tranquillité d'esprit des personnes concernées;
- affecte ou est susceptible d'affecter la condition ou la situation économique ou financière des personnes concernées;
- expose les personnes concernées à la discrimination ou à un traitement inéquitable;
- comporte l'analyse de catégories particulières de données à caractère personnel ou d'autres données intrusives, en particulier de données à caractère personnel relatives aux enfants;
- incite ou est susceptible d'inciter des personnes à modifier sensiblement leur comportement;
- a des conséquences improbables, inattendues ou indésirables pour les personnes concernées;
- cause une gêne ou entraîne d'autres effets négatifs, notamment une atteinte à la réputation; ou
- nécessite le traitement d'une gamme étendue de données à caractère personnel.

Enfin, le critère de l'«incidence sensible» vise à garantir que les autorités de contrôle sont uniquement tenues de coopérer de manière formelle dans le cadre du mécanisme de contrôle de la cohérence instauré par le règlement général «*lorsqu'une autorité de contrôle entend adopter une mesure destinée à produire des effets juridiques en ce qui concerne des opérations de traitement qui affectent sensiblement un nombre important de personnes concernées dans plusieurs États membres*» *(considérant 135).*

4

1.2. Autorité de contrôle chef de file

Pour dire les choses simplement, une «autorité de contrôle chef de file» est l'autorité qui assume la responsabilité principale de la gestion d'une activité de traitement transfrontalier, par exemple lorsqu'une personne concernée introduit une réclamation concernant le traitement de ses données à caractère personnel.

L'autorité de contrôle chef de file coordonnera toute enquête éventuelle, en y associant les autres autorités de contrôle «concernées».

La désignation de l'autorité de contrôle chef de file dépend du lieu de l'«établissement principal» ou de l'«établissement unique» dans l'Union du responsable du traitement. L'article 56 du règlement général dispose que:

- «*l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure* [de coopération] *prévue à l'article 60*».

1.3. Établissement principal

La notion d'«établissement principal» est définie comme suit à l'article 4, point 16), du règlement général:

- *en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son **administration centrale** dans l'Union, à moins que les **décisions quant aux finalités et aux moyens** du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le **pouvoir de faire appliquer ces décisions**, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal;*

- *en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent règlement.*

2. Étapes de la désignation de l'autorité de contrôle chef de file

2.1. Désignation de l'«établissement principal» des responsables du traitement

Pour localiser l'établissement principal, il est avant tout nécessaire d'identifier l'administration centrale du responsable du traitement dans l'Union, s'il y en a une[1].

[1] Le règlement général présente de l'intérêt pour l'EEE et s'y appliquera après son intégration dans l'accord EEE. Il fait actuellement l'objet d'un examen en vue de cette intégration, voir http://www.efta.int/eea-lex/32016R0679

Conformément à l'approche ressortant du règlement général, l'administration centrale dans l'Union est le lieu où sont prises les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel, et ce lieu a le pouvoir de faire appliquer ces décisions.

L'essence-même du principe de l'autorité chef de file établi par le règlement général est que le contrôle du traitement transfrontalier ne doit être effectué que par une seule autorité de contrôle dans l'Union. Lorsque des décisions portant sur différentes activités de traitement transfrontalier sont prises au sein de l'administration centrale dans l'Union, il n'y aura qu'une seule autorité de contrôle chef de file pour les diverses activités de traitement de données effectuées par la société multinationale. Il se peut toutefois qu'un établissement autre que le lieu de l'administration centrale prenne des décisions autonomes quant aux finalités et aux moyens d'une activité de traitement spécifique. Cela signifie que, dans certaines situations, plusieurs autorités chefs de file peuvent être identifiées à savoir lorsqu'une société multinationale décide de disposer de différents centres de décision, situés dans différents pays, pour différentes activités de traitement.

Il convient de rappeler que, lorsqu'une entreprise multinationale centralise l'ensemble des décisions quant aux finalités et aux moyens du traitement dans un de ses établissements situés dans l'Union (et que cet établissement a le pouvoir de faire appliquer ces décisions), une seule autorité de contrôle chef de file sera désignée pour cette multinationale.

En pareilles situations, il est essentiel que les entreprises déterminent avec précision le lieu où sont prises les décisions quant aux finalités et aux moyens du traitement. Il est de l'intérêt des responsables du traitement et des sous-traitants de déterminer correctement l'établissement principal dans la mesure où cela leur permet de savoir quelle est l'autorité de contrôle compétente au regard des nombreuses obligations qui leur incombent en vertu du règlement général. Il peut s'agir, le cas échéant, de désigner un délégué à la protection des données ou de solliciter des conseils au sujet d'une activité de traitement à risque pour laquelle le responsable du traitement ne peut atténuer les risques par des moyens raisonnables. Les dispositions en la matière du règlement général visent à permettre le respect de ces obligations.

Les exemples ci-dessous illustrent ces dispositions.

Exemple 1: Un détaillant de produits alimentaires a son siège (c'est-à-dire le «lieu de son administration centrale») à Rotterdam, aux Pays-Bas. Il possède des établissements dans plusieurs autres États membres, qui y entretiennent des contacts avec des personnes. Tous ces établissements utilisent le même logiciel pour traiter les données à caractère personnel des consommateurs à des fins de marketing. Toutes les décisions quant aux finalités et aux moyens du traitement des données à caractère personnel des consommateurs à des fins de marketing sont prises au siège, à Rotterdam. De ce fait, l'autorité de contrôle chef de file de cette société au regard de cette activité de traitement transfrontalier est l'autorité de contrôle des Pays-Bas.

Exemple 2: Une banque a son siège à Francfort, à partir duquel elle organise toutes[2] ses activités de traitement bancaire, mais son service «Assurances» se trouve à Vienne. Conformément à l'article 4, point 16), du règlement général, si l'établissement de Vienne est habilité à prendre des décisions concernant les activités de traitement de données relatives aux assurances et à faire appliquer ces décisions dans l'ensemble de l'Union, l'autorité de contrôle autrichienne serait alors l'autorité chef de file pour ce qui concerne le traitement transfrontalier de données à caractère personnel à des fins d'assurances, et les autorités allemandes (l'autorité de contrôle du Land de Hesse) seraient chargées du contrôle du traitement des données à caractère personnel à des fins bancaires, peu importe où les clients sont établis[3].

2.1.1. Critères pour la désignation de l'établissement principal du responsable du traitement lorsqu'il ne s'agit pas du lieu de l'administration centrale de celui-ci dans l'Union

Le considérant 36 du règlement général apporte un éclairage sur le facteur essentiel à prendre en considération pour déterminer l'établissement principal d'un responsable du traitement lorsque le critère de l'administration centrale ne s'applique pas. Il convient ainsi de déterminer le lieu de l'exercice effectif et réel des activités de gestion déterminant les principales décisions quant aux finalités et aux moyens du traitement dans le cadre d'un dispositif stable. Le considérant 36 précise également que «[l]a présence et l'utilisation de moyens techniques et de technologies de traitement de données à caractère personnel ou d'activités de traitement ne constituent pas, en elles-mêmes, un établissement principal et ne sont, dès lors, pas des critères déterminants pour un établissement principal».

Le responsable du traitement détermine lui-même où se situe son établissement principal et, dès lors, sous quelle autorité de contrôle chef de file il se place. Toutefois, ce point peut être contesté ultérieurement par l'autorité de contrôle concernée.

Les facteurs énoncés ci-dessous sont utiles pour déterminer le lieu de l'établissement principal d'un responsable du traitement, au sens du règlement général, lorsqu'il ne s'agit pas du lieu de son administration centrale dans l'Union.

- Où les décisions finales quant aux finalités et aux moyens du traitement sont-elles prises?
- Où les décisions relatives aux activités commerciales nécessitant un traitement de données sont-elles prises?
- Où le pouvoir de faire appliquer les décisions se concentre-t-il effectivement?

[2] Nous sommes conscients que le traitement de données à caractère personnel à des fins bancaires englobe un grand nombre d'activités de traitement différentes. Toutefois, dans un souci de simplification, nous les considérons comme un tout. Il en va de même pour le traitement effectué à des fins d'assurances.

[3] Il convient de rappeler également que le règlement général prévoit la possibilité d'effectuer un contrôle local dans certains cas. Voir le considérant 127: *«Chaque autorité de contrôle* ***qui ne fait pas office d'autorité de contrôle chef de file devrait être compétente pour traiter les cas de portée locale*** *lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres mais que l'objet du traitement spécifique ne se rapporte* ***qu'à un traitement effectué dans un seul État membre et ne porte que sur des personnes concernées de ce seul État membre****, par exemple lorsqu'il s'agit de traiter des données à caractère personnel relatives à des employés dans le contexte des relations de travail propre à un État membre.»* Ce principe signifie que le contrôle des données relatives aux ressources humaines en rapport avec le marché du travail local pourrait incomber à plusieurs autorités de contrôle.

- Où le directeur (ou les directeurs) assumant la responsabilité générale de la gestion du traitement transfrontalier est-il établi?
- Où le responsable du traitement ou le sous-traitant est-il inscrit au registre des sociétés, s'il est implanté dans un seul territoire?

Veuillez noter que cette liste n'est pas exhaustive. En fonction du responsable du traitement ou de l'activité de traitement en cause, d'autres facteurs peuvent se révéler pertinents. Si une autorité de contrôle a des raisons de douter que l'établissement indiqué par le responsable du traitement est l'établissement principal aux fins de l'application du règlement général, elle peut – bien entendu – exiger du responsable du traitement qu'il fournisse les informations supplémentaires nécessaires afin de prouver le lieu de l'établissement principal.

2.1.2. Groupes d'entreprises

Lorsque le traitement est effectué par un groupe d'entreprises dont le siège est établi dans l'Union, l'établissement de l'entreprise qui exerce le contrôle global est réputé être le centre de décision lié au traitement des données à caractère personnel, et sera donc considéré comme étant l'établissement principal du groupe, excepté lorsque les décisions quant aux finalités et aux moyens du traitement sont prises par un autre établissement. L'établissement principal sera probablement la société mère ou le siège opérationnel du groupe d'entreprises dans l'Union, puisque c'est là que se trouvera l'administration centrale de ce dernier.

La référence, dans la définition, au lieu de l'administration centrale d'un responsable du traitement fonctionne bien pour les organisations disposant d'un siège décisionnel centralisé et d'une structure en succursales. Il est clair, en pareil cas, que le pouvoir de prendre des décisions concernant le traitement de données transfrontalier et de les faire appliquer relève de la compétence du siège de la société. Il est aisé, dans une telle situation, de déterminer le lieu de l'établissement principal et, par là même, l'autorité de contrôle qui fera office d'autorité de contrôle chef de file. Toutefois, il se peut que le système décisionnel de certains groupes d'entreprises soit plus complexe, différents établissements se voyant confier des pouvoirs décisionnels indépendants en matière de traitement transfrontalier. Les critères établis ci-dessus devraient aider les groupes d'entreprises à désigner leur établissement principal.

2.1.3. Responsables conjoints du traitement

Le règlement général ne couvre pas spécifiquement la question de la désignation d'une autorité chef de file lorsque plusieurs responsables du traitement établis dans l'Union déterminent conjointement les finalités et les moyens du traitement, c'est-à-dire en cas de responsables conjoints du traitement. L'article 26, paragraphe 1, et le considérant 79 indiquent clairement que, dans cette situation, les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du règlement. Par conséquent, pour pouvoir bénéficier du principe de guichet unique, les responsables conjoints du traitement doivent désigner celui de leurs établissements (parmi ceux où les décisions sont prises) qui aura le pouvoir de faire appliquer les décisions concernant le traitement à l'égard de l'ensemble des responsables conjoints du traitement. Cet établissement sera alors considéré comme l'établissement principal pour les traitements impliquant des responsables conjoints du traitement. L'accord entre les responsables conjoints du traitement est sans préjudice des règles en matière de responsabilité établies par le règlement général, en particulier à l'article 82, paragraphe 4.

2.2. Cas particuliers

Dans certains cas particuliers et complexes, il sera difficile d'établir le lieu de l'établissement principal ou de déterminer où les décisions concernant le traitement de données sont prises. Ce peut être le cas lorsqu'il y a une activité de traitement transfrontalier et que le responsable du traitement est établi dans plusieurs États membres, mais qu'il n'y a pas d'administration centrale dans l'Union et qu'aucun des établissements dans l'Union ne prend de décisions quant au traitement (c'est-à-dire que les décisions sont prises exclusivement en dehors de l'Union).

Dans le cas de figure ci-dessus, la société qui effectue le traitement transfrontalier peut souhaiter être contrôlée par une autorité chef de file afin de bénéficier du principe de guichet unique. Or, le règlement général ne prévoit pas de solution pour ce type de situation. En pareilles circonstances, la société devrait désigner en tant qu'établissement principal l'établissement qui est habilité à faire appliquer les décisions relatives à l'activité de traitement et à assumer la responsabilité de ce traitement, notamment en disposant d'actifs suffisants. Si aucun établissement principal n'est ainsi désigné par la société, il ne sera pas possible de désigner une autorité chef de file, mais les autorités de contrôle pourront toujours mener des enquêtes plus poussées, s'il y a lieu.

Le règlement général n'autorise pas l'élection de juridiction («forum shopping»). Si une société affirme avoir son établissement principal dans un État membre, mais qu'aucun exercice réel d'activités de gestion ou aucune prise de décision concernant le traitement de données à caractère personnel n'y a lieu, les autorités de contrôle compétentes (ou, en dernier recours, le comité européen de la protection des données – CEPD) désigneront l'autorité de contrôle «chef de file», sur la base de critères objectifs et des éléments de preuve disponibles. Le processus visant à déterminer le lieu de l'établissement principal peut exiger des autorités de contrôle qu'elles enquêtent et coopèrent activement. Les conclusions ne peuvent reposer exclusivement sur des déclarations de l'organisation considérée. La charge de la preuve incombe en dernier ressort aux responsables du traitement et aux sous-traitants, qui doivent fournir aux autorités de contrôle concernées la preuve du lieu où les décisions relatives au traitement de données sont prises et du lieu où réside le pouvoir de faire appliquer ces décisions. La tenue de registres des activités de traitement de données aiderait à la fois les organisations et les autorités de contrôle à déterminer quelle est l'autorité chef de file. L'autorité de contrôle chef de file, ou les autorités concernées, peuvent réfuter l'analyse du responsable du traitement sur la base d'un examen objectif des faits pertinents, en demandant des informations complémentaires si nécessaire.

Dans certains cas, les autorités de contrôle compétentes demanderont au responsable du traitement de démontrer clairement, conformément à toutes lignes directrices du CEPD, où se trouve le lieu de son établissement principal ou le lieu dans lequel sont prises les décisions relatives à une activité de traitement en particulier. Les éléments de preuve fournis seront dûment pris en considération et les autorités de contrôle concernées coopéreront pour décider laquelle d'entre elles agira en tant que chef de file lors des enquêtes. Ces cas ne seront portés devant le CEPD pour décision en vertu de l'article 65, paragraphe 1, point b), du règlement général que lorsque les autorités de contrôle auront des points de vue divergents quant à la désignation de l'autorité de contrôle chef de file. Toutefois, dans la plupart des cas, les autorités de contrôle compétentes devraient être en mesure de convenir d'une ligne de conduite mutuellement satisfaisante.

2.3. Sous-traitant

En vertu du règlement général, les sous-traitants visés par ledit règlement et établis dans plusieurs États membres peuvent également bénéficier du système de guichet unique.

Selon l'article 4, point 16) b), du règlement général, l'établissement principal du sous-traitant sera le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement dans l'Union où se déroule l'essentiel de ses activités de traitement.

Toutefois, conformément au considérant 36, lorsque le responsable du traitement et le sous-traitant sont tous deux concernés, l'autorité de contrôle chef de file compétente devrait être celle du responsable du traitement. Dans cette situation, l'autorité de contrôle du sous-traitant sera une «autorité de contrôle concernée» et devrait participer à la procédure de coopération. Cette règle ne s'applique que lorsque le responsable du traitement est établi dans l'Union. Les responsables du traitement visés à l'article 3, paragraphe 2, du règlement général ne seront pas soumis au mécanisme de guichet unique. Un sous-traitant, par exemple un grand fournisseur de services en nuage, peut fournir des services à de multiples responsables du traitement situés dans différents États membres. Dans ce cas, l'autorité de contrôle chef de file sera l'autorité de contrôle compétente pour agir en tant que chef de file pour le responsable du traitement. Dans la pratique, cela signifie qu'un sous-traitant pourrait devoir traiter avec plusieurs autorités de contrôle.

3. Autres questions pertinentes

3.1. Le rôle de l'«autorité de contrôle concernée»

Aux termes de l'article 4, point 22), du règlement général, on entend par:

> *«autorité de contrôle concernée», une autorité de contrôle qui est concernée par le traitement de données à caractère personnel parce que: a) le responsable du traitement ou le sous-traitant est établi sur le territoire de l'État membre dont cette autorité de contrôle relève; b) des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être; ou c) une réclamation a été introduite auprès de cette autorité de contrôle.*

Le concept d'autorité de contrôle concernée vise à garantir que le modèle de l'«autorité chef de file» n'empêche pas les autres autorités de contrôle d'avoir un droit de regard sur la façon dont une question est traitée lorsque, par exemple, des personnes résidant en dehors de la juridiction de l'autorité chef de file sont sensiblement affectées par une activité de traitement de données. Pour ce qui est du point a) de la définition, les mêmes considérations valent pour la désignation d'une autorité chef de file. Il convient de noter qu'au point b), la personne concernée doit simplement résider dans l'État membre en question; elle ne doit pas nécessairement être ressortissante de cet État. En ce qui concerne le point c), il sera généralement aisé d'établir, de manière formelle, si une autorité de contrôle en particulier a reçu une réclamation.

L'article 56, paragraphes 2 et 5, du règlement général permet à une autorité de contrôle concernée de participer au traitement d'un cas sans être l'autorité de contrôle chef de file.

Lorsqu'une autorité de contrôle chef de file décide de ne pas traiter un cas, l'autorité de contrôle concernée qui l'a informée le traite. Cette disposition est conforme aux procédures prévues à l'article 61 (assistance mutuelle) et à l'article 62 (opérations conjointes des autorités de contrôle) du règlement général. Ce cas de figure peut se présenter lorsqu'une entreprise de commercialisation dont l'établissement principal est à Paris lance un produit qui n'affecte que des personnes concernées résidant au Portugal. En pareille situation, les autorités de contrôle française et portugaise peuvent convenir qu'il y a lieu de désigner l'autorité de contrôle portugaise comme chef de file pour le traitement de ce cas. Les autorités de contrôle peuvent exiger des responsables du traitement qu'ils fournissent des informations précisant les modalités qui les lient. Dès lors que cette activité de traitement a des effets purement locaux – c'est-à-dire qu'elle n'affecte que des personnes résidant au Portugal – les autorités de contrôle française et portugaise ont le pouvoir discrétionnaire de choisir l'autorité de contrôle qui traitera ce cas, conformément au considérant 127 du règlement général.

En vertu du règlement général, l'autorité de contrôle chef de file et les autorités de contrôle concernées sont tenues de coopérer, dans le respect des points de vue de chacune d'entre elles, pour garantir que le cas est examiné et résolu à la satisfaction de chaque autorité, en offrant un droit de recours effectif aux personnes concernées. Les autorités de contrôle s'efforceront d'adopter une ligne de conduite mutuellement acceptable. Le mécanisme formel de contrôle de la cohérence ne devrait être invoqué que lorsque la coopération ne permet pas de parvenir à une solution mutuellement acceptable.

L'acceptation mutuelle des décisions peut s'appliquer non seulement aux conclusions de fond, mais également aux décisions relatives à la ligne de conduite adoptée, y compris en ce qui concerne les activités visant à garantir le respect des règles (enquête approfondie ou enquête de portée limitée, par exemple). Elle peut également s'appliquer à une décision de ne pas traiter un cas conformément au règlement général, en raison, par exemple, d'une politique de priorités, ou de l'existence d'autres autorités concernées, telles que décrit plus haut.

L'adoption d'une approche consensuelle et la bonne volonté des autorités de contrôle sont fondamentales pour la réussite du processus de coopération et de contrôle de la cohérence établi par le règlement général.

3.2. Traitement local

L'activité de traitement local de données ne relève pas des dispositions du règlement général relatives à la coopération et au contrôle de la cohérence. Les autorités de contrôle respecteront leur compétence respective à traiter localement les activités de traitement local de données. Les traitements effectués par des autorités publiques seront toujours examinés au niveau «local» également.

3.3. Sociétés établies en dehors de l'Union

Le mécanisme de coopération et de contrôle de la cohérence prévu par le règlement général ne s'applique qu'aux responsables du traitement possédant au moins un établissement dans l'Union européenne. Si la société ne possède aucun établissement dans l'Union, la simple présence d'un représentant dans un État membre ne permet pas d'appliquer le système de guichet unique. Cela signifie que les responsables du traitement ne possédant aucun établissement dans l'Union doivent s'adresser aux autorités de contrôle locales dans chaque

État membre dans lesquels ils exercent des activités, par l'intermédiaire de leur représentant local.

Fait à Bruxelles, le 13 décembre 2016

Pour le groupe de travail,
La présidente
Isabelle FALQUE-PIERROTIN

Version révisée et adoptée le 5 avril 2017

Pour le groupe de travail
La présidente
Isabelle FALQUE-PIERROTIN

12

ANNEXE – Questions relatives à la désignation de l'autorité de contrôle chef de file

1. Le responsable du traitement ou le sous-traitant effectue-t-il un traitement transfrontalier de données à caractère personnel?

a. Oui, si:

- le responsable du traitement ou le sous-traitant est établi dans plus d'un État membre et
- le traitement de données à caractère personnel a lieu dans le cadre des activités d'établissements situés dans plus d'un État membre.

➢ Dans ce cas, allez au point 2.

b. Oui, si:

- le traitement de données à caractère personnel a lieu dans le cadre des activités de l'établissement unique d'un responsable du traitement ou d'un sous-traitant dans l'Union, mais
- affecte sensiblement ou est susceptible d'affecter sensiblement des personnes dans plus d'un État membre.

➢ Dans ce cas, l'autorité chef de file est l'autorité dont relève l'établissement unique du responsable du traitement ou du sous-traitant dans un seul État membre. Il doit, en toute logique, s'agir de l'établissement principal du responsable du traitement ou du sous-traitant, étant donné que c'est leur seul établissement.

2. Comment désigner l'«autorité de contrôle chef de file»

a. Dans le cas où il y a uniquement un responsable du traitement:

i. déterminer le lieu de l'administration centrale du responsable du traitement dans l'Union;

ii. l'autorité de contrôle du pays où se situe le lieu de l'administration centrale est l'autorité chef de file du responsable du traitement.

Toutefois:

iii. si les décisions quant aux finalités et aux moyens du traitement sont prises dans un autre établissement situé dans l'Union, et que cet établissement a le pouvoir de faire appliquer ces décisions, l'autorité chef de file est alors celle du pays où est situé cet établissement.

b. Dans le cas où il y a un responsable du traitement et un sous-traitant:

i. vérifier si le responsable du traitement est établi dans l'Union et s'il est soumis au système de guichet unique. Si tel est le cas;

ii. désigner l'autorité de contrôle chef de file du responsable du traitement. Cette autorité sera également l'autorité de contrôle chef de file pour le sous-traitant;

iii. l'autorité de contrôle (non-chef de file) dont relève le sous-traitant sera une «autorité concernée» – voir le point 3 ci-dessous.

c. Dans le cas où il y a uniquement un sous-traitant:

i. déterminer le lieu de l'administration centrale du sous-traitant dans l'Union;

ii. si le sous-traitant n'a pas d'administration centrale dans l'Union, déterminer l'établissement dans l'Union où ont lieu ses activités de traitement principales.

d. Dans le cas où il y a des responsables conjoints du traitement:

i. vérifier si les responsables conjoints du traitement sont établis dans l'Union;

ii. désigner, parmi les établissements où sont prises les décisions quant aux finalités et aux moyens du traitement, celui qui a le pouvoir de faire appliquer ces décisions à l'égard de l'ensemble des responsables conjoints du traitement. Cet établissement sera alors considéré comme l'établissement principal pour le traitement effectué par les responsables conjoints du traitement. L'autorité chef de file est celle du pays où se situe cet établissement.

3. Y a-t-il des «autorités de contrôle concernées»?

Une autorité est une «autorité concernée»:

- lorsque le responsable du traitement ou le sous-traitant dispose d'un établissement sur son territoire; ou
- lorsque des personnes concernées présentes sur son territoire sont sensiblement affectées par le traitement ou susceptibles de l'être; ou
- lorsqu'une réclamation a été reçue par une autorité particulière.

Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679 (WP248)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP 248 rév. 01

Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679

Adoptées le 4 avril 2017

Telles que modifiées et adoptées en dernier lieu le 4 octobre 2017

Ce groupe de travail a été institué en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant traitant des questions liées à la protection des données et au respect de la vie privée. Ses missions sont décrites à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Son secrétariat est assuré par la Direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale de la justice de la Commission européenne, B-1049 Bruxelles, Belgique, bureau nº MO-59 03/075.

Site internet: http://ec.europa.eu/justice/data-protection/index_en.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué en vertu de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ARRÊTÉ LES PRÉSENTES LIGNES DIRECTRICES:

SOMMAIRE

I. Introduction

Le règlement (UE) 2016/679[1] (RGPD) s'appliquera à partir du 25 mai 2018. De la même manière que la directive 2016/680[2], l'article 35 du RGPD introduit la notion d'analyse d'impact relative à la protection des données (AIPD[3]),

Une AIPD est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de leurs données à caractère personnel[4], en les évaluant et en déterminant les mesures nécessaires pour y faire face. Les AIPD sont un outil important au regard du principe de responsabilité, compte tenu de leur utilité pour les responsables du traitement non seulement aux fins du respect des exigences du RGPD, mais également en ce qui concerne leur capacité à démontrer que des mesures appropriées ont été prises pour assurer la conformité au règlement (voir également l'article 24)[5]. Autrement dit, **une AIPD est un processus qui vise à assurer la conformité aux règles et à pouvoir en apporter la preuve**.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[2] L'article 27 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données dispose également qu'une analyse d'impact sur la vie privée est nécessaire lorsque le traitement «*est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques*».

[3] On parle souvent, dans d'autres contextes, d'«analyse d'impact sur la vie privée» pour désigner la même notion.

[4] Si le RGPD ne définit pas formellement la notion d'AIPD en tant que telle,

- l'article 35, paragraphe 7, dispose que l'analyse doit au moins contenir:
  - «*a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;*
  - *b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;*
  - *c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et*
  - *d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées»;*
- son sens et son rôle sont clarifiés au considérant 84 comme suit: «*Afin de mieux garantir le respect du présent règlement lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque*».

[5] Voir également le considérant 84: «*Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement*».

En vertu du RGPD, le non-respect des exigences applicables en matière d'AIPD peut donner lieu à des amendes imposées par l'autorité de contrôle compétente. Le fait de ne pas effectuer d'AIPD alors que le traitement est soumis à l'obligation d'une telle analyse (article 35, paragraphes 1, 3 et 4), de réaliser l'analyse d'une manière incorrecte (article 35, paragraphes 2 et 7 à 9) ou de ne pas consulter l'autorité de contrôle compétente lorsque la situation l'exige (article 36, paragraphe 3, point e), est passible d'une amende administrative pouvant s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

II. Objectifs des présentes lignes directrices

Les présentes lignes directrices tiennent compte:

- de la déclaration 14/EN WP 218 du groupe de travail «Article 29» sur la protection des données (GT29)[6];
- des lignes directrices 16/EN WP 243 du GT29 relatives aux délégués à la protection des données[7];
- de l'avis 13/EN WP 203 du GT29 relatif à la limitation des finalités[8];
- des normes internationales pertinentes[9].

Conformément à l'approche par les risques préconisée par le RGPD, il n'est pas obligatoire d'effectuer une AIPD pour chaque opération de traitement. Une AIPD n'est requise que lorsque le traitement est «*susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*» (article 35, paragraphe 1). Afin de garantir une interprétation cohérente des situations dans lesquelles une AIPD est obligatoire (article 35, paragraphe 3), les présentes lignes directrices s'appliquent en premier lieu à éclaircir cet aspect et fournissent des critères pour les listes que les autorités de protection des données (APD) sont tenues d'adopter en vertu de l'article 35, paragraphe 4.

Conformément à l'article 70, paragraphe 1, point e), le Comité européen de la protection des données (CEPD) pourra publier des lignes directrices, recommandations et bonnes pratiques afin d'encourager une application cohérente du RGPD. Le présent document ayant pour objet d'anticiper les travaux futurs du CEPD, il s'emploie à clarifier les dispositions pertinentes du RGPD afin de faciliter le

[6] Déclaration 14/EN WP 218 du G29 concernant le rôle d'une approche par les risques dans les cadres juridiques de la protection des données (en anglais), adoptée le 30 mai 2014.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Lignes directrices 16/EN WP 243 du G29 relatives aux délégués à la protection des données (en anglais), adoptées le 13 décembre 2016.
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Avis 13/EN WP 203 du G29 de mars 2013 relatif à la limitation des finalités, adopté le 2 avril 2013.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Par ex., ISO 31000:2009, *Management du risque – Principes et lignes directrices*, Organisation internationale de normalisation (ISO); ISO/IEC 29134 (projet, indisponible en français), *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'évaluation d'impacts sur la vie privée*, Organisation internationale de normalisation (ISO).

respect de la législation par les responsables du traitement et de procurer une sécurité juridique aux responsables du traitement tenus d'effectuer une AIPD.

Ces lignes directrices s'efforcent également de promouvoir la mise en place:

- d'une liste commune à l'échelle de l'Union des opérations de traitement pour lesquelles une AIPD est obligatoire (article 35, paragraphe 4);
- d'une liste commune à l'échelle de l'Union des opérations de traitement pour lesquelles une AIPD n'est pas nécessaire (article 35, paragraphe 5);
- de critères communs concernant la méthodologie à suivre pour la réalisation d'une AIPD (article 35, paragraphe 5);
- de critères communs pour la détermination des cas dans lesquels l'autorité de contrôle doit être consultée (article 36, paragraphe 1);
- de recommandations basées sur l'expérience acquise dans les États membres de l'UE, dans la mesure du possible.

III. Les AIPD: explication du règlement

Le RGPD exige des responsables du traitement qu'ils mettent en œuvre des mesures appropriées pour assurer et être en mesure de démontrer la conformité de leurs opérations avec les dispositions du règlement, en tenant compte notamment «des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques» (article 24, paragraphe 1). L'obligation pour les responsables du traitement d'effectuer une AIPD dans certaines situations doit être comprise dans le contexte de leur obligation générale de gérer de manière appropriée les risques[10] que présente le traitement de données personnelles.

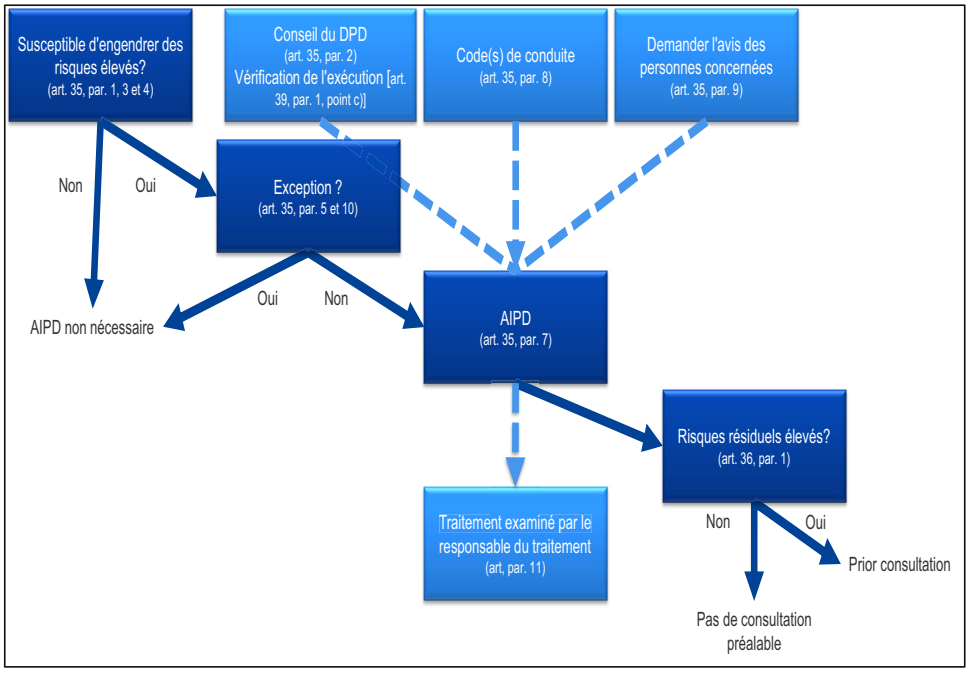
Un «risque» est un scénario qui décrit un événement et ses effets, estimés en termes de gravité et de probabilité. La «gestion du risque» peut, quant à elle, se définir comme un ensemble d'activités coordonnées dans le but de diriger et de piloter un organisme vis-à-vis du risque.

L'article 35 évoque un risque potentiellement élevé «pour les droits et libertés des personnes physiques». Comme indiqué dans la déclaration du GT29 concernant le rôle d'une approche par les risques dans les cadres juridiques de la protection des données, la référence aux «droits et libertés» des personnes concernées vise principalement les droits à la protection des données et à la vie privée, mais s'entend également, le cas échéant, pour d'autres droits fondamentaux, tels que la liberté de parole, la liberté de pensée, la liberté de circulation, l'interdiction de toute discrimination, le droit à la liberté ainsi que la liberté de conscience et de religion.

Conformément à l'approche par les risques préconisée par le RGPD, il n'est pas obligatoire d'effectuer une AIPD pour chaque opération de traitement. Ainsi, une AIPD n'est requise que lorsqu'un type de traitement est «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques» (article 35, paragraphe 1). Le simple fait que les conditions déclenchant l'obligation d'effectuer une AIPD ne soient pas remplies ne restreint toutefois pas l'exigence générale faite aux responsables du traitement de mettre en œuvre des mesures pour gérer de manière appropriée les risques pour les droits et libertés des personnes concernées. Concrètement, cela signifie que les responsables du traitement sont tenus d'évaluer de manière continue les risques créés par leurs activités de traitement dans le but d'identifier quand un type de traitement est «susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques».

[10] Il convient de souligner que la gestion des risques pour les droits et libertés des personnes physiques suppose d'identifier ces risques, de les analyser, de les estimer, de les évaluer, de les traiter (par ex. en les atténuant) et de les réexaminer régulièrement. Les responsables du traitement ne sauraient se soustraire à leurs responsabilités en recourant à des polices d'assurance pour couvrir les risques.

Le schéma suivant illustre les principes de base adoptés par le RGPD en ce qui concerne les AIPD:



A. Sur quoi porte une AIPD? Une opération de traitement unique? Un ensemble d'opérations de traitement similaires?

Une AIPD peut concerner une opération de traitement de données unique. Cependant, l'article 35, paragraphe 1 dispose qu'«*une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires*». Le considérant 92 ajoute qu'«*il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée*».

Une seule et même AIPD peut être utilisée pour évaluer plusieurs opérations de traitement similaires en termes de nature, de portée, de contexte, de finalités et de risques. En effet, les AIPD visent à assurer l'étude systématique des nouvelles situations susceptibles d'entraîner des risques élevés pour les droits et libertés des personnes physiques, et il n'est pas nécessaire de procéder à une AIPD dans les cas (à savoir des opérations de traitement effectuées dans un contexte spécifique et à des fins spécifiques) qui ont déjà été étudiés. Tel peut être le cas lorsque des technologies similaires sont utilisées pour collecter le même type de données pour les mêmes finalités. Par exemple, un groupe d'autorités municipales mettant chacune en place un système similaire de surveillance par CCTV pourrait se contenter d'une AIPD unique couvrant le traitement envisagé par chacun de ces responsables distincts; un opérateur ferroviaire (un seul responsable du traitement) pourrait quant à lui couvrir la vidéosurveillance de l'ensemble de ses gares au moyen d'une seule et même AIPD. Ceci

peut également valoir pour des opérations de traitement similaires mises en œuvre par différents responsables du traitement. Dans pareils cas, il y a lieu qu'une AIPD de référence soit partagée ou rendue publiquement accessible, les mesures décrites dans l'AIPD doivent être mises en œuvre et une justification de la réalisation d'une AIPD unique doit être fournie.

Lorsque l'opération de traitement implique des responsables conjoints du traitement, ceux-ci doivent définir précisément leurs obligations respectives. Il convient que leur AIPD détermine quelle partie est responsable des différentes mesures destinées à faire face aux risques et à protéger les droits et libertés des personnes concernées, et que chaque responsable du traitement exprime ses besoins et partage les informations utiles en veillant à ne pas compromettre de secrets (secrets d'affaires, propriété intellectuelle, informations commerciales confidentielles, par ex.) et à ne pas divulguer de vulnérabilités.

Une AIPD peut également être utile pour évaluer l'impact sur la protection des données d'un produit technologique, par exemple un matériel ou un logiciel, lorsque celui-ci est susceptible d'être utilisé par divers responsables du traitement pour réaliser différentes opérations de traitement. Bien entendu, le responsable du traitement déployant le produit reste tenu d'effectuer sa propre AIPD pour ce qui concerne sa mise en œuvre spécifique, mais il peut s'appuyer pour cela sur une AIPD élaborée par le fournisseur du produit, le cas échéant. Prenons l'exemple de la relation entre fabricants de compteurs intelligents et entreprises de services publics. Il conviendrait que chaque fournisseur ou sous-traitant partage les informations utiles en s'assurant de ne compromettre aucun secret ni de menacer la sécurité en divulguant des vulnérabilités.

B. Quelles sont les opérations de traitement qui requièrent une AIPD? Sauf cas exceptionnel, toutes celles qui sont «*susceptibles d'engendrer un risque élevé*».

Cette section explique dans quels cas une AIPD est obligatoire et dans quels cas elle n'est pas nécessaire.

À moins que l'opération de traitement ne relève d'un cas exceptionnel [III, B, a)], il convient d'effectuer une AIPD dès lors que le traitement est «*susceptible d'engendrer un risque élevé*» [III, B, b)].

a) Quand une AIPD est-elle obligatoire? Lorsque le traitement est «*susceptible d'engendrer un risque élevé*».

Le RGPD n'exige pas une AIPD pour toute opération de traitement qui pourrait engendrer des risques pour les droits et libertés des personnes physiques. La réalisation d'une AIPD n'est obligatoire que quand le traitement est *«susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques»* (article 35, paragraphe 1, illustré par l'article 35, paragraphe 3, et complété par l'article 35, paragraphe 4). Elle est particulièrement pertinente en cas de recours à une nouvelle technologie de traitement[11].

En cas de doute quant à la nécessité d'effectuer une AIPD, dans la mesure où les AIPD sont un outil important pour les responsables du traitement aux fins du respect de la législation sur la protection des données, le GT29 recommande d'en effectuer une malgré tout.

[11] Les considérants 89 et 91 ainsi que l'article 35, paragraphes 1 et 3, fournissent d'autres d'exemples.

Même si une AIPD peut également être requise dans d'autres situations, l'article 35, paragraphe 3, considère que le traitement est *«susceptible d'engendrer un risque élevé»* en particulier dans les cas suivants:

- *«a) l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire*[12]*;*
- *b) le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10*[13]*; ou*
- *c) la surveillance systématique à grande échelle d'une zone accessible au public»*.

Comme le laissent entendre les mots *«en particulier»* dans la phrase introductive de l'article 35, paragraphe 3, du RGPD, il s'agit là d'une liste non exhaustive. Même si elles ne figurent pas dans cette liste, d'autres opérations de traitement peuvent néanmoins présenter un risque aussi élevé. Ces opérations de traitement doivent également faire l'objet d'une AIPD. C'est la raison pour laquelle les critères exposés ci-dessous vont parfois au-delà d'une simple explication de ce que les trois exemples de l'article 35, paragraphe 3, du RGPD donnent à comprendre.

Pour donner une vision plus concrète des opérations de traitement qui nécessitent une AIPD du fait d'un risque inhérent élevé, compte tenu des éléments particuliers de l'article 35, paragraphes 1 et 3, points a) à c), de la liste à adopter au niveau national en vertu de l'article 35, paragraphe 4, et des considérants 71, 75 et 91, ainsi que des autres références du RGPD aux opérations de traitement «*susceptibles d'engendrer un risque élevé*»[14], il convient de prendre en compte les neuf critères ci-après.

1. Évaluation ou notation, y compris les activités de profilage et de prédiction, portant notamment sur des «*aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements*» (considérants 71 et 91). À titre d'exemples, prenons le cas d'un établissement financier passant ses clients au crible d'une base de données de cote de crédit ou d'une base de données dédiée à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) ou «antifraude», celui d'une société de biotechnologie proposant des tests génétiques directement aux consommateurs afin d'évaluer et de prédire les risques de maladie/de problèmes de santé, ou encore celui d'une entreprise analysant les usages ou la navigation sur son site Web pour créer des profils comportementaux ou marketing.

[12] Voir le considérant 75: *«notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels»*.

[13] Voir le considérant 75: *«lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes»*.

[14] Voir par exemple les considérants 75, 76, 92 et 116.

2. Prise de décisions automatisée avec effet juridique ou effet similaire significatif: traitement ayant pour finalité la prise de décisions à l'égard des personnes concernées produisant «*des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire*» [article 35, paragraphe 3, point a)]. Le traitement pourrait, par exemple, entraîner l'exclusion ou une discrimination. Les traitements n'ayant que peu ou pas d'effet sur les personnes ne répondent pas à ce critère particulier. Des explications complémentaires concernant ces notions seront fournies dans les prochaines lignes directrices du GT29 relatives au profilage.
3. Surveillance systématique: traitement utilisé pour observer, surveiller ou contrôler les personnes concernées, y compris la collecte de données via des réseaux ou par «*la surveillance systématique [...] d'une zone accessible au public*» [article 35, paragraphe 3, point c)][15]. Ce type de surveillance est un critère étant donné que la collecte des données à caractère personnel est susceptible d'intervenir dans des circonstances telles que les personnes concernées ne savent pas qui collecte leurs données et de quelle façon elles seront utilisées. En outre, il peut être impossible pour les personnes de se soustraire à un tel traitement dans l'espace public (ou accessible au public) considéré.
4. Données sensibles ou données à caractère hautement personnel: il s'agit de catégories particulières de données à caractère personnel visées à l'article 9 (informations concernant les opinions politiques des personnes, par exemple) ainsi que des données à caractère personnel relatives aux condamnations pénales ou aux infractions visées à l'article 10. À titre d'exemple, citons les dossiers médicaux que peut conserver un hôpital général ou encore les informations sur des auteurs d'infractions que peut détenir un enquêteur privé. Au-delà des dispositions du RGPD, certaines catégories de données peuvent être considérées comme augmentant le risque possible pour les droits et libertés des personnes. Ces données à caractère personnel sont considérées comme sensibles (au sens commun du terme) dans la mesure où elles sont liées à des activités domestiques et privées (communications électroniques dont la confidentialité doit être protégée, par exemple), dans la mesure où elles ont un impact sur l'exercice d'un droit fondamental (données de localisation dont la collecte met en cause la liberté de circulation, par exemple) ou dans la mesure où leur violation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple). À cet égard, il peut être pertinent de déterminer si les données ont déjà été rendues publiques par la personne concernée ou par des tiers. Le fait que les données à caractère personnel soient publiquement disponibles peut être pris en compte en tant que facteur dans l'analyse lorsqu'il est prévu une utilisation ultérieure des données pour certaines finalités. Ce critère peut également inclure les données telles que les documents personnels, les courriers électroniques, les agendas, les notes des liseuses équipées

[15] Pour le GT29, s'entend comme «*systématique*» toute surveillance qui remplit un ou plusieurs des critères suivants (voir les lignes directrices 16/EN WP 243 du GT29 relatives aux délégués à la protection des données):
- se déroule selon un système;
- préparée, organisée ou méthodique;
- se déroule dans le cadre d'un plan général de collecte de données;
- réalisée dans le cadre d'une stratégie.

Pour le GT29, s'entend comme une «*zone accessible au public*» tout lieu, quel qu'il soit, ouvert à tout un chacun, tel qu'une place, un centre commercial, une rue, un marché, une gare ou encore une bibliothèque publique, par exemple.

de fonctions de prise de notes ainsi que les informations à caractère très personnel contenues dans les applications de «life-logging».

5. Données traitées à grande échelle: le RGPD ne précise pas ce qu'il faut entendre par «grande échelle», même si le considérant 91 fournit quelques indications à ce sujet. Quoi qu'il en soit, pour déterminer si le traitement est effectué à grande échelle, le GT29 recommande de prendre en compte, en particulier, les facteurs suivants:[16]
    a. le nombre de personnes concernées, soit en valeur absolue, soit en proportion de la population considérée;
    b. le volume de données et/ou l'éventail des différents éléments de données traitées;
    c. la durée ou la permanence de l'activité de traitement de données;
    d. l'étendue géographique de l'activité de traitement.
6. Croisement ou combinaison d'ensembles de données, par exemple issus de deux opérations de traitement de données, ou plus, effectuées à des fins différentes et/ou par différents responsables du traitement, d'une manière qui outrepasserait les attentes raisonnables de la personne concernée[17].
7. Données concernant des personnes vulnérables (considérant 75): le traitement de ce type de données est un critère en raison du déséquilibre des pouvoirs accru qui existe entre les personnes concernées et le responsable du traitement, ce qui signifie que les premières peuvent se trouver dans l'incapacité de consentir, ou de s'opposer, aisément au traitement de leurs données ou d'exercer leurs droits. Peuvent être considérés comme des personnes concernées vulnérables, les enfants (qui peuvent être vus comme incapables de s'opposer ou de consentir sciemment et de manière réfléchie au traitement de leurs données), les employés, les segments les plus vulnérables de la population nécessitant une protection particulière (personnes souffrant de maladie mentale, demandeurs d'asile et personnes âgées, patients, etc.) et, en tout état de cause, toutes autres personnes pour lesquelles un déséquilibre dans la relation avec le responsable du traitement peut être identifié.
8. Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles: utilisation combinée, par exemple, de systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale pour améliorer le contrôle des accès physiques, etc. Le RGPD indique clairement (article 35, paragraphe 1, et considérants 89 et 91) que l'utilisation d'une nouvelle technologie, définie en «*conformité avec l'état des connaissances technologiques*» (considérant 91), peut déclencher la nécessité d'une AIPD, et ce en raison du fait que l'utilisation de la technologie en question peut impliquer de nouvelles formes de collecte et d'utilisation des données, présentant potentiellement un risque élevé pour les droits et libertés des personnes. En effet, les conséquences personnelles et sociales du déploiement d'une nouvelle technologie peuvent être inconnues, et une AIPD aidera le responsable du traitement à comprendre et à traiter de tels risques. Par exemple, certaines applications de «l'internet des objets» sont susceptibles d'avoir un impact important sur la vie quotidienne et la vie privée des personnes, et nécessitent par conséquent une AIPD.
9. Traitements en eux-mêmes qui *«empêchent [les personnes concernées] d'exercer un droit ou de bénéficier d'un service ou d'un contrat»* (article 22 et considérant 91). Ces traitements incluent notamment les opérations visant à autoriser, modifier ou refuser l'accès à un service ou la conclusion d'un contrat. À titre d'exemple, prenons le cas d'une banque passant ses

[16] Voir les lignes directrices 16/EN WP 243 du GT29 relatives aux délégués à la protection des données.
[17] Voir l'explication fournie dans l'avis 13/EN WP 203 du GT29 relatif à la limitation des finalités, p. 24.

clients au crible d'une base de données de cote de crédit avant d'arrêter ses décisions d'octroi de prêt.

Dans la plupart des cas, le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une AIPD. D'une manière générale, le GT29 estime que plus le traitement remplit de critères, plus il est susceptible de présenter un risque élevé pour les droits et libertés des personnes concernées et par conséquent de nécessiter une AIPD, quelles que soient les mesures que le responsable du traitement envisage d'adopter.

Néanmoins, dans certains cas, **le responsable du traitement peut considérer que même si son traitement ne satisfait qu'à un seul de ces critères, il requiert malgré tout une AIPD.**

Les exemples qui suivent illustrent la façon dont il convient d'utiliser les critères pour déterminer si une opération de traitement considérée nécessite une AIPD.

Exemples d'opérations de traitement	**Critères potentiellement pertinents**	**AIPD potentiellement requise?**
Traitement par un hôpital des données génétiques et des données de santé de ses patients (système d'information hospitalier).	- Données sensibles ou données à caractère hautement personnel. - Données concernant des personnes vulnérables. - Données traitées à grande échelle.	Oui
Utilisation d'un système de caméras pour surveiller les comportements routiers. Le responsable du traitement envisage d'utiliser un système d'analyse vidéo intelligente pour isoler les véhicules et reconnaître automatiquement les plaques d'immatriculation.	- Surveillance systématique. - Utilisation innovante ou application de solutions technologiques ou organisationnelles.	
Surveillance systématique par une entreprise des activités de ses employés, y compris leur poste de travail, leur activité sur internet, etc.	- Surveillance systématique. - Données concernant des personnes vulnérables.	
Collecte de données sur les réseaux sociaux publics dans le but de générer des profils.	- Évaluation ou notation. - Données traitées à grande échelle. - Croisement ou combinaison d'ensembles de données. - Données sensibles ou données à caractère hautement personnel.	
Création par une institution d'une base de données spécialisée dans la notation de crédit ou «antifraude» au niveau national.	- Évaluation ou notation. - Prise de décisions automatisée avec effet juridique ou effet similaire significatif. - Empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat. - Données sensibles ou données à caractère hautement personnel.	
Stockage à des fins d'archivage de données à	- Données sensibles.	

13

Exemples d'opérations de traitement	Critères potentiellement pertinents	AIPD potentiellement requise?
caractère personnel sensibles, pseudonymisées, concernant des personnes vulnérables participant à des projets de recherche ou à des essais cliniques.	- Données concernant des personnes vulnérables. - Empêche les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat.	
Traitement de «données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel» (considérant 91).	- Données sensibles ou données à caractère hautement personnel. - Données concernant des personnes vulnérables.	Non
Utilisation par un magazine en ligne d'une liste de diffusion pour communiquer à ses abonnés son digest générique quotidien.	- Données traitées à grande échelle.	
Diffusion par un site de commerce électronique de publicités pour des pièces automobiles anciennes impliquant un profilage limité, basé sur les articles visualisés ou achetés sur le site internet.	- Évaluation ou notation.	

À l'inverse, une opération de traitement peut correspondre à l'un des cas susmentionnés et être néanmoins considérée par le responsable du traitement comme non «susceptible d'engendrer un risque élevé». Dans pareil cas, il convient que le responsable du traitement explique et documente les motifs de sa décision de ne pas procéder à une AIPD en incluant/rapportant par ailleurs l'opinion à cet égard du délégué à la protection des données.

De plus, dans le cadre du principe de responsabilité, il est prévu que les responsables du traitement «*tiennent un registre des activités de traitement effectuées sous leur responsabilité*», lequel doit consigner un certain nombre d'informations, dont les finalités du traitement, une description des catégories de données concernées et des destinataires des données et «*dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1*» (article 30, paragraphe 1), et chacun d'eux a l'obligation d'évaluer la probabilité d'un risque élevé, y compris s'il décide finalement de ne pas effectuer d'AIPD.

Remarque: les autorités de contrôle sont tenues d'établir, de publier et de communiquer au Comité européen de la protection des données (CEPD) une liste des opérations de traitement nécessitant une AIPD (article 35, paragraphe 4)[18]. Les critères susmentionnés peuvent aider les autorités de contrôle à constituer une telle liste, à laquelle d'autres éléments spécifiques pourront être intégrés en temps voulu, le cas échéant. Par exemple, le traitement de tout type de données biométriques ainsi que celui

[18] Dans ce contexte, «*l'autorité de contrôle compétente applique le mécanisme de contrôle de la cohérence visé à l'article 63, lorsque ces listes comprennent des activités de traitement liées à l'offre de biens ou de services à des personnes concernées ou au suivi de leur comportement dans plusieurs États membres, ou peuvent affecter sensiblement la libre circulation des données à caractère personnel au sein de l'Union*» (article 35, paragraphe 6).

des données des enfants pourraient également être considérés comme pertinents aux fins de l'établissement de la liste visée à l'article 35, paragraphe 4.

b) Quand une AIPD n'est-elle pas nécessaire? Lorsque le traitement n'est pas *«susceptible d'engendrer un risque élevé»* ou qu'une AIPD similaire existe déjà ou que le traitement a été autorisé avant mai 2018 ou qu'il a une base juridique ou encore qu'il figure dans la liste des opérations de traitement qui ne requièrent pas d'AIPD.

Le GT29 considère qu'une AIPD n'est pas nécessaire dans les cas suivants:

- **lorsque le traitement n'est pas «*susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*»** (article 35, paragraphe 1);
- **lorsque le traitement est très similaire en termes de nature, de portée, de contexte et de finalités à un autre traitement qui a fait l'objet d'une AIPD.** Dans un tel cas, les résultats de l'AIPD réalisée pour le traitement similaire peuvent être utilisés (article 35, paragraphe 1[19]);
- lorsque le traitement a fait l'objet d'un examen mené par une autorité de contrôle avant mai 2018 dans des conditions spécifiques qui n'ont pas changé[20] (voir III, C);
- **lorsque le traitement,** effectué en application de l'article 6, paragraphe 1, point c) ou e), **a une base juridique** dans le droit de l'Union ou dans le droit de l'État membre, que ce droit règlemente l'opération de traitement spécifique **et qu'une AIPD a déjà été réalisée** dans le cadre de l'établissement de la base juridique en question (article 35, paragraphe 10)[21], à moins qu'un État membre n'estime qu'il est nécessaire de procéder à une telle analyse avant les activités de traitement;
- **lorsque le traitement figure dans la liste facultative (établie par l'autorité de contrôle) des opérations de traitement** qui ne requièrent pas d'AIPD (article 35, paragraphe 5). Cette liste peut recenser les activités de traitement conformes aux conditions fixées par l'autorité en question, en particulier par l'intermédiaire de lignes directrices, de décisions ou autorisations spécifiques, de règles de conformité, etc. (par ex. en France, autorisations, dispenses, règles simplifiées, packs de conformité...). Dans pareil cas et sous réserve d'une réévaluation par l'autorité de contrôle compétente, il n'est pas nécessaire d'effectuer une AIPD, à la condition exclusive, toutefois, que le traitement relève strictement du champ d'application de la procédure pertinente indiquée dans la liste et continue de satisfaire pleinement à toutes les exigences applicables du RGPD.

C. Et qu'en est-il des opérations de traitement déjà existantes? Une AIPD est nécessaire dans certains cas.

[19] «*Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires*».

[20] «*Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées*» (considérant 171).

[21] Dans le cas d'une AIPD réalisée au stade de l'élaboration de la législation conférant une base juridique au traitement, un réexamen pourra être nécessaire avant le lancement des opérations, la législation adoptée étant susceptible de différer de la proposition d'une manière affectant les questions liées à la protection de la vie privée et à la protection des données. En outre, il est possible que les détails techniques disponibles en ce qui concerne le traitement effectif soient insuffisants au moment de l'adoption de la législation, même si une AIPD a été effectuée. Dans de tels cas, il pourra s'avérer nécessaire d'effectuer une AIPD spécifique avant d'exécuter les activités de traitement proprement dites.

L'obligation d'effectuer une AIPD s'applique aux opérations de traitement existantes susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques et pour lesquelles les risques associés ont évolué, compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Aucune AIPD n'est nécessaire pour les opérations de traitement qui ont fait l'objet d'un examen par une autorité de contrôle ou par le détaché à la protection des données, conformément à l'article 20 de la directive 95/46/CE, et dont la mise en œuvre n'a pas changé depuis le contrôle préalable. En effet, «*Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées*» (considérant 171).

À l'inverse, ceci signifie que tout traitement de données dont les conditions de mise en œuvre (portée, finalités, données à caractère personnel collectées, identité des responsables du traitement ou des destinataires des données, durée de conservation des données, mesures techniques et organisationnelles, etc.) ont changé depuis l'examen préalable effectué par l'autorité de contrôle ou le détaché à la protection des données et sont susceptibles d'engendrer un risque élevé doit faire l'objet d'une AIPD.

De plus, une AIPD peut être nécessaire à la suite d'une évolution des risques découlant des opérations de traitement[22], par exemple en raison du recours à une nouvelle technologie ou de l'utilisation des données à caractère personnel à des fins différentes. Les opérations de traitement peuvent évoluer rapidement et de nouvelles vulnérabilités peuvent apparaître. Par conséquent, il convient de noter que la révision d'une AIPD est non seulement utile dans un souci d'amélioration continue, mais également essentielle pour maintenir le niveau de protection des données dans un environnement qui change au fil du temps. Une AIPD peut également devenir nécessaire du fait d'une évolution du contexte organisationnel ou sociétal de l'activité de traitement, par exemple s'il s'avère que les effets de certaines décisions automatisées se sont accrus ou que de nouvelles catégories de personnes concernées apparaissent vulnérables à la discrimination. Dans chacun de ces exemples, le facteur en cause peut entraîner une évolution des risques découlant de l'activité de traitement concernée.

Inversement, certaines évolutions peuvent aussi réduire les risques. Prenons par exemple le cas d'une opération de traitement ayant évolué de telle sorte que les prises de décisions ne sont plus automatisées ou celui d'une activité de surveillance ayant perdu son caractère systématique. Dans ce cas, le réexamen des risques peut montrer qu'une AIPD n'est plus nécessaire.

À titre de bonne pratique, **une AIPD devrait faire l'objet d'un examen continu et être régulièrement réévaluée.** Par conséquent, même si une AIPD ne s'avère pas nécessaire le 25 mai 2018, il conviendra, le moment venu, que le responsable du traitement procède à une telle AIPD dans le cadre de ses obligations générales de responsabilité.

D. Comment effectuer une AIPD?

a) Quand convient-il d'effectuer une AIPD? Préalablement au lancement du traitement.

[22] Eu égard aux différents aspects suivants: contexte, données collectées, finalités, fonctionnalités, données à caractère personnel traitées, destinataires, combinaisons de données, risques (actifs de soutien, sources de risques, impacts potentiels, menaces, etc.), mesures de sécurité et transferts internationaux.

L'AIPD doit être effectuée «*avant le traitement*» (article 35, paragraphes 1 et 10, considérants 90 et 93)[23]. Cette exigence est cohérente avec les principes de protection des données dès la conception et de protection des données par défaut (article 25 et considérant 78). L'AIPD doit être considérée comme un outil d'aide à la prise de décisions en ce qui concerne le traitement.

L'AIPD doit être lancée le plus tôt possible dans le cycle de conception du traitement, même si certaines opérations de traitement sont encore inconnues. La mise à jour de l'AIPD tout au long du projet assurera la prise en compte des questions liées à la protection des données et de la vie privée et encouragera la création de solutions favorisant la conformité. Il peut également être nécessaire de répéter les différentes étapes de l'évaluation au fur et à mesure de l'avancée du processus de développement étant donné que le choix de certaines mesures techniques ou organisationnelles peut modifier la gravité ou la probabilité des risques associés au traitement.

Le fait que l'AIPD puisse devoir être actualisée après le lancement effectif du traitement n'est pas une raison valable pour la différer ou pour ne pas l'effectuer. Une telle analyse est un processus continu, en particulier lorsque l'opération de traitement est dynamique et soumise à de constants changements. **La réalisation d'une AIPD relève d'un processus continu et n'est pas un exercice ponctuel**.

b) Qui est tenu d'effectuer l'AIPD? Le responsable du traitement, avec le DPD et les sous-traitants.

La responsabilité de veiller à ce qu'une AIPD soit effectuée incombe au responsable du traitement (article 35, paragraphe 2). L'AIPD peut être réalisée par quelqu'un d'autre, à l'intérieur ou à l'extérieur de l'organisation, mais le responsable du traitement reste responsable en dernier ressort de cette tâche.

Le responsable du traitement est également tenu de prendre conseil auprès du délégué à la protection des données (DPD), si un tel délégué a été désigné (article 35, paragraphe 2), et il convient que l'AIPD documente les conseils ainsi recueillis ainsi que les décisions prises par le responsable du traitement. Le DPD a également pour mission de vérifier l'exécution de l'AIPD [article 39, paragraphe 1, point c)]. Des précisions complémentaires sont fournies dans les lignes directrices 16/EN WP 243 du GT29 relatives aux délégués à la protection des données.

Si le traitement est entièrement ou partiellement effectué par un sous-traitant, **ce dernier doit aider le responsable du traitement à effectuer l'AIPD** et fournir toutes les informations nécessaires [en application de l'article 28, paragraphe 3, point f)].

Le responsable du traitement «*demande l'avis des personnes concernées ou de leurs représentants*» (article 35, paragraphe 9), «*le cas échéant*». Le GT29 considère que:

- ces avis peuvent être recueillis par divers moyens, selon le contexte (par ex. une étude générique en lien avec les finalités et les moyens de l'opération de traitement, un questionnaire soumis aux représentants du personnel, ou des enquêtes de type habituel envoyées aux futurs clients du responsable du traitement), le responsable du traitement devant s'assurer de s'appuyer sur une base juridique pour le traitement de toutes données à caractère personnel

[23] À moins qu'il s'agisse d'un traitement déjà existant ayant préalablement fait l'objet d'un examen par l'autorité de contrôle, auquel cas l'AIPD sera effectuée avant toute mise en œuvre de modifications significatives.

impliquées dans cette collecte d'avis. Il convient toutefois de noter que demander le consentement au traitement n'est évidemment pas un moyen de recueillir l'avis des personnes concernées;

- si la décision finale du responsable du traitement diffère de l'avis des personnes concernées, il y a lieu qu'il documente les raisons de sa décision de persévérer ou non;
- le responsable du traitement doit également justifier toute décision de ne pas recueillir l'avis des personnes concernées s'il juge la démarche inappropriée, en estimant par exemple que cela compromettrait la confidentialité de plans d'affaires ou serait disproportionné ou irréalisable.

Enfin, il est de bonne pratique de définir et de documenter les autres rôles et responsabilités spécifiques, en fonction de la politique interne et des processus et règles en jeu; par exemple:

- en cas de proposition faite par une unité opérationnelle spécifique de procéder à une AIPD, l'unité en question devrait ensuite contribuer à l'AIPD et devrait être impliquée dans le processus de validation de l'analyse;
- le cas échéant, il est recommandé de recueillir les conseils d'experts indépendants de différentes professions[24] (avocats, experts en informatique, experts en sécurité, sociologues, experts en déontologie, etc.);
- les rôles et responsabilités de tout sous-traitant doivent être définis contractuellement, et l'AIPD doit être effectuée avec son aide, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant (article 28, paragraphe 3, point f)];
- le responsable de la sécurité des systèmes d'information (RSSI), si un tel responsable a été désigné, ainsi que le DPD, peuvent être amenés à suggérer au responsable du traitement d'effectuer une AIPD sur une opération de traitement spécifique et devraient dès lors apporter leur appui aux parties prenantes en ce qui concerne la méthodologie à suivre, participer à l'évaluation de la qualité de l'analyse des risques et de l'acceptabilité des risques résiduels, et contribuer au développement des connaissances spécifiques au contexte du responsable du traitement;
- le responsable de la sécurité des systèmes d'information (RSSI), si un tel responsable a été désigné, et/ou le service informatique, devraient apporter leur assistance au responsable du traitement et peuvent être amenés à proposer la réalisation d'une AIPD sur une opération de traitement spécifique, en fonction des besoins en matière de sécurité ou des besoins opérationnels.

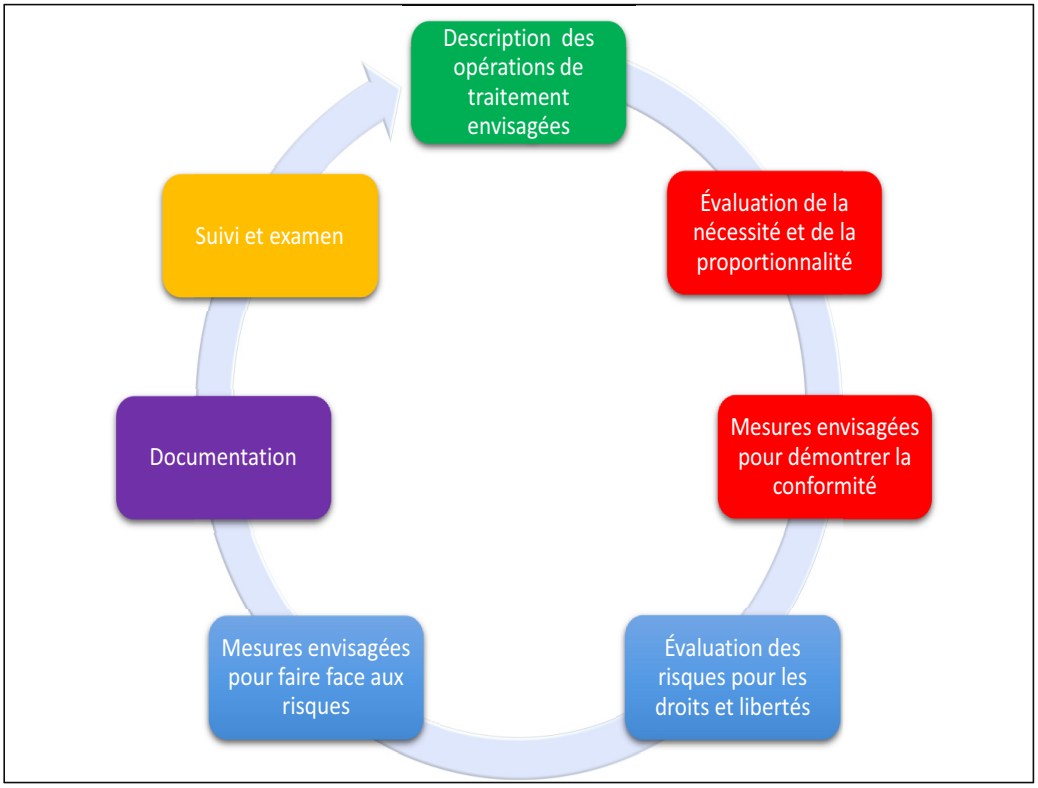
c) Quelle est la méthodologie à suivre pour effectuer une AIPD? Différentes méthodologies mais des critères communs.

[24] *Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Le RGPD dispose qu'une AIPD (article 35, paragraphe 7, et considérants 84 et 90) doit au moins contenir:

- «*une description systématique des opérations de traitement envisagées et des finalités du traitement*»;
- «*une évaluation de la nécessité et de la proportionnalité des opérations de traitement*»;
- «*une évaluation des risques pour les droits et libertés des personnes concernées*»;
- «*les mesures envisagées pour:*
  - «*faire face aux risques*»;
  - «*apporter la preuve du respect [du] règlement*».

Le schéma suivant illustre le processus itératif générique suggéré pour la réalisation d'une AIPD[25]:



Le respect d'un code de conduite (article 40) doit être pris en compte (article 35, paragraphe 8) lors de l'évaluation de l'impact d'une opération de traitement de données. Ceci peut être utile pour démontrer que des mesures adéquates ont été choisies ou mises en place, à condition toutefois que le code de conduite soit approprié pour l'opération de traitement considérée. Il convient également de prendre en

[25] Il convient de souligner que le processus décrit ici est itératif: dans la pratique, chacune des étapes devra probablement être réexaminée plusieurs fois avant que l'AIPD ne puisse être finalisée.

compte les garanties que représentent les certifications, labels et marques destinés à démontrer la conformité au RGPD des opérations de traitement effectuées par les responsables du traitement et les sous-traitants (article 42) ainsi que l'application de règles d'entreprise contraignantes (REC).

Toutes les exigences pertinentes établies dans le RGPD fournissent un cadre général et générique pour la conception et la réalisation d'une AIPD. La mise en œuvre pratique de l'AIPD sera dès lors fonction des exigences du RGPD pouvant être complétées par des indications pratiques plus détaillées. La mise en œuvre d'une AIPD est donc en ce sens adaptable. Cela signifie que même un responsable du traitement opérant sur de petites quantités de données peut concevoir et mettre en œuvre une AIPD adaptée à ses opérations de traitement.

Le considérant 90 du RGPD mentionne un certain nombre d'éléments d'une AIPD qui recouvrent des composantes bien définies de la gestion des risques (par ex. dans la norme ISO 31000[26]). En termes de gestion des risques, une AIPD a pour objectif d'aider à «gérer les risques» pour les droits et libertés des personnes physiques en:

- établissant le contexte: «*compte tenu de la nature, de la portée, du contexte et des finalités du traitement et des sources du risque*»;
- appréciant le risque: «*évaluer la probabilité et la gravité particulières du risque élevé*»;
- traitant le risque: «*atténuer ce risque*» et «*assurer la protection des données à caractère personnel*», et «*démontrer le respect du présent règlement*».

Remarque: l'AIPD au sens du RGPD est un outil de gestion des risques pour les droits des personnes concernées et se place ainsi sous l'angle de leurs droits, comme c'est également le cas dans certains autres domaines tels que la sécurité sociétale, par exemple. À l'inverse, dans d'autres domaines encore (par ex. la sécurité de l'information), la gestion des risques est axée sur l'organisation.

La souplesse offerte par le RGPD permet au responsable du traitement de déterminer la structure et la forme précises de l'AIPD afin qu'elles soient adaptées aux pratiques de travail existantes. Il existe un certain nombre de processus établis au sein de l'UE et dans le monde qui tiennent compte des éléments décrits au considérant 90. Cependant, quelle que soit sa forme, une AIPD se doit d'être une véritable évaluation des risques, permettant au responsable du traitement de prendre des mesures pour y faire face.

Différentes méthodologies (voir l'annexe 1 pour des exemples de méthodologies d'analyse d'impact sur la protection des données et la vie privée) peuvent être utilisées pour faciliter la mise en œuvre des exigences de base énoncées dans le RGPD. Afin de permettre le développement de ces différentes approches, tout en aidant les responsables du traitement à respecter les dispositions du RGPD, des critères communs ont été identifiés (voir l'annexe 2). Ces derniers clarifient les exigences de base du règlement, mais offrent suffisamment de marge de manœuvre pour autoriser différentes formes de mise en œuvre. Ces critères peuvent être utilisés pour démontrer qu'une méthodologie d'AIPD considérée satisfait aux normes établies par le RGPD. **Il appartient au responsable du traitement de choisir une méthodologie, mais cette méthodologie doit satisfaire aux critères visés à l'annexe 2.**

[26] Processus de gestion des risques: communication et consultation, établissement du contexte, appréciation du risque, traitement du risque, suivi et évaluation (voir la section Termes et définitions et la table des matières dans l'aperçu de la norme ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

Le GT29 encourage le développement de cadres sectoriels pour les AIPD qui, dans la mesure où ils se fondent sur des connaissances sectorielles spécifiques, permettent dès lors à l'AIPD de prendre en compte les spécificités d'un type particulier d'opération de traitement (par ex.: types particuliers de données, d'actifs d'entreprise, d'impacts potentiels, de menaces, de mesures). L'AIPD est ainsi en mesure de traiter les problèmes qui se posent dans un secteur économique donné, ou lors de l'utilisation de technologies particulières ou encore de l'exécution de types particuliers d'opérations de traitement.

Enfin, si nécessaire, «*le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement*» (article 35, paragraphe 11[27]).

d) Est-il obligatoire de publier l'AIPD? Non, mais la publication d'un résumé peut être de nature à susciter la confiance, et l'AIPD complète doit être communiquée à l'autorité de contrôle en cas de consultation préalable ou sur demande de l'APD.

Le RGPD ne fait pas obligation de publier l'AIPD, et il relève de la discrétion du responsable du traitement de la publier ou non. Cependant, une publication au moins partielle, sous la forme d'un résumé ou d'une conclusion de son AIPD, devrait être envisagée par le responsable du traitement.

Une telle pratique serait utile pour susciter la confiance dans les opérations de traitement du responsable du traitement et pour donner des gages de responsabilité et de transparence. Il est notamment de bonne pratique de publier une AIPD lorsque des citoyens sont affectés par l'opération de traitement. Tel peut en particulier être le cas lorsqu'une autorité publique réalise une AIPD.

L'AIPD publiée n'a pas besoin d'inclure l'intégralité de l'analyse, notamment lorsque celle-ci pourrait donner des informations spécifiques relatives à des risques en matière de sécurité concernant le responsable du traitement ou divulguer des secrets d'affaires ou des informations commercialement sensibles. Dans pareille situation, la version publiée peut consister simplement en un résumé des principales constatations de l'AIPD, ou même uniquement en une déclaration selon laquelle une AIPD a été effectuée.

De plus, lorsqu'une AIPD révèle des risques résiduels élevés, le responsable du traitement est tenu de se tourner vers l'autorité de contrôle pour une consultation préalable concernant le traitement (article 36, paragraphe 1). Dans le cadre cette dernière, l'AIPD doit être communiquée dans son intégralité [article 36, paragraphe 3, point e)]. L'autorité de contrôle peut fournir un avis[28], et veillera à protéger le secret des affaires et à ne pas divulguer de vulnérabilités dans la sécurité, sous réserve des principes applicables dans chaque État membre en matière d'accès du public aux documents officiels.

E. Quand convient-il de consulter l'autorité de contrôle? En présence de risques résiduels élevés.

[27] Seule l'application des paragraphes 1 à 7 de l'article 35 est explicitement exclue par l'article 35, paragraphe 10.

[28] La communication d'un avis écrit au responsable du traitement n'est nécessaire que si l'autorité de contrôle juge que le traitement envisagé ne respecte pas les dispositions du règlement, conformément à l'article 36, paragraphe 2.

Comme expliqué précédemment:

- une AIPD est requise lorsque le traitement «*est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques*» [article 35, paragraphe 1; voir III, B, a)]. À titre d'exemple, le traitement de données de santé à grande échelle est considéré comme susceptible d'engendrer un risque élevé et nécessite une AIPD;
- dès lors, il appartient au responsable du traitement d'évaluer les risques pour les droits et libertés des personnes concernées et d'identifier les mesures[29] envisagées pour réduire ces risques à un niveau acceptable et apporter la preuve du respect du RGPD [article 35, paragraphe 7; voir III, C, c)]. Par exemple, dans un cas de stockage de données à caractère personnel sur ordinateurs portables, l'application de mesures de sécurité techniques et organisationnelles appropriées (chiffrement efficace et complet des disques, gestion des clés rigoureuse, contrôle approprié des accès, sauvegardes sécurisées, etc.) en plus des règles existantes (avis, consentement, droit d'accès, droit d'opposition, etc.).

Dans l'exemple des ordinateurs portables ci-dessus, à condition que les risques aient été jugés suffisamment réduits par le responsable du traitement et après prise en compte de l'article 36, paragraphe 1, et des considérants 84 et 94, le traitement pourrait être mis en œuvre sans consultation de l'autorité de contrôle. Ce n'est que lorsque les risques identifiés ne peuvent pas être suffisamment réduits par le responsable du traitement (à savoir en présence de risques résiduels élevés) que ce dernier est tenu de consulter l'autorité de contrôle.

Un risque résiduel peut notamment être considéré comme élevé et inacceptable dès lors qu'il exposerait les personnes à des conséquences importantes, voire irréversibles, qu'elles seraient susceptibles de ne pas pouvoir surmonter (par ex:. un accès illégitime à leurs données qui pourrait menacer leur vie, entraîner une mise à pied, mettre en péril leur situation financière) et/ou lorsqu'il semble évident que le risque se concrétisera (par ex.: dans la mesure où il n'est pas possible de réduire le nombre de personnes accédant aux données en raison de leurs modes de partage, d'utilisation ou de distribution, ou en présence d'une vulnérabilité bien connue non corrigée).

Lorsque le responsable du traitement ne parvient pas à identifier des mesures suffisantes pour réduire les risques à un niveau acceptable (à savoir que les risques résiduels demeurent élevés), une consultation de l'autorité de contrôle est obligatoire[30].

En outre, l'autorité de contrôle devra être consultée dans tous les cas où le droit de l'État membre exige que les responsables du traitement consultent l'autorité de contrôle et/ou obtiennent son autorisation préalable en ce qui concerne un traitement que le responsable du traitement envisage dans le cadre d'une mission d'intérêt public dont il est investi, notamment pour les traitements en rapport avec la protection sociale et la santé publique (article 36, paragraphe 5).

[29] En tenant également compte des orientations existantes du CEPD et des autorités de contrôle, ainsi que des possibilités techniques les plus récentes et des coûts de mise en œuvre, comme prévu à l'article 35, paragraphe 1.

[30] Remarque: «*la pseudonymisation et le chiffrement des données à caractère personnel*» (tout comme la minimisation des données, les mécanismes de contrôle, etc.) ne sont pas nécessairement des mesures appropriées. Il ne s'agit là que d'exemples. Les mesures appropriées dépendent du contexte et des risques spécifiques aux opérations de traitement.

Il convient toutefois de noter que, indépendamment de la nécessité ou non de consulter l'autorité de contrôle en fonction du niveau du risque résiduel, les obligations de conserver un rapport de l'AIPD et de mettre celle-ci à jour en temps utile demeurent.

IV. Conclusions et recommandations

Les AIPD sont un outil utile pour les responsables du traitement aux fins de l'établissement de systèmes de traitement de données répondant aux exigences du RGPD et peuvent être obligatoires pour certains types d'opérations de traitement. Leur mise en œuvre est adaptable et elles peuvent prendre différentes formes, même si le RGPD fixe les conditions de base à remplir pour une AIPD effective. La réalisation d'une AIPD devrait être considérée par les responsables du traitement comme une activité utile et positive aidant à se conformer à la législation.

L'article 24, paragraphe 1, définit comme suit la responsabilité fondamentale du responsable du traitement aux fins du respect du RGPD: «*Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire*».

L'AIPD est un élément essentiel de la mise en conformité avec le règlement lorsqu'un traitement de données à risque élevé est prévu ou déjà effectué. Il convient par conséquent que les responsables du traitement utilisent les critères définis dans le présent document pour déterminer si une AIPD est ou non nécessaire. Dans sa politique interne, le responsable du traitement peut étendre cette liste au-delà des obligations légales fixées par le RGPD, ce qui pourra lui attirer une confiance accrue de la part des personnes concernées et des autres responsables du traitement.

Lorsqu'un traitement à risque potentiellement élevé est prévu, le responsable du traitement doit:

- choisir une méthodologie d'AIPD (voir les exemples donnés à l'annexe 1) qui satisfait aux critères de l'annexe 2, ou spécifier et mettre en œuvre un processus d'AIPD systématique:
  - conforme aux critères de l'annexe 2;
  - intégré aux processus existants de conception, de développement, de modification, de gestion des risques et d'examen opérationnel, selon les processus, le contexte et la culture internes;
  - impliquant les parties intéressées et définissant clairement leurs responsabilités (responsable du traitement, DPD, personnes concernées ou leurs représentants, unités opérationnelles, services techniques, sous-traitants, responsable de la sécurité des systèmes d'information, etc.);
- communiquer son rapport d'AIPD à l'autorité de contrôle compétente si la demande lui en est faite;
- consulter l'autorité de contrôle s'il n'a pas réussi à identifier des mesures suffisantes pour atténuer les risques élevés;
- procéder à un réexamen périodique de l'AIPD et du traitement qu'elle évalue, au moins lorsqu'un changement intervient dans les risques présentés par le traitement;
- documenter les décisions prises.

Annexe 1 — Exemples de cadres européens existants pour la réalisation d'une AIPD

Le RGPD ne précise pas la procédure à suivre pour effectuer une AIPD et laisse le loisir aux responsables du traitement de recourir à un cadre qui complète leurs pratiques de travail existantes, sous réserve néanmoins que celui-ci prenne en compte les éléments décrits à l'article 35, paragraphe 7. Il peut s'agir d'un cadre sur mesure pour le responsable du traitement ou commun à un secteur particulier. Un certain nombre de cadres développés par les APD de l'UE ainsi que de cadres sectoriels européens ont été publiés, dont en particulier les suivants:

Exemples de cadres européens génériques:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: *Étude d'impacts sur la vie privée (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/etude-dimpacts-sur-la-vie-privee-suivez-la-methode-de-la-cnil
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Exemples de cadres européens sectoriels:

- Cadre relatif à l'analyse de l'impact sur la vie privée et la protection des données pour les applications RFID [32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure [33]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

[31] Unanimement et positivement adopté (avec l'abstention de la Bavière) par la 92e conférence des autorités indépendantes pour la protection des données du Bund et des Länder qui s'est tenue à Kühlungsborn les 9 et 10 novembre 2016.

[32] Voir aussi:

- la recommandation de la Commission du 12 mai 2009 sur la mise en œuvre des principes de respect de la vie privée et de protection des données dans les applications reposant sur l'identification par radiofréquence;
  http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32009H0387&from=FR
- l'avis 9/2011 sur la proposition révisée des entreprises relative au cadre d'évaluation de l'impact sur la protection des données et de la vie privée des applications reposant sur l'identification par radiofréquence (RFID).
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_fr.pdf

[33] Voir aussi l'avis 07/2013 sur le modèle d'analyse d'impact relative à la protection des données pour les réseaux intelligents et les systèmes de relevés intelligents (modèle d'AIPD) élaboré par le groupe d'experts 2 de la task-force sur les réseaux intelligents de la Commission. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_fr.pdf

Une norme internationale fournit également des lignes directrices concernant les méthodologies applicables pour la réalisation d'une AIPD (ISO/IEC 29134[34]).

[34] ISO/IEC 29134 (projet, indisponible en français), *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'évaluation d'impacts sur la vie privée*, Organisation internationale de normalisation (ISO).

25

Annexe 2 — Critères d'acceptabilité d'une AIPD

Les critères suivants proposés par le GT29 peuvent être utilisés par les responsables du traitement pour déterminer si une AIPD ou une méthodologie d'AIPD considérée est suffisamment complète aux fins du respect des exigences du RGPD:

- ☐ une description systématique du traitement est fournie [article 35, paragraphe 7, point a)]:
  - ☐ la nature, la portée, le contexte et les finalités du traitement sont pris en compte (considérant 90);
  - ☐ les données à caractère personnel concernées, les destinataires et la durée pendant laquelle les données à caractère personnel seront conservées sont précisés;
  - ☐ une description fonctionnelle de l'opération de traitement est fournie;
  - ☐ les actifs sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier) sont identifiés;
  - ☐ le respect de codes de conduite approuvés est pris en compte (article 35, paragraphe 8);
- ☐ la nécessité et la proportionnalité sont évaluées [article 35, paragraphe 7, point b)]:
  - ☐ les mesures envisagées pour assurer la conformité au règlement sont déterminées [article 35, paragraphe 7, point d), et considérant 90], avec prise en compte:
    - ☐ de mesures contribuant au respect des principes de proportionnalité et de nécessité du traitement, fondées sur les exigences suivantes:
      - ☐ finalités déterminées, explicites et légitimes (article 5, paragraphe 1, point b)];
      - ☐ licéité du traitement (article 6);
      - ☐ données adéquates, pertinentes et limitées à ce qui est nécessaire [article 5, paragraphe 1, point c)];
      - ☐ durée de conservation limitée [article 5, paragraphe 1, point e)];
    - ☐ de mesures contribuant aux droits des personnes concernées:
      - ☐ informations fournies à la personne concernée (articles 12, 13 et 14);
      - ☐ droit d'accès et droit à la portabilité des données (articles 15 et 20);
      - ☐ droit de rectification et droit à l'effacement (articles 16, 17 et 19);
      - ☐ droit d'opposition et droit à la limitation du traitement (articles 18, 19 et 21);
      - ☐ relations avec les sous-traitants (article 28);
      - ☐ garanties entourant le ou les transferts internationaux (chapitre V);
      - ☐ consultation préalable (article 36);
- ☐ les risques pour les droits et libertés des personnes concernées sont gérés [article 35, paragraphe 7, point c)]:
  - ☐ l'origine, la nature, la particularité et la gravité des risques sont évalués (considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime aux données, modification non désirée des données, disparition des données) du point de vue des personnes concernées:
    - ☐ les sources de risques sont prises en compte (considérant 90);
    - ☐ les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'événements tels qu'un accès illégitime aux données, une modification non désirée de celles-ci ou leur disparition.
    - ☐ les menaces qui pourraient conduire à un accès illégitime aux données, à une modification non désirée de celles-ci ou à leur disparition sont identifiées;
    - ☐ la probabilité et la gravité sont évaluées (considérant 90);
  - ☐ les mesures envisagées pour faire face à ces risques sont déterminées [article 35, paragraphe 7, point d), et considérant 90];
- ☐ les parties intéressées sont impliquées:
  - ☐ l'avis du DPD est recueilli (article 35, paragraphe 2);

☐ le point de vue des personnes concernées ou de leurs représentants est recueilli, le cas échéant (article 35, paragraphe 9).

27

Lignes directrices sur la notification des violation de données personnelles (WP250)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

18/FR

WP250rev.01

Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679

Adoptées le 3 octobre 2017

Version révisée et adoptée le 6 février 2018

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

TABLE DES MATIERES

INTRODUCTION

Le règlement général sur la protection des données (ci-après le «RGPD») introduit l'exigence que toute violation de données à caractère personnel (ci-après la «violation») soit notifiée à l'autorité de contrôle nationale compétente[1] (ou en cas de violation transfrontalière, à l'autorité chef de file) et, dans certains cas, communiquée aux personnes dont les données à caractère personnel ont été affectées par ladite violation.

L'obligation de notifier les violations existe déjà à l'heure actuelle pour certaines organisations, telles que les fournisseurs de services de communications électroniques accessibles au public [comme prévu par la directive 2009/136/CE et le règlement (CE) nº 611/2013][2]. Certains États membres disposent par ailleurs déjà de leur propre obligation de notification des violations. Il peut s'agir de l'obligation de notifier les violations impliquant certaines catégories de responsables du traitement autres que les fournisseurs de services de communications électroniques accessibles au public (par exemple, en Allemagne et en Italie), ou de l'obligation de notifier toutes les violations portant sur des données à caractère personnel (par exemple, aux Pays-Bas). D'autres États membres peuvent disposer de codes de bonne pratique pertinents (par exemple, en Irlande[3]). Cependant, si un certain nombre d'autorités européennes chargées de la protection des données encouragent actuellement les responsables du traitement à notifier les violations, la directive 95/46/CE sur la protection des données[4], que le RGPD remplace, ne contient pas d'obligation spécifique à cet égard. Une telle exigence sera donc nouvelle pour de nombreuses organisations. Le RGPD rend en effet cette notification obligatoire pour tous les responsables du traitement à moins qu'une violation soit peu susceptible d'engendrer un risque pour les droits et libertés des individus[5]. Les sous-traitants ont également un rôle important à jouer et doivent notifier toute violation au responsable du traitement[6].

Le groupe de travail «Article 29» (G29) considère que cette nouvelle exigence de notification présente plusieurs avantages. Lors de la notification à l'autorité de contrôle, les responsables du traitement peuvent notamment obtenir des conseils afin de savoir s'il convient d'informer les personnes concernées. En effet, l'autorité de contrôle peut ordonner au responsable du traitement d'informer lesdites personnes de la violation[7]. D'un autre côté, la communication d'une violation aux personnes concernées permet au responsable du traitement de leur fournir des informations sur les risques résultant de la violation et sur les mesures qu'elles peuvent prendre afin de se protéger des conséquences potentielles. Tout plan de réaction à une violation devrait viser à protéger les individus et leurs données à caractère personnel. Aussi la notification des violations devrait-elle être vue comme

[1] Voir article 4, paragraphe 21, du RGPD.

[2] Voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32009L0136 et http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32013R0611

[3] Voir https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] Voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:31995L0046

[5] Les droits consacrés par la Charte des droits fondamentaux de l'Union européenne, disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:12012P/TXT

[6] Voir article 33, paragraphe 2. Ce concept est similaire à celui de l'article 5 du règlement (UE) nº 611/2013, qui dispose qu'un fournisseur auquel il est fait appel pour fournir une partie d'un service de communications électroniques (sans qu'il soit directement lié par contrat avec les abonnés) est tenu d'informer le fournisseur qui l'a engagé en cas de violation de données à caractère personnel.

[7] Voir article 34, paragraphe 4, et article 58, paragraphe 2, point e).

un outil permettant de renforcer la conformité en matière de protection des données à caractère personnel. Parallèlement, il convient de noter que la non-communication d'une violation aux personnes concernées ou à l'autorité de contrôle pourrait entraîner une sanction pour le responsable du traitement en vertu de l'article 83.

Les responsables du traitement et les sous-traitants sont ainsi encouragés à prévoir à l'avance et à mettre en place des processus leur permettant de détecter et d'endiguer rapidement toute violation, d'évaluer les risques pour les personnes concernées[8] et de déterminer ensuite s'il est nécessaire d'informer l'autorité de contrôle compétente et de communiquer, si nécessaire, la violation aux personnes concernées. La notification à l'autorité de contrôle devrait faire partie intégrante de ce plan de réaction aux incidents.

Le RGPD contient des dispositions concernant les cas où une violation doit être notifiée, les personnes et entités auxquelles il convient de la notifier ainsi que les informations que devrait comprendre cette notification. Les informations requises pour une telle notification peuvent certes être communiquées de façon échelonnée, mais les responsables du traitement devraient réagir à toute violation dans des délais appropriés.

Dans son avis 03/2014 sur la notification des violations de données à caractère personnel[9], le G29 a fourni des orientations aux responsables du traitement afin de les aider à décider s'il convient d'informer les personnes concernées en cas de violation. L'avis portait sur l'obligation imposée aux fournisseurs de communications électroniques au titre de la directive 2002/58/CE, fournissait des exemples tirés de nombreux secteurs, dans le contexte du RGPD, encore à l'état de projet à l'époque, et présentait une série de bonnes pratiques à l'intention de tous les responsables du traitement.

Les présentes lignes directrices expliquent les obligations établies par le RGPD en matière de notification et de communication des violations ainsi que certaines des mesures que les responsables du traitement et les sous-traitants peuvent adopter en vue de respecter ces nouvelles obligations. Elles fournissent également des exemples de différents types de violations et des entités et personnes à informer dans différents cas de figure.

I. Notification d'une violation de données à caractère personnel en vertu du RGPD

A. Considérations de base concernant la sécurité

L'une des exigences du RGPD est que les données à caractère personnel soient traitées de façon à garantir un niveau de sécurité approprié desdites données, et notamment à les protéger contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées[10].

Le RGPD exige par conséquent des responsables du traitement et des sous-traitants qu'ils mettent en place des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pour les données à caractère personnel traitées. Ils devraient tenir compte de l'état

[8] Ceci peut se faire dans le cadre de l'exigence de suivi et d'examen de l'analyse d'impact relative à la protection des données (AIPD), requise pour les opérations de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques (article 35, paragraphes 1 et 11).

[9] Voir l'avis 03/2014 sur la notification des violations de données à caractère personnel http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_fr.pdf

[10] Article 5, paragraphe 1, point f), et article 32.

des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques[11]. Le RGPD exige également que toutes les mesures de protection techniques et organisationnelles appropriées soient mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite, ce qui déterminera si l'obligation de notification s'applique[12].

Aussi l'un des éléments clés de toute politique de sécurité des données est-il d'être en mesure de prévenir toute violation dans la mesure du possible et, lorsqu'une telle violation se produit malgré tout, d'y réagir dans les meilleurs délais.

B. Qu'est-ce qu'une violation de données à caractère personnel?

1. Définition

Avant de pouvoir remédier à une violation, le responsable du traitement doit être capable de la reconnaître. À son article 4, paragraphe 12, le RGPD définit une «violation de données à caractère personnel» comme:

> «une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données».

Ce que l'on entend par «destruction» de données à caractère personnel devrait être assez clair: il s'agit des cas où les données n'existent plus, ou n'existent plus sous une forme utile pour le responsable du traitement. «Dommage» devrait également être relativement clair: il s'agit des cas où les données à caractère personnel ont été altérées, corrompues ou ne sont plus complètes. Pour ce qui est de la «perte» de données à caractère personnel, cela signifie que les données pourraient toujours exister, mais que le responsable du traitement a perdu tout contrôle ou tout accès à ces données, ou encore qu'il ne les a plus en sa possession. Enfin, le traitement non autorisé ou illicite peut inclure la divulgation de données à caractère personnel à des destinataires (ou l'accès à de telles données par ceux-ci) n'étant pas autorisés à les recevoir (ou à y avoir accès), ou toute autre forme de traitement en infraction au RGPD.

Exemple

Il peut, par exemple, y avoir perte de données à caractère personnel lorsqu'un appareil contenant une copie de la base de données client d'un responsable du traitement est perdu ou volé. Un autre exemple de perte serait lorsque la copie unique d'un ensemble de données à caractère personnel a été cryptée par un rançongiciel, ou par le responsable du traitement à l'aide d'une clé qui n'est plus en sa possession.

Il convient avant tout de garder à l'esprit qu'une violation est une forme d'incident de sécurité. Toutefois, comme indiqué à l'article 4, paragraphe 12, le RGPD ne s'applique que lorsqu'il s'agit d'une violation de *données à caractère personnel*. Une telle violation aura pour conséquence que le responsable du traitement ne sera plus en mesure d'assurer la conformité avec les principes relatifs au traitement de données à caractère personnel tels que définis à l'article 5 du RGPD. Cette nuance met en lumière la différence entre un incident de sécurité et une violation de données à caractère

[11] Article 32; voir également considérant 83.

[12] Voir considérant 87.

personnel: si toutes les violations de données à caractère personnel constituent des incidents de sécurité, tous les incidents de sécurité ne constituent pas nécessairement des violations de données à caractère personnel[13].

Les éventuelles conséquences négatives d'une violation pour les personnes concernées sont envisagées ci-après.

2. Types de violations de données à caractère personnel

Dans son avis 03/2014 sur la notification des violations, le G29 expliquait que les violations pouvaient être classées selon trois principes de sécurité de l'information bien connus[14]:

- «violation de la confidentialité» – la divulgation ou l'accès non autorisés ou accidentels à des données à caractère personnel;
- «violation de l'intégrité» – l'altération non autorisée ou accidentelle de données à caractère personnel;
- «violation de la disponibilité» – la destruction ou la perte accidentelles ou non autorisées de l'accès[15] à des données à caractère personnel.

Il convient également de noter qu'en fonction des circonstances, une violation peut concerner à la fois la confidentialité, l'intégrité et la disponibilité de données à caractère personnel ou une combinaison de ces éléments.

S'il est relativement facile de déterminer si une violation de la confidentialité ou de l'intégrité s'est produite, il peut être moins évident de déterminer l'existence d'une violation de la disponibilité. Une violation sera toujours considérée comme une violation de la disponibilité en cas de perte ou de destruction permanente de données à caractère personnel.

Exemple

Il peut, par exemple, y avoir perte de disponibilité lorsque des données ont été supprimées, soit accidentellement, soit par une personne non autorisée, ou encore, dans le cas de données cryptées de façon sécurisée, lorsque la clé de décryptage a été perdue. Si le responsable du traitement n'est pas en mesure de restaurer l'accès aux données, par exemple au moyen d'une sauvegarde, alors la perte de disponibilité sera considérée comme permanente.

Une perte de disponibilité peut également se produire en cas de perturbation majeure du service normal d'une organisation, par exemple dans le cas d'une panne de courant ou d'une attaque par déni de service rendant les données à caractère personnel indisponibles.

[13] Il convient de noter qu'un incident de sécurité ne se limite pas à des modèles de menaces où une entité extérieure s'attaque à une organisation, mais qu'il inclut également les incidents de traitement internes qui enfreignent les principes de sécurité.

[14] Voir l'avis 03/2014.

[15] Il est bien établi que l'«accès» est une composante fondamentale de la «disponibilité». Voir par exemple NIST SP800-53rev4, qui définit la «disponibilité» comme: «[l]'assurance d'une utilisation et d'un accès opportuns et fiables à des informations», disponible à l'adresse suivante: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Le CNSSI-4009 mentionne également: «L'accès rapide et fiable aux données et services d'information pour les utilisateurs autorisés.» Voir https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. L'ISO/IEC 27000:2016 définit également la disponibilité comme la «propriété d'être accessible et utilisable à la demande par une entité autorisée»: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:fr

La question pourrait se poser de savoir si une perte de disponibilité temporaire des données à caractère personnel doit être considérée comme une violation, et, si tel est le cas, s'il est nécessaire de la notifier. L'article 32 du RGPD sur la «sécurité du traitement» explique que, lors de la mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, il convient d'envisager, entre autres, «des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement», ainsi que «des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique».

Par conséquent, un incident de sécurité entraînant l'indisponibilité temporaire de données à caractère personnel est également considéré comme un type de violation, dès lors que la perte de l'accès aux données peut avoir une incidence significative sur les droits et libertés des personnes physiques. Il convient de préciser que l'indisponibilité de données à caractère personnel en raison d'un entretien planifié du système n'est pas considérée comme une «violation de la sécurité» au sens de l'article 4, paragraphe 12.

Une violation entraînant une perte de disponibilité temporaire devrait être documentée conformément à l'article 33, paragraphe 5, au même titre qu'une perte ou une destruction permanente de données à caractère personnel (ou tout autre type de violation). Cela aidera le responsable du traitement à démontrer son respect du principe de responsabilité à l'autorité de contrôle, qui pourrait demander à consulter ces registres[16]. Toutefois, en fonction des circonstances de la violation, il peut être nécessaire ou non de la notifier à l'autorité de contrôle et de la communiquer aux personnes concernées. Afin d'en juger, le responsable du traitement devra évaluer la probabilité et la gravité de l'incidence de la perte de disponibilité des données à caractère personnel sur les droits et libertés des personnes physiques. Conformément à l'article 33, le responsable du traitement devra en effet notifier la violation, à moins que celle-ci ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Ce point devra évidemment faire l'objet d'une appréciation au cas par cas.

Exemples

Si des données médicales critiques concernant les patients d'un hôpital sont rendues indisponibles, ne serait-ce que temporairement, cela pourrait présenter un risque pour les droits et libertés des personnes concernées; des opérations pourraient par exemple être annulées et des vies mises en danger.

Inversement, si les systèmes d'une entreprise médiatique ne sont pas disponibles pendant plusieurs heures (p. ex. en raison d'une panne de courant), et que l'entreprise en question n'est de ce fait plus en mesure d'envoyer des bulletins d'information à ses abonnés, il est peu probable que cela représente un risque pour les droits et libertés des personnes concernées.

Il convient de noter que, bien qu'une perte de disponibilité des systèmes du responsable du traitement puisse être uniquement temporaire et n'avoir aucune incidence sur les personnes physiques, il est important que le responsable du traitement envisage toutes les conséquences potentielles d'une violation, dès lors qu'elle peut encore nécessiter une notification pour d'autres raisons.

Exemple

Une attaque par rançongiciel (logiciel malveillant qui crypte les données du responsable du traitement jusqu'à ce qu'une rançon soit versée) pourrait entraîner une perte temporaire de disponibilité si les données peuvent être restaurées au moyen d'une sauvegarde. Cependant, une intrusion dans le réseau

[16] Voir l'article 33, paragraphe 5.

s'est tout de même produite et sa notification pourrait se révéler nécessaire si l'incident est considéré comme une violation de la confidentialité (c.-à-d. que le pirate a accédé aux données à caractère personnel) et que cela présente un risque pour les droits et libertés des personnes physiques.

3. Les conséquences possibles d'une violation de données à caractère personnel

Une violation peut potentiellement avoir, pour les personnes concernées, toute une série de conséquences négatives, susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral. Le RGPD explique que ces dommages et préjudices peuvent inclure une perte de contrôle sur leurs données à caractère personnel, la limitation de leurs droits, une discrimination, un vol ou une usurpation d'identité, une perte financière, un renversement non autorisé de la procédure de pseudonymisation, une atteinte à la réputation ou une perte de confidentialité de données à caractère personnel protégées par le secret professionnel. Ils peuvent également comprendre tout autre dommage économique ou social important pour les personnes concernées[17].

Le RGPD exige donc du responsable du traitement qu'il notifie toute violation à l'autorité de contrôle, à moins qu'elle ne soit pas susceptible d'engendrer le risque que de telles conséquences négatives ne se produisent. Lorsqu'en revanche, ce risque est élevé, le RGPD exige du responsable du traitement qu'il communique la violation aux personnes concernées dans les meilleurs délais[18].

Le considérant 87 du RGPD souligne l'importance d'être en mesure d'identifier une violation, d'évaluer ses risques pour les personnes concernées et de la notifier, le cas échéant:

«Il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement.»

Des orientations complémentaires sur l'évaluation du risque de conséquences négatives pour les personnes concernées sont disponibles au chapitre IV du présent document.

Si les responsables du traitement ne notifient pas une violation de données à l'autorité de contrôle, aux personnes concernées ou aux deux, alors que les conditions établies à l'article 33 et/ou 34 sont remplies, l'autorité de contrôle sera amenée à effectuer un choix, dans le cadre duquel elle sera tenue d'envisager toutes les mesures correctrices à sa disposition, notamment l'imposition d'une amende administrative appropriée[19], que celle-ci accompagne l'une des mesures correctrices définies par l'article 58, paragraphe 2, ou soit imposée comme une sanction indépendante. Si une telle amende administrative est choisie, celle-ci pourra s'élever jusqu'à 10 000 000 EUR ou jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'entreprise conformément à l'article 83, paragraphe 4, point a), du RGPD. Il importe également de garder à l'esprit que dans certains cas, la non-notification d'une violation pourrait trahir une absence de mesures de sécurité ou l'inadéquation des mesures de sécurité

[17] Voir aussi les considérants 85 et 75.

[18] Voir également le considérant 86.

[19] Pour plus de détails, vois les lignes directrices du G29 sur l'application et la fixation des amendes administratives, disponible à l'adresse suivante: https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/wp253-fr.pdf

existantes. Les lignes directrices du G29 sur les amendes administratives disposent que: «[l]a survenance de plusieurs violations différentes commises simultanément dans un cas particulier implique que l'autorité de contrôle a la possibilité d'infliger les amendes administratives à un niveau qui rend celles-ci efficaces, proportionnées et dissuasives, dans les limites de la violation la plus grave». Dans un tel cas, l'autorité de contrôle aura également la possibilité de prononcer des sanctions pour non-notification ou non-communication d'une violation (articles 33 et 34), d'une part, et pour absence de mesures de sécurité (adéquates) (article 32), d'autre part, dès lors qu'il s'agit de deux violations distinctes.

II. Article 33 – Notification à l'autorité de contrôle

A. Quand procéder à la notification

1. Exigences de l'article 33

L'article 33, paragraphe 1, dispose ce qui suit:

> «En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.»

Le considérant 87 prévoit[20]:

> «Il convient de vérifier si toutes les mesures de protection techniques et organisationnelles appropriées ont été mises en œuvre pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer rapidement l'autorité de contrôle et la personne concernée. Il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation des données à caractère personnel et de ses conséquences et effets négatifs pour la personne concernée. Une telle notification peut amener une autorité de contrôle à intervenir conformément à ses missions et à ses pouvoirs fixés par le présent règlement.»

2. Quand un responsable du traitement prend-il «connaissance»?

Comme indiqué ci-dessus, en cas de violation, le RGPD exige du responsable du traitement qu'il notifie la violation en question dans les meilleurs délais, et, si possible, 72 heures au plus tard après en avoir pris connaissance. Cette exigence soulève la question de savoir quand un responsable du traitement peut être considéré comme ayant pris «connaissance» d'une violation. Le G29 considère qu'un responsable du traitement devrait être considéré comme ayant pris «connaissance» lorsqu'il est raisonnablement certain qu'un incident de sécurité s'est produit et que cet incident a compromis des données à caractère personnel.

Cependant, comme indiqué précédemment, le RGPD exige du responsable du traitement qu'il mette en œuvre toutes les mesures de protection techniques et organisationnelles appropriées pour établir immédiatement si une violation des données à caractère personnel s'est produite et pour informer

[20] Le considérant 85 est également important à cet égard.

rapidement l'autorité de contrôle et les personnes concernées. Il dispose également qu'il convient d'établir que la notification a été faite dans les meilleurs délais, compte tenu en particulier de la nature et de la gravité de la violation et de ses conséquences et effets négatifs pour la personne concernée[21]. Le responsable du traitement se voit ainsi tenu de prendre les mesures nécessaires pour s'assurer de prendre «connaissance» de toute violation dans les meilleurs délais afin de pouvoir réagir de façon appropriée.

Le moment exact où un responsable du traitement peut être considéré comme ayant pris «connaissance» d'une violation spécifique dépendra des circonstances de la violation en question. Dans certains cas, il sera relativement clair dès le début qu'une violation s'est produite, tandis que dans d'autres, un certain temps pourrait être nécessaire avant de pouvoir déterminer si des données à caractère personnel ont été compromises. L'accent devrait toutefois être mis sur une intervention et une enquête rapide visant à déterminer s'il y a effectivement eu violation de données à caractère personnel, et, si tel est le cas, à prendre des mesures correctives et à avertir qui de droit, le cas échéant.

Exemples

1. Dans le cas de la perte d'une clé USB contenant des données à caractère personnel cryptées, il est souvent impossible d'évaluer si des personnes non autorisées ont eu accès auxdites données. Cependant, bien que le responsable du traitement ne soit pas en mesure de déterminer si une violation de la confidentialité s'est produite, un tel cas doit être notifié dès lors qu'il est raisonnablement certain qu'une violation de la disponibilité a eu lieu; le responsable du traitement aurait pris «connaissance» de cette violation lorsqu'il s'est rendu compte de la disparition de la clé USB.

2. Un tiers informe un responsable du traitement qu'il a accidentellement reçu les données à caractère personnel de l'un de ses clients et fournit la preuve de cette divulgation non autorisée. Dès lors que le responsable du traitement a reçu des preuves claires attestant d'une violation de la confidentialité, il ne fait aucun doute qu'il en a pris «connaissance».

3. Un responsable du traitement remarque une possible intrusion dans son réseau. Il vérifie son système afin de déterminer si les données à caractère personnel qui y sont conservées ont été compromises et confirme que tel est le cas. Une fois encore, dès lors que le responsable du traitement dispose à présent de preuves claires attestant d'une violation, il ne fait aucun doute qu'il en a pris «connaissance».

4. Un cybercriminel contacte le responsable du traitement après avoir piraté son système afin de lui demander une rançon. Dans ce cas, après avoir vérifié son système en vue de confirmer qu'il a été piraté, le responsable du traitement dispose de preuves claires attestant qu'une violation s'est produite, et il ne fait aucun doute qu'il en a pris connaissance.

Après avoir été informé d'une possible violation par un individu, par une organisation médiatique ou par une autre source, ou encore lorsqu'il a lui-même détecté un incident de sécurité, le responsable du traitement peut mener une brève enquête afin de déterminer si une violation s'est effectivement produite. Lors de cette période d'enquête, le responsable du traitement peut ne pas être considéré comme ayant pris «connaissance». Cette période d'enquête initiale devrait cependant débuter aussi rapidement que possible et déterminer avec un degré de certitude raisonnable si une violation s'est produite; une enquête plus détaillée pourra alors suivre.

[21] Voir le considérant 87.

Après avoir pris connaissance d'un incident, le responsable du traitement devra notifier toute violation soumise à l'obligation de notification dans les meilleurs délais, et, si possible, dans les 72 heures. Pendant cette période, le responsable du traitement devrait évaluer le risque probable pour les personnes concernées afin de déterminer si l'obligation de notification s'applique et quelle ou quelles mesures doivent être prises afin de remédier à cette violation. Un responsable du traitement peut cependant déjà disposer d'une évaluation initiale des risques potentiels qui pourraient résulter d'une violation dans le cadre d'une analyse d'impact relative à la protection des données (AIPD)[22] effectuée préalablement aux opérations de traitement concernées. Une AIPD est néanmoins plus générale que les circonstances spécifiques de toute violation réelle. Aussi une évaluation complémentaire tenant compte de ces circonstances devra-t-elle être réalisée en tout état de cause. Pour plus d'informations sur l'évaluation du risque, voir le chapitre IV.

Dans la plupart des cas, ces mesures préliminaires devraient être prises peu de temps après l'alerte initiale (c.-à-d. lorsque le responsable du traitement ou le sous-traitant suspecte qu'un incident de sécurité portant sur des données à caractère personnel pourrait avoir eu lieu). À l'exception de certains cas exceptionnels, cette procédure ne devrait pas être plus longue que dans l'exemple ci-dessous.

Exemple

Une personne informe le responsable du traitement qu'elle a reçu un courrier électronique dont l'expéditeur se fait passer pour le responsable du traitement et qui contient des données à caractère personnel concernant son utilisation (réelle) des services du responsable du traitement, ce qui indiquerait que la sécurité de ce dernier a été compromise. Le responsable du traitement procède à une brève enquête et repère une intrusion dans son réseau ainsi que des preuves signalant un accès non autorisé à des données à caractère personnel. Le responsable du traitement sera désormais considéré comme ayant pris «connaissance» de la violation et devra en informer l'autorité de contrôle, à moins que ladite violation ne soit peu susceptible d'engendrer un risque pour les droits et libertés des individus. Le responsable du traitement devra prendre des mesures correctives appropriées afin de remédier à la violation.

Le responsable du traitement devrait disposer de procédures internes afin d'être en mesure de détecter une violation et d'y remédier. Par exemple, afin de détecter certaines irrégularités dans le traitement des données, un responsable du traitement ou un sous-traitant peut avoir recours à certaines mesures techniques telles que des analyseurs de flux de données et de journaux, qui permettront de définir des incidents et des alertes en établissant des corrélations entre des données journal[23]. Il est important qu'une fois détectée, une violation soit communiquée au niveau de direction approprié afin qu'il soit possible d'y remédier et, le cas échéant, de la notifier conformément à l'article 33 et, si nécessaire, à l'article 34. De telles mesures et de tels mécanismes de notification devraient être détaillés dans le plan de réaction aux incidents et/ou dans les accords de gouvernance. Ceux-ci aideront le responsable du traitement à planifier et à déterminer efficacement à qui échoit la responsabilité opérationnelle au sein de l'organisation concernant la gestion d'une violation, ainsi que s'il faut, et comment, rapporter une violation de façon appropriée.

[22] Voir les lignes directrices du G29 sur les AIPD à l'adresse suivante: https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

[23] Il convient de noter que les données journal facilitant la vérifiabilité par exemple du stockage, des modifications ou de l'effacement des données peuvent aussi être qualifiées de données à caractère personnel concernant la personne qui a lancé les opérations de traitement respectives.

Le responsable du traitement devrait également disposer d'accords avec tout sous-traitant auquel il a recours, lui-même soumis à l'obligation d'avertir le responsable du traitement en cas de violation (voir plus bas).

S'il incombe aux responsables du traitement et aux sous-traitants de mettre en place les mesures appropriées afin d'être en mesure de prévenir une violation, d'y réagir et d'y remédier, certaines mesures pratiques devraient être prises en toutes circonstances.

- Des informations concernant tous les incidents de sécurité devraient être communiquées à une personne responsable ou aux personnes chargées de remédier aux incidents, d'établir l'existence d'une violation et d'évaluer le risque.
- Le risque pour les personnes concernées résultant d'une violation devrait ensuite être évalué (risque inexistant, risque, ou risque élevé) et les services concernés de l'organisation devraient être informés.
- Le cas échéant, il conviendra subséquemment de notifier la violation à l'autorité de contrôle et de la communiquer aux personnes concernées.
- Parallèlement, le responsable du traitement devrait prendre des mesures pour endiguer la violation et y remédier.
- La violation devrait être documentée tout au long de son évolution.

Il doit donc être clair que le responsable du traitement a l'obligation de réagir à une alerte initiale et de déterminer si une violation a effectivement eu lieu. Cette brève période permet au responsable du traitement de procéder à une enquête et de collecter des preuves et autres informations pertinentes. Une fois que le responsable du traitement a établi, avec un degré de certitude raisonnable, qu'une violation a eu lieu, si les conditions de l'article 33, paragraphe 1, sont remplies, il doit alors la notifier à l'autorité de contrôle dans les meilleurs délais et, si possible, dans les 72 heures[24]. Si un responsable du traitement ne réagit pas dans les meilleurs délais et qu'il apparaît de façon évidente qu'une violation a eu lieu, ce manque de réaction pourrait être considéré comme une non-notification en vertu de l'article 33.

L'article 32 dispose clairement que le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté des données à caractère personnel: la capacité de détecter une violation, d'y remédier et de la communiquer dans les meilleurs délais devrait être considérée comme un élément essentiel de ces mesures.

3. Responsables conjoints du traitement

L'article 26 concerne les responsables conjoints du traitement et dispose que ceux-ci devraient définir leurs obligations respectives aux fins d'assurer le respect du RGPD[25]. Ceci impliquera de déterminer quelle partie sera responsable du respect des obligations définies aux articles 33 et 34. Le G29 recommande que les arrangements contractuels entre les responsables conjoints du traitement comprennent des dispositions déterminant quel responsable du traitement prendra la direction ou sera responsable du respect de l'obligation de notification des violations établie par le RGPD.

4. Obligations du sous-traitant

[24] Voir le règlement (CEE, Euratom) nº 1182/71 portant détermination des règles applicables aux délais, aux dates et aux termes, disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31971R1182

[25] Voir également le considérant 79.

Si le responsable du traitement conserve la responsabilité générale en matière de protection des données à caractère personnel, le rôle du sous-traitant est essentiel afin de permettre au responsable du traitement de respecter ses obligations, notamment en termes de notification des violations. En effet, l'article 28, paragraphe 3, précise que le traitement par un sous-traitant est régi par un contrat ou un autre acte juridique. L'article 28, paragraphe 3, point f), dispose que le contrat ou l'autre acte juridique doit prévoir que le sous-traitant «aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant».

L'article 33, paragraphe 2, indique clairement que si un responsable du traitement a recours à un sous-traitant et que celui-ci prend connaissance d'une violation des données à caractère personnel qu'il traite au nom du responsable du traitement, il doit la lui notifier «dans les meilleurs délais». Il convient de noter que le sous-traitant ne doit pas évaluer la probabilité qu'un risque découle d'une violation avant de la notifier au responsable du traitement; il appartient au responsable du traitement d'effectuer cette évaluation après avoir pris connaissance de la violation. Le sous-traitant doit simplement établir si une violation s'est produite puis la notifier au responsable du traitement. Le responsable du traitement a recours au sous-traitant pour atteindre ses objectifs; aussi le responsable du traitement doit-il en principe être considéré comme ayant pris «connaissance» une fois que le sous-traitant l'a informé de la violation. L'obligation faite au sous-traitant de notifier la violation au responsable du traitement permet à ce dernier d'y remédier et de déterminer s'il est nécessaire d'avertir l'autorité de contrôle conformément à l'article 33, paragraphe 1, ainsi que les personnes concernées conformément à l'article 34, paragraphe 1. Le responsable du traitement pourrait également analyser lui-même la violation en question, dès lors que le sous-traitant pourrait ne pas connaître tous les éléments pertinents liés à la violation. Il pourrait par exemple ne pas savoir si le responsable du traitement conserve toujours une copie ou une sauvegarde des données à caractère personnel détruites ou perdues par le sous-traitant. Ces éléments pourraient avoir une incidence sur l'obligation de notification du responsable du traitement.

Le RGPD ne définit pas de délai spécifique dans lequel le sous-traitant doit alerter le responsable du traitement, si ce n'est qu'il doit le faire «dans les meilleurs délais». Aussi le G29 recommande-t-il au sous-traitant de notifier rapidement la violation en question au responsable du traitement et de lui fournir des informations complémentaires à ce sujet au fur et à mesure que des détails supplémentaires se font jour. Cette communication est essentielle afin d'aider le responsable du traitement à satisfaire à son obligation de notifier la violation à l'autorité de contrôle dans les 72 heures.

Comme expliqué plus haut, le contrat entre le responsable du traitement et le sous-traitant devrait inclure des dispositions précisant la façon de satisfaire aux exigences définies à l'article 33, paragraphe 2, parallèlement à d'autres dispositions du RGPD. Ces dispositions pourraient inclure des exigences de notification rapide par le sous-traitant, ce qui aiderait le responsable du traitement à respecter l'obligation d'informer l'autorité de contrôle dans les 72 heures.

Lorsque le sous-traitant propose ses services à plusieurs responsables du traitement affectés par le même incident, le sous-traitant devra communiquer les détails dudit incident à tous les responsables du traitement.

Un sous-traitant pourrait effectuer une notification au nom du responsable du traitement si celui-ci lui en a donné l'autorisation et si cela fait partie des dispositions contractuelles entre le responsable du traitement et le sous-traitant. Une telle notification doit être effectuée conformément aux articles 33 et 34. Il est cependant important de noter que le titulaire de l'obligation légale de notification reste le responsable du traitement

B. Fournir des informations à l'autorité de contrôle

1. Informations à fournir

15

Lorsqu'un responsable du traitement notifie une violation à l'autorité de contrôle, l'article 33, paragraphe 3, prévoit que la notification doit, à tout le moins:

> «a) décrire la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
>
> b) communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
>
> c) décrire les conséquences probables de la violation de données à caractère personnel;
>
> d) décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives».

Le RGPD ne définit pas les catégories de personnes concernées ni les enregistrements de données à caractère personnel. Toutefois, le G29 suggère que les catégories de personnes concernées se réfèrent aux différents types d'individus dont les données à caractère personnel ont été affectées par une violation: en fonction des descripteurs utilisés, cela pourrait inclure, entre autres, les enfants et autres groupes vulnérables, les personnes handicapées, les employés ou les clients. De façon similaire, les catégories d'enregistrements des données à caractère personnel pourraient se référer aux différents types d'enregistrement que le responsable du traitement pourrait traiter, telles que les données concernant la santé, les dossiers de scolarité, les informations relatives à l'assistance sociale, les données financières, les numéros de compte bancaire, les numéros de passeport, etc.

Le considérant 85 indique clairement que l'obligation de notification a pour finalité de limiter les dommages pour les personnes physiques. Par conséquent, si les types de personnes concernées ou les types de données à caractère personnel témoignent d'un risque de dommages particuliers causés par une violation (p. ex. usurpation d'identité, fraude, perte financière, menace envers le secret professionnel), il est important que la notification indique ces catégories. De cette façon, l'obligation de définir les catégories est liée à l'obligation de décrire les conséquences probables de la violation.

L'absence d'informations précises (p. ex. le nombre exact de personnes concernées affectées) ne devrait pas constituer un obstacle à la notification d'une violation dans les meilleurs délais. Le RGPD accepte que des chiffres approximatifs soient communiqués quant au nombre de personnes et d'enregistrements de données concernés. Il convient de se concentrer davantage sur le fait de remédier aux conséquences négatives de la violation que sur la fourniture de chiffres précis. Aussi, lorsqu'il a été clairement établi qu'une violation s'est produite, mais que sa portée exacte n'est pas encore connue, une notification échelonnée (voir ci-après) est-elle une bonne manière de satisfaire à l'obligation de notification.

L'article 33, paragraphe 3, dispose que le responsable du traitement doit «à tout le moins» inclure les informations listées dans toute notification, ce qui signifie qu'un responsable du traitement peut, si nécessaire, décider de fournir plus d'informations. Les différents types de violations (confidentialité, intégrité ou disponibilité) peuvent nécessiter la fourniture d'informations complémentaires afin d'expliquer en détail les circonstances de chaque cas.

Exemple

Le responsable du traitement pourrait trouver utile d'inclure le nom de son sous-traitant dans sa notification à l'autorité de contrôle si celui-ci est à l'origine de la violation, notamment si cette dernière a entraîné un incident ayant affecté les enregistrements de données à caractère personnel de nombreux autres responsables du traitement ayant recours au même sous-traitant.

16

En tout état de cause, l'autorité de contrôle peut demander des informations complémentaires dans le cadre de son enquête sur la violation.

2. Notification échelonnée

En fonction de la nature de la violation, il peut être nécessaire que le responsable du traitement effectue une enquête complémentaire afin d'établir tous les faits pertinents liés à l'incident. Aussi l'article 33, paragraphe 4, dispose-t-il ce qui suit:

> «Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.»

Cela signifie que le RGPD reconnaît que les responsables du traitement ne disposeront pas toujours de toutes les informations nécessaires concernant une violation dans les 72 heures après en avoir pris connaissance, dès lors que l'ensemble des détails de l'incident peuvent ne pas être systématiquement disponibles au cours de cette période initiale. Il autorise donc une notification échelonnée. Une telle notification interviendra plus probablement dans le cas de violations plus complexes, telles que certains types d'incidents de cybersécurité nécessitant par exemple une enquête approfondie et détaillée afin d'établir pleinement la nature de la violation et la mesure dans laquelle des données à caractère personnel ont été compromises. Dans de nombreux cas, le responsable du traitement devra ainsi poursuivre son enquête et fournir des informations complémentaires à l'autorité de contrôle par la suite. Il y est autorisé à condition de justifier son retard conformément à l'article 33, paragraphe 1. Le G29 recommande que, si le responsable du traitement ne dispose pas encore de toutes les informations nécessaires, il en informe l'autorité de contrôle dans le cadre de sa notification initiale et précise qu'il fournira des informations plus détaillées par la suite. L'autorité de contrôle devrait déterminer la façon et le moment où des informations complémentaires devraient être fournies. Cela n'empêche toutefois pas le responsable du traitement de fournir des informations complémentaires à tout autre moment s'il prend connaissance d'informations complémentaires pertinentes concernant la violation devant être communiquées à l'autorité de contrôle.

L'obligation de notification a pour objectif d'encourager les responsables du traitement à réagir rapidement à une violation, à l'endiguer et, si possible, à récupérer les données à caractère personnel compromises, ainsi qu'à solliciter des conseils auprès de l'autorité de contrôle. La notification à l'autorité de contrôle dans les premières 72 heures peut permettre au responsable du traitement de s'assurer que sa décision concernant la communication ou non de la violation aux personnes concernées est correcte.

L'objectif de cette notification à l'autorité de contrôle n'est cependant pas uniquement d'obtenir des conseils relatifs à la notification éventuelle des personnes concernées. Dans certains cas, il sera évident qu'en raison de la nature de la violation et de la gravité du risque, le responsable du traitement devra informer les personnes concernées dans les meilleurs délais. Par exemple, s'il existe un risque immédiat d'usurpation d'identité, ou si des catégories particulières de données à caractère personnel[26] sont divulguées sur le web, le responsable du traitement devrait réagir dans les meilleurs délais afin d'endiguer la violation et de la communiquer aux personnes concernées (voir chapitre III). Dans des circonstances exceptionnelles, cette communication peut même être effectuée avant la notification à l'autorité de contrôle. De façon plus générale, la notification à l'autorité de contrôle ne peut servir de justification à la non-communication de la violation aux personnes concernées lorsque celle-ci est nécessaire.

Il convient également de préciser que si une enquête de suivi met au jour, après la notification initiale, des preuves indiquant que l'incident de sécurité a été endigué et qu'aucune violation n'a

[26] Voir l'article 9.

effectivement eu lieu, le responsable du traitement peut en informer l'autorité de contrôle. Cette information pourrait alors être ajoutée aux informations déjà fournies à l'autorité de contrôle et l'incident classé comme n'étant pas une violation. Aucune sanction n'est prévue en cas de notification d'un incident qui s'avère, en fin de compte, ne pas constituer une violation.

Exemple

Un responsable du traitement informe l'autorité de contrôle, dans les 72 heures suivant la détection de la violation, de la perte d'une clé USB contenant une copie des données à caractère personnel de certains de ses clients. Il s'avère par la suite que ladite clé USB avait été rangée au mauvais endroit dans les locaux du responsable du traitement et qu'elle a été retrouvée. Le responsable du traitement en informe l'autorité de contrôle et demande à ce que sa notification soit modifiée.

Il convient de noter qu'une telle approche échelonnée de la notification existe déjà en vertu des obligations découlant de la directive 2002/58/CE et du règlement nº 611/2013 ainsi que dans le cadre d'autres incidents autodéclarés.

3. Notification tardive

L'article 33, paragraphe 1, indique clairement que lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard. Cette disposition reconnaît, au même titre que le concept de notification échelonnée, qu'un responsable du traitement pourrait ne pas toujours être en mesure de notifier une violation dans ce délai, et qu'une notification tardive pourrait être autorisée.

Un tel scénario pourrait par exemple se produire lorsqu'un responsable du traitement constate, sur une courte période, plusieurs violations similaires affectant de façon identique de grandes quantités de personnes concernées. Un responsable du traitement pourrait prendre connaissance d'une violation et, en entreprenant son enquête et avant la notification, détecter d'autres violations similaires dont la cause diffère. En fonction des circonstances, il pourrait falloir un certain temps au responsable du traitement pour établir la portée des violations et pour élaborer une notification constructive comprenant différentes violations très similaires, mais aux causes potentiellement différentes, plutôt que de notifier chaque violation individuellement. La notification à l'autorité de contrôle pourrait par conséquent avoir lieu plus de 72 heures après la prise de connaissance de ces violations par le responsable du traitement.

À proprement parler, chaque violation individuelle est un incident devant être notifié. Toutefois, afin d'éviter que la notification ne soit excessivement fastidieuse, le responsable du traitement pourrait soumettre une notification «groupée» énumérant toutes ces violations, à condition qu'elles concernent un seul type de données à caractère personnel compromises de façon similaire et qu'elles se soient produites sur une période de temps relativement courte. Si une série de violations concernant différents types de données à caractère personnel compromises de façon différente se produisent, la notification devra alors se faire selon la procédure classique, c'est-à-dire que chaque violation devra être notifiée conformément à l'article 33.

Si le RGPD autorise dans une certaine mesure les notifications tardives, celles-ci restent exceptionnelles. Il convient de signaler qu'une notification groupée peut également être effectuée pour des violations similaires multiples notifiées dans les 72 heures.

C. Violations transfrontalières et violations dans des établissements de pays tiers

1. Violations transfrontalières

En cas de traitement transfrontalier[27] de données à caractère personnel, une violation peut affecter des personnes concernées dans plus d'un État membre. L'article 33, paragraphe 1, indique clairement qu'en cas de violation, le responsable du traitement doit la notifier à l'autorité de contrôle compétente conformément à l'article 55 du RGPD[28]. L'article 55, paragraphe 1, dispose ce qui suit:

> «Chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'État membre dont elle relève.»

Toutefois, l'article 56, paragraphe 1, prévoit ce qui suit:

> «Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60.»

Par ailleurs, l'article 56, paragraphe 6, énonce ce qui suit:

> «L'autorité de contrôle chef de file est le seul interlocuteur du responsable du traitement ou du sous-traitant pour le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant.»

Cela signifie qu'en cas de violation dans le cadre d'un traitement transfrontalier nécessitant une notification, le responsable du traitement devra informer l'autorité de contrôle chef de file[29]. Aussi un responsable du traitement doit-il, lors de la rédaction de son plan de réaction à une violation, évaluer quelle autorité de contrôle est l'autorité de contrôle chef de file qu'il devra informer[30]. Cela permettra au responsable du traitement de réagir rapidement à une violation et de respecter ses obligations au titre de l'article 33. Il doit être clair qu'en cas de violation impliquant un traitement transfrontalier, il convient de notifier la violation à l'autorité de contrôle chef de file, qui n'est pas nécessairement celle de l'endroit où les personnes concernées résident ou de l'endroit où la violation a eu lieu. Lorsqu'il notifie la violation à l'autorité de contrôle chef de file, le responsable du traitement devrait indiquer, le cas échéant, si la violation implique des établissements situés dans d'autres États membres et les États membres dans lesquels des personnes concernées sont susceptibles d'être affectées par la violation. Si le responsable du traitement a des doutes concernant l'identité de l'autorité de contrôle chef de file, il devrait, à tout le moins, informer l'autorité de contrôle locale de l'endroit où la violation s'est produite.

2. Violations dans des établissements de pays tiers

[27] Voir l'article 4, paragraphe 23.

[28] Voir également le considérant 122.

[29] Voir les lignes directrices du G29 sur la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant disponibles à l'adresse suivante: https://www.cnil.fr/sites/default/files/atoms/files/wp244rev01_fr.pdf

[30] Une liste des coordonnées de toutes les autorités de protection des données nationales est disponible à l'adresse suivante: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

L'article 3 concerne le champ d'application territorial du RGPD, y compris lorsqu'il s'applique au traitement de données à caractère personnel par un responsable du traitement ou un sous-traitant n'étant pas établi dans l'UE. Plus précisément, l'article 3, paragraphe 2, énonce ce qui suit[31]:

> «Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées:
>
> a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou
>
> b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.»

L'article 3, paragraphe 3, est également pertinent en la matière et dispose que[32]:

> «[l]e présent règlement s'applique au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public».

Lorsqu'un responsable du traitement qui n'est pas établi dans l'UE est soumis à l'article 3, paragraphe 2, ou à l'article 3, paragraphe 3, et constate une violation, il est par conséquent toujours tenu de respecter les obligations de notification définies aux articles 33 et 34. L'article 27 dispose qu'un responsable du traitement (ou un sous-traitant) doit désigner un représentant dans l'UE lorsque l'article 3, paragraphe 2, s'applique. Dans de tels cas, le G29 recommande que la notification soit adressée à l'autorité de contrôle de l'État membre dans lequel le représentant du responsable du traitement dans l'UE est établi[33]. De la même façon, lorsqu'un sous-traitant est soumis à l'article 3, paragraphe 2, il sera tenu de respecter les obligations incombant aux sous-traitants, et notamment l'obligation de notifier la violation au responsable du traitement conformément à l'article 33, paragraphe 2.

D. Conditions dans lesquelles la notification n'est pas obligatoire

L'article 33, paragraphe 1, indique clairement qu'une violation qui n'est «pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques» ne doit pas être notifiée à l'autorité de contrôle. Tel pourrait par exemple être le cas lorsque les données à caractère personnel sont déjà disponibles pour le public et qu'une divulgation desdites données n'est pas susceptible d'engendrer un risque pour les personnes concernées. Ceci contraste avec les obligations de notification s'appliquant aux fournisseurs de services de communications électroniques accessibles au public en vertu de la directive 2009/136/CE, qui dispose que toutes les violations pertinentes doivent être notifiées à l'autorité compétente.

Dans son avis 03/2014 sur la notification des violations[34], le G29 expliquait qu'une violation de la confidentialité de données à caractère personnel qui ont été cryptées à l'aide d'un algorithme de

[31] Voir aussi les considérants 23 et 24.

[32] Voir également le considérant 25.

[33] Voir le considérant 80 et l'article 27.

[34] Avis 03/2014 du G29 sur la notification des violations, http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_fr.pdf

pointe constituait tout de même une violation de données à caractère personnel, et que celle-ci devait être notifiée. Néanmoins, si la confidentialité de la clé de cryptage est intacte – c.-à-d. que la clé n'a été compromise dans aucune violation de sécurité et a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser –, les données sont en principe incompréhensibles. La violation n'est donc pas susceptible de porter atteinte aux personnes concernées et n'aurait donc pas besoin de leur être communiquée[35]. Toutefois, même lorsque les données sont cryptées, une perte ou une altération peut avoir des conséquences négatives pour les personnes concernées lorsque le responsable du traitement ne dispose pas de sauvegardes adéquates. Dans ce cas de figure, il convient de communiquer la violation aux personnes concernées, même si les données elles-mêmes ont fait l'objet de mesures de cryptage adéquates.

Le G29 expliquait aussi que le même raisonnement s'appliquait dans les cas où les données à caractère personnel, telles les mots de passe, sont hachées et salées en mode sécurisé, où la valeur hachée a été calculée à l'aide d'une fonction de hachage à clé cryptographique de pointe, où la clé utilisée pour hacher les données n'a été compromise dans aucune violation de sécurité et où celle-ci a été générée de façon à ne pouvoir être trouvée, par aucun moyen technologique existant, par quelqu'un qui n'est pas autorisé à l'utiliser.

Par conséquent, si les données à caractère personnel ont été rendues incompréhensibles pour tout tiers non autorisé et si les données en question constituent une copie ou qu'il en existe une sauvegarde, une violation de la confidentialité portant sur des données à caractère personnel correctement cryptées ne doit pas être notifiée à l'autorité de contrôle. La raison en est qu'une telle violation est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Cela signifie bien entendu que la personne concernée ne devra pas non plus être informée dès lors que la violation est peu susceptible d'engendrer un risque élevé. Il convient toutefois de garder à l'esprit que si la notification peut ne pas être requise dans un premier temps dans la mesure où il n'existe pas de risque probable pour les droits et libertés des personnes physiques, cet état des choses peut évoluer avec le temps, et le risque devra alors être réévalué. Par exemple, si l'on se rend ultérieurement compte que la clé est compromise ou si l'on découvre une vulnérabilité dans le logiciel de cryptage, une notification pourrait toujours être nécessaire.

Il convient en outre de noter qu'une violation de données cryptées ne disposant pas d'une sauvegarde constitue une violation de la disponibilité, ce qui pourrait engendrer un risque pour les personnes concernées et donc nécessiter une notification. De la même façon, une violation qui entraîne la perte de données cryptées disposant d'une sauvegarde peut toujours constituer une violation à notifier en fonction de la période de temps nécessaire pour restaurer les données à partir de la sauvegarde en question et des conséquences de cette perte de disponibilité pour les personnes physiques. Comme indiqué à l'article 32, paragraphe 1, point c), un facteur de sécurité important est en effet l'existence de «moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique».

Exemple

Une violation qui ne nécessiterait aucune notification à l'autorité de contrôle serait la perte d'un appareil mobile crypté de façon sécurisée et utilisé par le responsable du traitement et son personnel. Si la clé de cryptage reste en la possession du responsable du traitement et que les données à caractère personnel affectées ne constituent pas une copie unique, celles-ci seraient inaccessibles à tout pirate. Cela signifie que la violation est peu susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. Si, par la suite, il devient évident que la clé de cryptage a été compromise ou

[35] Voir également l'article 4, paragraphes 1 et 2, du règlement (UE) nº 611/2013.

que le logiciel ou algorithme de cryptage est vulnérable, le risque pour les droits et libertés des personnes physiques s'en verra affecté et une notification pourra alors être nécessaire.

Cependant, si un responsable du traitement n'informe pas l'autorité de contrôle alors que les données n'ont pas été effectivement cryptées de façon sécurisée, il se trouvera en situation de non-respect de l'article 33. Ainsi, en choisissant leur logiciel de cryptage, les responsables du traitement devraient être particulièrement attentifs à la qualité et à la bonne application du cryptage envisagé, s'assurer de comprendre le niveau de protection qu'il fournit effectivement et évaluer s'il convient aux risques potentiels. Les responsables du traitement devraient également connaître en détail le fonctionnement de leur produit de cryptage. Par exemple, un appareil pourrait être crypté une fois éteint, mais pas lorsqu'il se trouve en mode veille. Certains produits de cryptage disposent par ailleurs de «clés par défaut» qui doivent être modifiées par chaque client afin d'être efficaces. Le cryptage pourrait également être considéré comme adéquat par des experts en sécurité au moment de sa mise en œuvre, mais pourrait être dépassé quelques années plus tard. Il ne serait alors plus certain que les données sont cryptées de façon suffisante par le produit en question et que celui-ci fournit un niveau de protection approprié.

III. **Article 34 – Communication à la personne concernée**

A. Informer les personnes concernées

Dans certains cas, en plus de notifier une violation à l'autorité de contrôle, le responsable du traitement est également tenu de la communiquer aux personnes concernées.

L'article 34, paragraphe 1, dispose que:

«[l]orsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais».

Les responsables du traitement devraient garder à l'esprit que la notification à l'autorité de contrôle est obligatoire, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. En outre, lorsqu'une violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, ces dernières doivent également être informées. Le seuil à atteindre est par conséquent plus élevé pour la communication aux personnes concernées que pour la notification à l'autorité de contrôle, et toutes les violations ne devront donc pas être communiquées aux personnes concernées, ce qui les protège de notifications excessives et non nécessaires.

Le RGPD indique que la communication d'une violation aux personnes concernées devrait se faire «dans les meilleurs délais», c'est-à-dire aussi vite que possible. L'objectif principal de la notification aux personnes concernées est de fournir des informations spécifiques concernant les mesures qu'elles devraient prendre pour se protéger[36]. Comme précisé ci-dessus, en fonction de la nature de la violation et des risques engendrés, une communication rapide aidera les personnes concernées à prendre des mesures pour se protéger contre toute conséquence négative de la violation.

[36] Voir également le considérant 86.

L'annexe B des présentes lignes directrices fournit une liste non exhaustive d'exemples de cas où une violation pourrait être susceptible d'engendrer un risque élevé pour les personnes concernées et, partant, de cas où un responsable du traitement devra notifier une violation aux personnes concernées.

B. Informations à fournir

Concernant la notification des personnes concernées, l'article 34, paragraphe 2, dispose que:

> «[l]a communication à la personne concernée visée au paragraphe 1 du présent article décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins les informations et mesures visées à l'article 33, paragraphe 3, points b), c) et d)».

Conformément à cette disposition, le responsable du traitement devrait au moins fournir les informations suivantes:

- une description de la nature de la violation;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact;
- une description des conséquences probables de la violation; et
- une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation, y compris, le cas échéant, des mesures pour en atténuer les éventuelles conséquences négatives.

À titre d'exemple de mesures prises pour remédier à la violation et pour en atténuer les conséquences négatives, un responsable du traitement pourrait indiquer qu'après avoir notifié la violation à l'autorité de contrôle pertinente, il a reçu des conseils sur la gestion de la violation et l'atténuation de ses conséquences. Le responsable du traitement devrait également, le cas échéant, fournir des conseils spécifiques aux personnes affectées concernant la façon de se protéger des éventuelles conséquences négatives de la violation, par exemple en réinitialisant leurs mots de passe si les informations de connexion ont été compromises. Une fois encore, un responsable du traitement peut choisir de fournir des informations complémentaires à celles présentées ici comme nécessaires.

C. Contacter les personnes concernées

En principe, la violation devrait être communiquée aux personnes concernées directement, à moins que cela n'exige des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace [article 34, paragraphe 3, point c)].

La communication d'une violation aux personnes concernées devrait se faire au moyen de messages dédiés ne contenant pas d'autres informations, telles que des comptes rendus réguliers, des bulletins d'informations ou des messages standard. La communication de la violation sera ainsi plus claire et transparente.

De telles méthodes de communication transparente pourraient être des messages directs (p. ex. e-mail, SMS, message direct), des notifications ou des bannières bien visibles sur le site internet, des communications postales et des annonces bien visibles dans des médias imprimés. Une notification se limitant uniquement à un communiqué de presse ou à un blog d'entreprise ne constituerait pas une méthode efficace de communication d'une violation à une personne. Le G29 recommande que les responsables du traitement choisissent une méthode qui maximise la probabilité que les informations soient communiquées comme il se doit à toutes les personnes concernées. En fonction des circonstances, cela peut impliquer que le responsable du traitement ait recours à plusieurs méthodes de communication, par opposition à un canal de contact unique.

Il pourrait également être nécessaire que les responsables du traitement s'assurent que la communication soit accessible dans des formats alternatifs appropriés ainsi que dans les langues pertinentes afin que les personnes concernées soient en mesure de comprendre les informations qui leur sont communiquées. Par exemple, la langue utilisée lors des échanges habituels préalables avec une personne concernée sera généralement appropriée pour communiquer une violation à cette même personne. Toutefois, si la violation touche des personnes concernées avec lesquelles le responsable du traitement n'a jamais interagi par le passé, ou en particulier des personnes qui résident dans un État membre ou un pays non membre de l'UE autre que celui où est établi le responsable du traitement, une communication dans la langue locale devrait être appropriée, compte tenu des ressources nécessaires. L'objectif principal est d'aider les personnes concernées à comprendre la nature de la violation ainsi que les mesures qu'elles peuvent mettre en place pour se protéger.

Les responsables du traitement sont les mieux placés pour déterminer le canal le plus approprié afin de communiquer une violation aux personnes concernées, en particulier s'ils interagissent fréquemment avec leurs clients. Cependant, un responsable du traitement devrait bien évidemment se montrer prudent dans l'utilisation d'un canal de contact compromis par une violation, dès lors que ce canal pourrait également être utilisé par le pirate pour se faire passer pour le responsable du traitement.

Parallèlement, le considérant 86 explique ce qui suit:

> «Il convient que de telles communications aux personnes concernées soient effectuées aussi rapidement qu'il est raisonnablement possible et en coopération étroite avec l'autorité de contrôle, dans le respect des directives données par celle-ci ou par d'autres autorités compétentes, telles que les autorités répressives. Par exemple, la nécessité d'atténuer un risque immédiat de dommage pourrait justifier d'adresser rapidement une communication aux personnes concernées, alors que la nécessité de mettre en œuvre des mesures appropriées empêchant la poursuite de la violation des données à caractère personnel ou la survenance de violations similaires peut justifier un délai plus long pour la communication.»

Les responsables du traitement pourraient dès lors contacter et consulter l'autorité de contrôle non seulement pour obtenir des conseils sur la façon d'informer les personnes concernées d'une violation conformément à l'article 34, mais également sur les messages adéquats à envoyer aux personnes concernées et sur la façon la plus appropriée de les contacter.

Parallèlement, le considérant 88 indique que la notification d'une violation devrait «tenir compte des intérêts légitimes des autorités répressives lorsqu'une divulgation prématurée risquerait d'entraver inutilement l'enquête sur les circonstances de la violation des données à caractère personnel». Cela peut signifier que, dans certaines circonstances, lorsque cela se justifie et sur les conseils des autorités répressives, le responsable du traitement peut retarder la communication de la violation aux personnes concernées jusqu'au moment où cette communication n'entraverait plus une telle enquête. Passé ce délai, les personnes concernées devront toutefois toujours être informées dans les meilleurs délais.

Dans le cas particulier où le responsable du traitement n'est pas en mesure de communiquer une violation à une personne concernée car il ne dispose pas d'informations suffisantes pour la contacter, il devrait l'informer dès que raisonnablement possible (p. ex. lorsqu'une personne concernée exerce son droit d'accès à ses données à caractère personnel au titre de l'article 15 et fournit au responsable du traitement les informations complémentaires nécessaires afin de la contacter).

D. Conditions dans lesquelles la communication n'est pas obligatoire

L'article 34, paragraphe 3, définit trois conditions dans lesquelles la communication aux personnes concernées n'est pas nécessaire en cas de violation, à savoir:

- le responsable du traitement a mis en œuvre les mesures techniques et organisationnelles appropriées afin de protéger les données à caractère personnel préalablement à la violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès. Cela pourrait par exemple inclure la protection des données à caractère personnel au moyen d'un chiffrement de pointe ou par tokénisation;
- le responsable du traitement a pris, immédiatement après la violation, des mesures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se concrétiser. Par exemple, en fonction des circonstances du cas d'espèce, le responsable du traitement peut avoir immédiatement déterminé et pris des mesures contre la personne ayant accédé aux données à caractère personnel avant qu'elle n'ait pu les utiliser. Il convient cependant toujours de tenir compte des conséquences potentielles de toute violation de la confidentialité, toujours en fonction de la nature des données concernées;
- contacter les personnes concernées exigerait des efforts disproportionnés[37], par exemple si leurs coordonnées ont été perdues à la suite de la violation ou ne sont tout simplement pas connues. Par exemple, l'entrepôt d'un bureau de statistiques a été inondé et les documents contenant les données à caractère personnel n'existaient qu'en format papier. Dans un tel cas, le responsable du traitement doit procéder à une communication publique ou prendre une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace. En cas d'efforts disproportionnés, des dispositions techniques pourraient également être envisagées afin que les informations concernant la violation soient disponibles sur demande, ce qui pourrait se révéler utile pour les personnes éventuellement affectées par la violation, mais que le responsable du traitement n'est pas en mesure de contacter par un autre biais.

Conformément au principe de responsabilité, les responsables du traitement devraient être en mesure de démontrer à l'autorité de contrôle qu'ils remplissent l'une ou plusieurs de ces conditions[38]. Il convient de garder à l'esprit que si la notification peut ne pas être requise dans un premier temps dans la mesure où il n'existe pas de risque pour les droits et libertés des personnes physiques, cet état des choses peut évoluer avec le temps, et le risque devra alors être réévalué.

Si un responsable du traitement décide de ne pas communiquer une violation aux personnes concernées, l'article 34, paragraphe 4, explique que l'autorité de contrôle peut exiger de lui qu'il procède à cette communication si elle considère que la violation est susceptible d'engendrer un risque élevé pour les personnes concernées. Elle peut également au contraire considérer que les conditions visées à l'article 34, paragraphe 3, sont remplies et qu'aucune communication aux personnes concernées n'est donc requise. Si l'autorité de contrôle juge que la décision de ne pas informer les personnes concernées n'est pas fondée, elle peut par ailleurs envisager de recourir aux pouvoirs et sanctions à sa disposition.

IV. Évaluation de l'existence d'un risque ou d'un risque élevé

A. Le risque en tant que déclencheur de la notification

[37] Voir les lignes directrices du G29 sur la transparence, qui aborderont la problématique des efforts disproportionnés, disponible à l'adresse suivante: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] Voir l'article 5, paragraphe 2.

Bien que le RGPD introduise l'obligation de notifier une violation, celle-ci ne s'impose pas en toutes circonstances:

- la notification à l'autorité de contrôle compétente est obligatoire à moins qu'une violation soit peu susceptible d'engendrer un risque pour les droits et libertés des individus;
- la communication d'une violation aux personnes concernées ne devient nécessaire que lorsque ladite violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

Cela signifie qu'immédiatement après avoir pris connaissance d'une violation, il est crucial que le responsable du traitement ne cherche pas uniquement à endiguer l'incident, mais qu'il évalue également le risque qui pourrait en résulter. Il y a deux raisons principales à cela: premièrement, si le responsable du traitement connaît la probabilité et la gravité potentielle des conséquences pour les personnes concernées, cela l'aidera à prendre des mesures efficaces pour endiguer et remédier à la violation; deuxièmement, cela l'aidera à déterminer s'il est tenu d'informer l'autorité de contrôle et, le cas échéant, les personnes concernées.

Comme expliqué plus haut, la notification d'une violation est obligatoire à moins que cette violation soit peu susceptible d'engendrer un risque pour les droits et libertés des individus, tandis que la communication d'une violation aux personnes concernées ne devient nécessaire que lorsque ladite violation est susceptible d'engendrer un risque *élevé* pour leurs droits et libertés. Un tel risque existe lorsqu'une violation est susceptible d'engendrer des dommages physiques, matériels ou un préjudice moral pour les personnes dont les données ont fait l'objet de la violation. Des exemples de tels dommages sont la discrimination, le vol ou l'usurpation d'identité, la perte financière ou l'atteinte à la réputation. Lorsque la violation implique des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ou des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes, de tels dommages sont considérés comme susceptibles de se produire[39].

B. Les facteurs à prendre en compte lors de l'évaluation du risque

Les considérants 75 et 76 du RGPD indiquent qu'en général, lors de l'évaluation du risque, il convient de tenir compte à la fois de la probabilité et de la gravité du risque pour les droits et libertés des personnes concernées. Ils disposent en outre que le risque devrait faire l'objet d'une évaluation objective.

Il est à noter que l'évaluation du risque présenté par une violation pour les droits et libertés des personnes concernées se fait selon une approche différente de celle adoptée dans le cadre d'une AIPD[40]. L'AIPD envisage en effet autant les risques encourus si le traitement des données est effectué comme prévu que les risques en cas de violation. Dans le cadre de son appréciation d'une éventuelle violation, une telle analyse évalue de façon générale la probabilité d'une telle violation ainsi que les dommages qu'elle pourrait engendrer pour les personnes concernées; il s'agit, en d'autres termes, de l'évaluation d'un incident hypothétique. En cas de violation réelle, l'incident s'est déjà produit et l'accent est donc entièrement mis sur le risque présenté par la violation pour les personnes concernées.

[39] Voir les considérants 75 et 85.

[40] Voir les lignes directrices du G29 sur les AIPD à l'adresse suivante: https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

Exemple

Une AIPD considère que l'utilisation envisagée d'un logiciel de sécurité donné afin de protéger les données à caractère personnel constitue une mesure appropriée pour assurer un niveau de sécurité adapté au risque que le traitement présenterait pour les personnes concernées sans ledit logiciel. Toutefois, si le logiciel révélait ultérieurement une vulnérabilité, cela changerait sa capacité à limiter le risque pour les données à caractère personnel protégées et il devrait donc être réévalué dans le cadre d'une AIPD continue.

Cette vulnérabilité est ensuite exploitée et une violation se produit. Le responsable du traitement devrait évaluer les circonstances spécifiques de la violation, les données concernées et la gravité potentielle des conséquences pour les personnes concernées, ainsi que la probabilité que le risque se concrétise.

En évaluant le risque présenté par une violation pour les personnes concernées, le responsable du traitement devrait par conséquent tenir compte des circonstances spécifiques de la violation, y compris la gravité des conséquences potentielles et la probabilité que celles-ci se produisent. Le G29 recommande donc que l'évaluation tienne compte des critères suivants[41]:

- Le type de violation

Le type de la violation survenue peut avoir une incidence sur le niveau de risque encouru par les personnes concernées. Par exemple, les conséquences d'une violation de la confidentialité dans le cadre de laquelle des informations médicales ont été divulguées à des parties non autorisées pourraient différer de celles engendrées par une violation dans le cadre de laquelle les informations médicales d'un patient ont été perdues ou ne sont plus disponibles.

- La nature, le caractère sensible et le volume des données à caractère personnel

De toute évidence, l'un des facteurs clés dans l'évaluation du risque est le type et le caractère sensible des données à caractère personnel qui ont été compromises par la violation. En général, plus les données sont sensibles, plus le risque de dommage sera élevé pour les personnes concernées, mais il convient également de tenir compte des autres données à caractère personnel qui pourraient déjà être disponibles au sujet de la personne concernée. Par exemple, dans des circonstances normales, la divulgation du nom et de l'adresse d'une personne est peu susceptible d'entraîner un préjudice important. Par contre, si le nom et l'adresse d'un parent adoptif sont divulgués à un parent biologique, les conséquences pourraient être considérables à la fois pour le parent adoptif et pour l'enfant.

Si, prises individuellement, des violations portant sur des données relatives à la santé, des documents d'identité ou des données financières, telles que des données de carte de crédit, peuvent nuire à la personne concernée, prises ensemble, elles pourraient être utilisées pour une usurpation d'identité. La combinaison de données à caractère personnel est ainsi généralement plus sensible que chaque type de données à caractère personnel pris séparément.

Si certains types de données à caractère personnel peuvent sembler, au premier abord, relativement inoffensifs, il convient tout de même d'évaluer minutieusement ce que les données pourraient révéler

[41] L'article 3, paragraphe 2, du règlement (UE) nº 611/2013 fournit des orientations sur les facteurs qui devraient être pris en compte pour ce qui est de la notification des violations dans le secteur des services de communications électroniques et pouvant être utiles dans le cadre de la notification en vertu du RGPD. Voir: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:fr:PDF

sur la personne concernée. Une liste de clients acceptant des livraisons régulières n'est a priori pas particulièrement sensible, mais ces mêmes données concernant des clients ayant demandé à ce que leurs livraisons soient interrompues lorsqu'ils partent en vacances constitueraient des informations utiles aux yeux de criminels.

De la même façon, si une petite quantité de données à caractère personnel hautement sensibles peut avoir d'importantes conséquences pour la personne concernée, un grand nombre de détails peut révéler une quantité d'informations plus grande encore au sujet de cette même personne. Une violation touchant de gros volumes de données à caractère personnel au sujet de très nombreuses personnes peut ainsi avoir des conséquences pour un tout aussi grand nombre de personnes.

- La facilité d'identification des personnes concernées

Un facteur important à prendre en compte est la facilité avec laquelle une partie ayant accès à des données à caractère personnel compromises peut identifier des individus spécifiques ou associer les données en question à d'autres informations afin d'identifier ces mêmes individus. Dans certaines circonstances, une identification pourrait être possible directement à partir des données à caractère personnel compromises, sans que des recherches spécifiques ne soient nécessaires pour découvrir l'identité de la personne concernée, tandis que dans d'autres, il pourrait être extrêmement difficile d'attribuer des données à caractère personnel à une personne spécifique, bien que cela puisse toujours être possible dans certaines conditions. Une identification peut être directement ou indirectement possible à partir des données compromises, comme elle peut dépendre des circonstances spécifiques de la violation et de la disponibilité publique de renseignements personnels connexes. Cette dernière éventualité serait plus pertinente en cas de violation de la confidentialité ou de la disponibilité.

Comme indiqué plus haut, les données à caractère personnel protégées par un niveau de cryptage approprié seront incompréhensibles pour tout tiers non autorisé sans la clé de décryptage. En outre, une pseudonymisation correctement mise en œuvre (définie à l'article 4, paragraphe 5, comme «le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable») peut également réduire la probabilité que des personnes physiques soient identifiées en cas de violation. Les techniques de pseudonymisation ne peuvent néanmoins pas être considérées comme suffisantes à elles seules pour rendre les données incompréhensibles.

- La gravité des conséquences pour les personnes concernées

En fonction de la nature des données à caractère personnel impliquées dans une violation, par exemple des catégories particulières de données, les dommages potentiels pour les personnes concernées peuvent être particulièrement graves, notamment lorsque la violation pourrait entraîner un vol ou une usurpation d'identité, un préjudice physique, une détresse psychologique, une humiliation ou une atteinte à la réputation. Si la violation concerne des données à caractère personnel de personnes vulnérables, celles-ci pourraient être exposées à un plus grand risque de dommages.

Le fait que le responsable du traitement ait connaissance ou non de ce que des données à caractère personnel se trouvent en la possession de personnes dont les intentions sont inconnues ou potentiellement malicieuses peut avoir une incidence sur le niveau de risque potentiel. Prenons le cas d'une violation de la confidentialité dans le cadre de laquelle des données à caractère personnel ont été accidentellement divulguées à un tiers, tel que défini à l'article 4, paragraphe 10, ou à un autre destinataire. Une telle situation peut par exemple se produire lorsque des données à caractère personnel sont envoyées par erreur au mauvais service d'une organisation ou à un organisme fournisseur fréquemment sollicité. Le responsable du traitement peut demander au destinataire de lui renvoyer les données reçues ou de les détruire de façon sécurisée. Dans les deux cas, dès lors que le

28

responsable du traitement entretient une relation continue avec le destinataire et qu'il pourrait avoir connaissance de ses procédures, de ses antécédents et de toute autre information pertinente, ce dernier peut être considéré comme «fiable». En d'autres termes, le responsable du traitement peut disposer d'un certain degré de confiance envers le destinataire, de manière à pouvoir raisonnablement s'attendre à ce que ce dernier ne lise pas les données envoyées par erreur ou n'y accède pas et à ce qu'il satisfasse à sa demande de les lui renvoyer. Quand bien même le destinataire aurait accédé aux données, le responsable du traitement pourrait toujours être convaincu qu'il n'entreprendra aucune autre action par rapport à celles-ci et qu'il les lui renverra rapidement et coopérera pour assurer leur récupération. Dans de tels cas, le responsable du traitement peut tenir compte de ce facteur dans son évaluation du risque présenté par la violation. Si le fait que le destinataire est considéré comme fiable peut neutraliser la gravité des conséquences de la violation, cela ne signifie en effet pas pour autant qu'aucune violation ne s'est produite. La probabilité que ladite violation engendre un risque pour les personnes concernées peut en revanche s'en voir invalidée et il ne serait dès lors plus nécessaire de la notifier à l'autorité de contrôle ou aux personnes concernées. Encore une fois, tout dépendra des circonstances spécifiques de chaque violation. Le responsable du traitement devra cependant toujours conserver les renseignements relatifs à la violation dans le cadre de son obligation générale de tenir des registres des violations (voir le chapitre V ci-après).

Il convient également de tenir compte de la permanence des conséquences pour les personnes concernées, celles-ci pouvant être considérées comme plus importantes si elles ont un effet à long terme.

- Les caractéristiques particulières des personnes concernées

Une violation peut toucher des données à caractère personnel concernant des enfants ou d'autres personnes vulnérables, qui pourraient alors être exposés à un risque plus important. D'autres facteurs spécifiques aux personnes concernées pourraient également affecter la gravité des conséquences de la violation pour les personnes en question.

- Les caractéristiques particulières du responsable du traitement

La nature et le rôle du responsable du traitement ainsi que de ses activités peuvent affecter le niveau de risque qu'engendre une violation pour les personnes concernées. Par exemple, dès lors qu'une organisation médicale traite des catégories particulières de données à caractère personnel, le risque pour les personnes concernées sera plus important en cas de violation de données à caractère personnel que s'il s'agissait d'une liste de diffusion d'un journal.

- Le nombre de personnes concernées

Une violation peut toucher uniquement une personne, un nombre restreint de personnes ou des milliers de personnes, voire davantage. En général, plus le nombre de personnes concernées est élevé, plus les conséquences potentielles d'une violation sont nombreuses. Une violation peut cependant également avoir de graves conséquences ne serait-ce que pour une seule personne en fonction de la nature des données à caractère personnel et du contexte dans lequel elles ont été compromises. La solution consiste à nouveau à évaluer la probabilité et la gravité des conséquences pour les personnes concernées.

- Éléments généraux

Lorsqu'il évalue le risque susceptible de résulter d'une violation, le responsable du traitement devrait ainsi examiner à la fois la gravité des conséquences potentielles pour les droits et libertés des personnes concernées et la probabilité que ces conséquences se produisent. Il est évident que lorsque les conséquences d'une violation sont potentiellement plus graves, le risque est plus élevé. De même, lorsque la probabilité que celles-ci se produisent est plus importante, le risque s'en verra également renforcé. En cas de doute, le responsable du traitement devrait opter pour la prudence et procéder à

29

une notification. L'annexe B fournit une série d'exemples utiles de différents types de violations représentant un risque ou un risque élevé pour les personnes concernées.

L'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié des recommandations relatives à la méthodologie à adopter pour évaluer la gravité d'une violation que les responsables du traitement et les sous-traitants pourraient trouver utiles lors de la conception de leur plan de réaction et d'intervention en cas de violation[42].

V. Responsabilité et tenue de registres

A. Documenter les violations

Qu'une violation doive être notifiée à l'autorité de contrôle ou non, le responsable du traitement est tenu de documenter toutes les violations, comme expliqué à l'article 33, paragraphe 5:

> «Le responsable du traitement documente toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect du présent article.»

Cette obligation de documentation est liée au principe de responsabilité du RGPD figurant à l'article 5, paragraphe 2. Cette exigence de tenir des registres des violations, qu'elles soient sujettes à notification ou non, est également liée aux obligations du responsable du traitement au titre de l'article 24, et l'autorité de contrôle peut demander à voir lesdits registres. Les responsables du traitement sont donc encouragés à établir un registre interne des violations, qu'ils soient tenus de les notifier ou non[43].

S'il appartient au responsable du traitement de déterminer la méthode et la structure à utiliser pour documenter une violation, certaines informations clés devraient être incluses en toutes circonstances. Comme requis à l'article 33, paragraphe 5, le responsable du traitement doit reprendre des informations concernant la violation, y compris les causes, les faits et les données à caractère personnel concernées. Il devrait également inclure les effets et les conséquences de la violation ainsi que les mesures prises par le responsable du traitement pour y remédier.

Le RGPD ne définit pas la période de conservation d'une telle documentation. Lorsque de tels registres contiennent des données à caractère personnel, il incombera au responsable du traitement de déterminer la période de conservation appropriée conformément aux principes liés au traitement de données à caractère personnel[44] et au fondement juridique du traitement[45]. Il devra conserver cette documentation conformément à l'article 33, paragraphe 5, dès lors que l'autorité de contrôle pourrait la réclamer à titre de preuve du respect dudit article, ou plus généralement du principe de

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[43] Le responsable du traitement peut décider de documenter les violations dans le cadre de son registre des activités de traitement tenu conformément à l'article 30. Un registre séparé n'est pas nécessaire, à condition que les informations concernant les violations soient clairement identifiables en tant que telles et puissent être extraites sur demande.

[44] Voir l'article 5.

[45] Voir l'article 6 et l'article 9.

responsabilité. De toute évidence, si les registres en eux-mêmes ne contiennent pas de données à caractère personnel, le principe de limitation de la conservation[46] du RGPD ne s'applique pas.

Outre ces informations, le G29 recommande que le responsable du traitement documente également le raisonnement justifiant les décisions prises en réaction à la violation. En particulier, lorsqu'une violation n'est pas notifiée, la justification de cette décision devrait être documentée. Cette justification devrait inclure les raisons pour lesquelles le responsable du traitement considère que la violation est peu susceptible d'engendrer un risque pour les droits et libertés des individus[47]. Si le responsable du traitement considère que l'une des conditions visées à l'article 34, paragraphe 3, est remplie, il devrait également pouvoir fournir des éléments de preuve appropriés à cet égard.

Lorsque le responsable du traitement ne notifie pas une violation à l'autorité de contrôle, mais que la notification est retardée, le responsable du traitement doit être en mesure de fournir les raisons d'un tel retard; une documentation à cet égard pourrait contribuer à démontrer que le retard de notification est bien justifié et n'est pas excessif.

Lorsque le responsable du traitement communique une violation aux personnes concernées, il devrait être transparent en ce qui concerne la violation en question et communiquer de façon efficace et en temps utile. Conserver la trace d'une telle communication aiderait ainsi le responsable du traitement à démontrer son respect du principe de responsabilité et du RGPD en général.

Dans le but de favoriser leur conformité avec les articles 33 et 34, il serait bénéfique à la fois pour les responsables du traitement et les sous-traitants de disposer d'une procédure de notification documentée définissant la procédure à suivre lorsqu'une violation est détectée, y compris concernant la façon d'endiguer, de gérer et de remédier à l'incident, d'évaluer le risque et de notifier la violation. À cet égard, toujours afin de prouver leur conformité avec le RGPD, il pourrait être utile de démontrer que les employés ont été informés de l'existence de tels mécanismes et procédures et qu'ils savent comment réagir en cas de violation.

Il convient de noter qu'en cas de manquement à cette obligation de documenter correctement une violation, l'autorité de contrôle pourrait exercer ses pouvoirs au titre de l'article 58 et/ou imposer une amende administrative conformément à l'article 83.

B. Rôle du délégué à la protection des données

Un responsable du traitement ou un sous-traitant peut disposer d'un délégué à la protection des données (DPD)[48] comme exigé à l'article 37 ou sur une base volontaire à titre de bonne pratique. L'article 39 du RGPD définit un certain nombre de tâches obligatoires pour le DPD, mais n'interdit nullement que d'autres tâches lui soient attribuées par le responsable du traitement si nécessaire.

Les tâches imposées au DPD et présentant un intérêt particulier pour la notification des violations comprennent, entre autres, celle d'informer et de conseiller le responsable du traitement ou le sous-traitant en matière de protection des données, de contrôler le respect du RGPD et de dispenser des conseils en ce qui concerne l'AIPD. Le DPD doit également coopérer avec l'autorité de contrôle et faire office de point de contact pour celle-ci ainsi que pour les personnes concernées. Il convient également de noter que, lors de la notification d'une violation à l'autorité de contrôle, l'article 33,

[46] Voir l'article 5, paragraphe 1, point e).

[47] Voir le considérant 85.

[48] Voir les lignes directrices du G29 concernant les DPD à l'adresse suivante: https://www.cnil.fr/sites/default/files/atoms/files/wp243rev01_fr.pdf

paragraphe 3, point b), exige du responsable du traitement qu'il communique le nom et les coordonnées de son DPD ou d'un autre point de contact.

Pour ce qui est de la documentation des violations, le responsable du traitement ou le sous-traitant pourrait solliciter l'avis de son DPD concernant la structure, l'organisation et l'administration d'une telle documentation. Le DPD pourrait également être chargé de tenir de tels registres.

Ces tâches indiquent que le DPD devrait jouer un rôle clé dans la prévention des violations et la préparation à une violation en fournissant des conseils et en contrôlant le respect du RGPD, ainsi que lors d'une telle violation (p. ex. lors de la notification à l'autorité de contrôle) et durant l'enquête subséquente de l'autorité de contrôle. À cet égard, le G29 recommande que le DPD soit rapidement informé de l'existence d'une violation et participe à la gestion et au processus de notification de la violation.

VI. Obligations de notification en vertu d'autres instruments juridiques

Outre la notification et la communication au titre du RGPD, et indépendamment de celles-ci, les responsables du traitement devraient également avoir connaissance de toute obligation de notification d'incidents de sécurité pouvant s'appliquer en vertu d'autres législations associées, ainsi que de la possibilité qu'ils soient ainsi tenus de notifier parallèlement à l'autorité de contrôle une violation de données à caractère personnel. De telles obligations peuvent varier d'un État membre à l'autre. Des exemples d'obligations de notification définies par d'autres instruments juridiques et de la façon dont celles-ci interagissent avec le RGPD peuvent toutefois être trouvés ci-dessous:

- Règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS)[49].

L'article 19, paragraphe 2, du règlement eIDAS exige des prestataires de services de confiance qu'ils notifient à l'organe de contrôle toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées. Le cas échéant – c.-à-d. lorsqu'une telle atteinte ou perte constitue une violation de données à caractère personnel en vertu du RGPD – le prestataire de services de confiance devrait également avertir l'autorité de contrôle.

- Directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive SRI)[50].

Les articles 14 et 16 de la directive SRI exigent des opérateurs de services essentiels et des fournisseurs de service numérique qu'ils notifient tout incident à leur autorité compétente. Le considérant 63 de la directive SRI[51] reconnaît que dans de nombreux cas, des données à caractère personnel peuvent être compromises à la suite d'incidents. Si la directive en question prévoit que les autorités compétentes et les autorités de contrôle coopèrent et échangent des informations dans ce cadre, il n'en reste pas moins que lorsque de tels incidents sont, ou deviennent, des violations de

[49] Voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.FRA

[50] Voir http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.FRA

51 Considérant 63: *«Dans de nombreux cas, des données à caractère personnel sont compromises à la suite d'incidents. Dans de telles circonstances, les autorités compétentes et les autorités chargées de la protection des données devraient coopérer et échanger des informations sur tous les aspects pertinents de la lutte contre toute atteinte aux données à caractère personnel à la suite d'incidents.»*

données à caractère personnel en vertu du RGPD, ces opérateurs et/ou fournisseurs sont tenus d'avertir l'autorité de contrôle indépendamment des exigences de notification des incidents définies par la directive SRI.

Exemple

Un fournisseur de services en nuage qui notifie une violation en vertu de la directive SRI pourrait également devoir la notifier à un responsable du traitement si ladite violation comprend une violation de données à caractère personnel. De la même façon, un prestataire de services de confiance au sens du règlement eIDAS peut également être tenu d'informer l'autorité chargée de la protection des données compétente en cas de violation.

- Directive 2009/136/CE (directive «Droits des citoyens») et règlement (UE) nº 611/2013 (règlement relatif à la notification des violations).

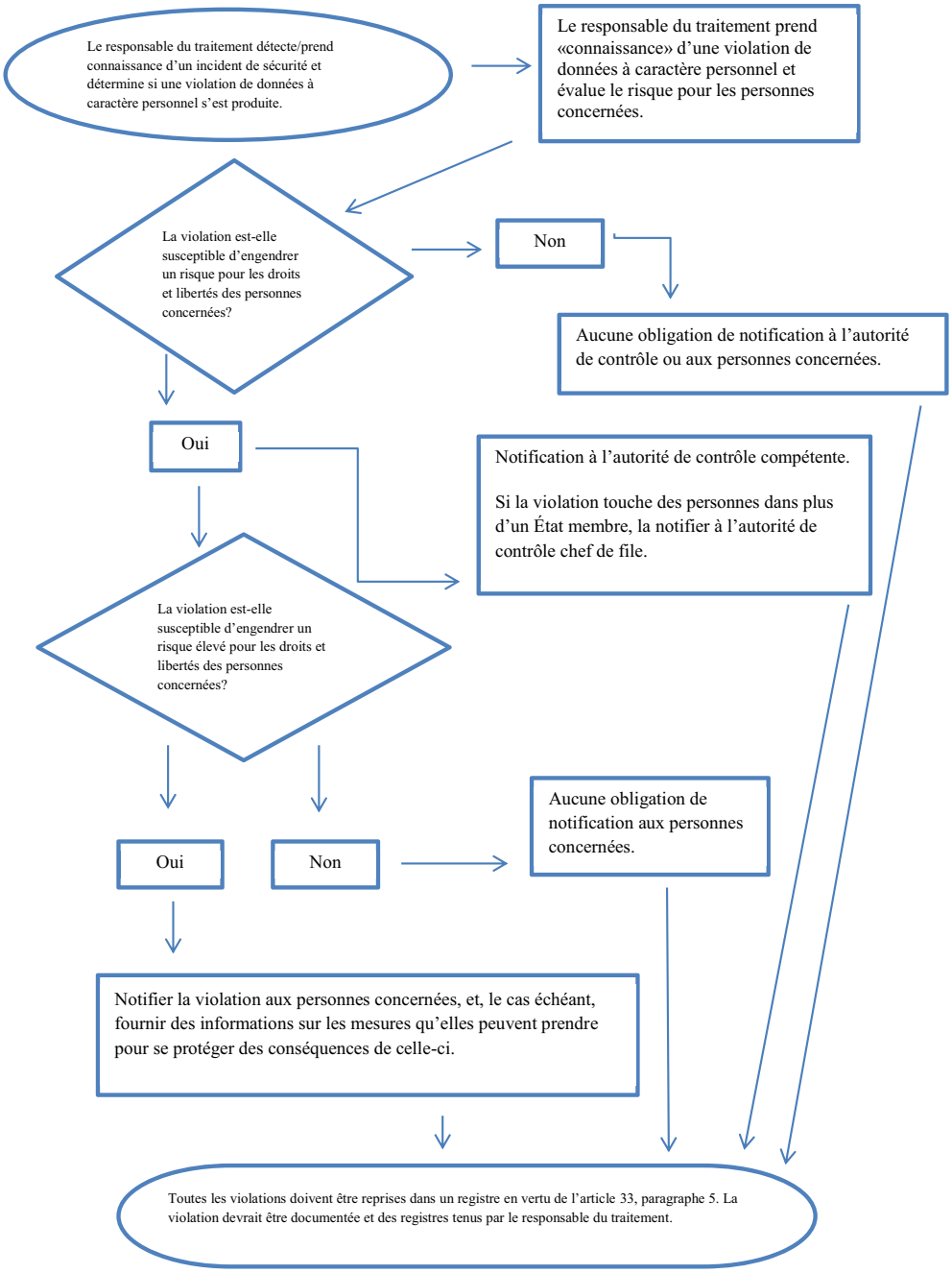
Les fournisseurs de services de communications électroniques accessibles au public au sens de la directive 2002/58/CE[52] sont tenus de notifier les violations aux autorités nationales compétentes.

Les responsables du traitement devraient également avoir connaissance de toute autre obligation de notification juridique, médicale ou professionnelle en vertu d'autres régimes applicables.

[52] Le 10 janvier 2017, la Commission européenne a proposé un règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, qui remplacera la directive 2009/136/CE et supprimera les exigences de notification de celle-ci. Toutefois, tant que la proposition n'est pas approuvée par le Parlement européen, l'actuelle exigence de notification reste en vigueur; voir https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. Annexe

A. Organigramme indiquant les obligations de notification



34

B. Exemples de violations de données à caractère personnel et à qui les notifier

Les exemples suivants, non exhaustifs, aideront les responsables du traitement à déterminer si l'obligation de notification s'applique dans différents cas de violation de données à caractère personnel. Ces exemples peuvent également aider à distinguer un risque d'un risque élevé pour les droits et libertés des personnes concernées.

Exemple	**Notifier la violation à l'autorité de contrôle?**	**Notifier la violation aux personnes concernées?**	**Notes/recommandations**
i. Un responsable du traitement a stocké une sauvegarde d'une archive de données à caractère personnel cryptées sur une clé USB. La clé est volée lors d'un cambriolage.	Non	Non	Tant que les données sont cryptées à l'aide d'un algorithme de pointe, que des sauvegardes des données existent, que la clé unique n'est pas compromise et que les données peuvent être restaurées en temps utile, cette violation peut ne pas devoir être notifiée. Si les données sont en revanche ultérieurement compromises, la notification est nécessaire.
ii. Un responsable du traitement assure un service en ligne. À la suite d'une cyberattaque sur ce service, des données à caractère personnel de personnes physiques en sont soutirées. Le responsable du traitement n'a de clients que dans un seul État membre.	Oui, avertir l'autorité de contrôle en cas de conséquences probables pour les personnes concernées.	Oui, avertir les personnes concernées en fonction de la nature des données à caractère personnel concernées et si la gravité des conséquences probables pour celles-ci est élevée.	
iii. Une courte panne de courant de quelques minutes dans le centre d'appel d'un responsable du traitement empêche les clients d'appeler ce dernier et d'accéder à leurs dossiers.	Non	Non	Pas d'obligation de notifier la violation, mais l'incident doit être documenté en vertu de l'article 33, paragraphe 5. Des registres appropriés devraient être tenus par le responsable du traitement.

35

iv. Un responsable du traitement est victime d'une cyberattaque au moyen d'un rançongiciel qui crypte toutes ses données. Aucune sauvegarde n'est disponible et les données ne peuvent pas être restaurées. L'enquête révèle que la seule fonctionnalité du rançongiciel était de crypter les données et qu'aucun autre programme malveillant n'est présent dans le système.	Oui, avertir l'autorité de contrôle en cas de conséquences probables pour les personnes concernées, dès lors qu'il s'agit d'une perte de disponibilité.	Oui, avertir les personnes concernées en fonction de la nature des données à caractère personnel concernées et des conséquences potentielles de la perte de disponibilité des données, ainsi que des autres conséquences probables.	Si une sauvegarde avait été disponible et si les données avaient pu être restaurées en temps utile, il n'aurait pas été nécessaire de notifier la violation à l'autorité de contrôle ou aux personnes concernées dès lors qu'il n'y aurait pas eu de perte permanente de la disponibilité ou de la confidentialité. Toutefois, si l'autorité de contrôle prenait connaissance de l'incident par d'autres moyens, elle pourrait envisager de procéder à une enquête afin d'évaluer le respect des exigences de sécurité plus générales de l'article 32.
v. Une personne appelle le centre d'appel d'une banque pour signaler une violation de données. La personne en question a reçu le relevé mensuel d'une autre personne. Le responsable du traitement procède à une courte enquête (c.-à-d. terminée sous 24 heures), établit, avec un degré de certitude raisonnable, qu'une violation de données à caractère personnel s'est produite et signale l'existence potentielle d'un défaut systémique impliquant que d'autres personnes sont ou pourraient être affectées.	Oui	Seules les personnes concernées sont informées en cas de risque élevé et s'il est évident qu'aucune autre personne n'a été affectée.	Si, après une enquête complémentaire, on s'aperçoit que davantage de personnes sont concernées, il convient de notifier cette évolution à l'autorité de contrôle et de prendre des mesures complémentaires afin d'informer les autres personnes concernées en cas de risque élevé pour celles-ci.

vi. Un responsable du traitement gère un marché en ligne et a des clients dans plusieurs États membres. Le marché en question est victime d'une cyberattaque et les noms d'utilisateur, les mots de passe et les historiques d'achat sont publiés en ligne par le pirate.	Oui, informer l'autorité de contrôle chef de file si l'attaque concerne un traitement transfrontalier.	Oui, dès lors que l'attaque pourrait engendrer un risque élevé.	Le responsable devrait prendre des mesures, p. ex. en forçant la réinitialisation des mots de passe des comptes touchés, ainsi que d'autres mesures pour limiter le risque. Le responsable du traitement devrait également tenir compte d'autres obligations de notification, p. ex. en vertu de la directive SRI en tant que fournisseur de service numérique.
vii. Une entreprise d'hébergement de sites internet agissant en tant que sous-traitant détecte une erreur dans le code qui contrôle l'autorisation utilisateur. En raison de ce défaut, n'importe quel utilisateur peut accéder aux informations de compte de n'importe quel autre utilisateur.	En tant que sous-traitant, l'entreprise d'hébergement de sites internet doit avertir les clients concernés (les responsables du traitement) dans les meilleurs délais. En partant du principe que l'entreprise d'hébergement de sites internet a mené sa propre enquête, les responsables du traitement concernés devraient être relativement certains de l'occurrence éventuelle d'une violation, et ils seront probablement considérés comme ayant «pris connaissance» une fois que l'entreprise d'hébergement (le sous-traitant) les en aura informés. Le responsable du traitement doit alors informer l'autorité de contrôle.	Si la violation est peu susceptible d'entraîner un risque élevé pour les personnes concernées, il ne sera pas nécessaire de la leur notifier.	L'entreprise d'hébergement de sites internet (sous-traitant) doit également tenir compte d'autres obligations de notification (p. ex. en vertu de la directive SRI en tant que fournisseur de service numérique). S'il n'existe aucune preuve que cette vulnérabilité a été exploitée chez l'un des responsables du traitement de l'entreprise, il se pourrait que l'incident ne soit pas soumis à l'obligation de notification, mais il est probable qu'il doive être documenté ou qu'il soit le signe d'une non-conformité à l'article 32.

37

viii. Une cyberattaque rend indisponibles les dossiers médicaux d'un hôpital pendant 30 heures.	Oui, l'hôpital est tenu de le signaler à l'autorité de contrôle dès lors qu'un risque élevé pour le bien-être des patients et leur vie privée pourrait en résulter.	Oui, informer les personnes concernées.	
ix. Des données à caractère personnel d'un grand nombre d'étudiants sont envoyées par erreur à une mauvaise liste d'adresses contenant plus de 1 000 destinataires.	Oui, avertir l'autorité de contrôle.	Oui, avertir les personnes concernées en fonction de la portée et du type de données à caractère personnel concernées ainsi que de la gravité des conséquences potentielles.	
x. Un courrier électronique de marketing direct est envoyé aux destinataires dans les champs «à:» ou «cc:», permettant ainsi à chaque destinataire de voir l'adresse électronique des autres destinataires.	Oui, il pourrait être obligatoire de le notifier à l'autorité de contrôle si un grand nombre de personnes sont touchées, si des données sensibles sont révélées (p. ex. une liste d'adresses de patients d'un psychothérapeute) ou si d'autres facteurs présentent des risques élevés (p. ex. le courrier électronique contient les mots de passe initiaux).	Oui, avertir les personnes concernées en fonction de la portée et du type de données à caractère personnel concernées ainsi que de la gravité des conséquences potentielles.	La notification pourrait ne pas être nécessaire si aucune donnée sensible n'est révélée et si seul un nombre limité d'adresses électroniques a été divulgué.

Lignes directrices sur la prise de décision individuelle automatisée et sur le profilage (WP251)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP251rev.01

Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679

Adoptées le 3 octobre 2017

Version révisée et adoptée le 6 février 2018

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

TABLE DES MATIERES

I. Introduction

Le règlement général sur la protection des données (RGPD) traite spécifiquement du profilage et de la prise de décision individuelle automatisée, y compris le profilage[1].

Le profilage et la prise de décision automatisée sont utilisés dans un nombre croissant de secteurs, tant privés que publics. La banque et la finance, la santé, la fiscalité, les assurances, la prospection et la publicité ne sont que quelques exemples de domaines où le profilage est régulièrement effectué pour faciliter la prise de décision.

Les progrès technologiques et les capacités en matière d'analyse de mégdonnées , d'intelligence artificielle et d'apprentissage automatique ont facilité la création de profils et la prise de décisions automatisées susceptibles d'avoir une incidence significative sur les droits et les libertés de chacun.

La disponibilité généralisée de données à caractère personnel sur internet et à partir de dispositifs IdO (internet des objets), et la capacité de trouver des corrélations et de créer des liens peuvent permettre de déterminer, d'analyser et de prédire des aspects de la personnalité, du comportement, des intérêts et des habitudes d'une personne.

Le profilage et la prise de décision automatisée peuvent être utiles pour les particuliers et les organisations, offrant des avantages tels que:

- une efficacité accrue; et
- des économies de ressources.

Ils présentent de nombreuses possibilités d'applications commerciales. Par exemple, ils peuvent être utilisés pour mieux segmenter les marchés et adapter les services et les produits aux besoins de chacun. La médecine, l'éducation, les soins de santé et les transports peuvent également tirer profit de ces processus.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1–88). Le profilage et la prise de décision individuelle automatisée sont également couverts par la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données. Bien que les présentes lignes directrices se concentrent sur le profilage et la prise de décision individuelle automatisée dans le cadre du RGPD, les orientations qu'elles fournissent sont également pertinentes en ce qui concerne les deux thèmes de la directive (UE) 2016/680, pour ce qui est des dispositions similaires au RGPD. L'analyse des caractéristiques spécifiques du profilage et de la prise de décision individuelle automatisée dans le cadre de la directive (UE) 2016/680 n'est pas incluse dans les présentes lignes directrices, puisque l'avis WP258 sur certaines questions clés de la directive (UE) 2016/680 (directive «police») [«Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)»], adopté par le groupe de travail «article 29» (GT29) le 29 novembre 2017, fournit des orientations à cet égard. Cet avis couvre la prise de décision individuelle automatisée et le profilage dans le contexte du traitement des données par les services répressifs aux pages 11 à 14 et est disponible à l'adresse suivante: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178.

Cependant, le profilage et la prise de décision automatisée peuvent poser des risques importants pour les droits et libertés des personnes, qui nécessitent alors des garanties appropriées.

Ces processus peuvent être opaques. Il se peut que les particuliers ne sachent pas qu'ils font l'objet d'un profilage ou qu'ils ne comprennent pas ce que cela implique.

Le profilage peut perpétuer les stéréotypes existants et la ségrégation sociale. Il peut aussi enfermer des personnes dans une catégorie spécifique et les limiter aux préférences qui leur sont suggérées. Cela peut porter atteinte à leur liberté de choix en ce qui concerne, par exemple, certains produits ou services tels que des livres, de la musique ou des fils d'actualités. Dans certains cas, le profilage peut donner lieu à des prévisions inexactes. Dans d'autres cas, il peut conduire à un déni de services et de biens et à une discrimination injustifiée.

Le RGPD introduit de nouvelles dispositions qui permettent de faire face aux risques découlant du profilage et de la prise de décision automatisée, notamment, mais sans s'y limiter, en ce qui concerne la protection de la vie privée. Les présentes lignes directrices ont pour but de clarifier ces dispositions.

Le document couvre les aspects suivants:

- définitions du profilage et de la prise de décision automatisée, et de l'approche du RGPD dans ces domaines en général – chapitre II
- dispositions générales sur le profilage et la prise de décision automatisée – chapitre III
- dispositions spécifiques concernant la prise de décision exclusivement automatisée définie à l'article 22 – chapitre IV
- enfants et profilage – chapitre V
- analyses d'impact relatives à la protection des données et délégués à la protection des données – chapitre VI

Les annexes contiennent des recommandations sur les bonnes pratiques, en s'appuyant sur l'expérience acquise dans les États membres de l'Union européenne.

Le groupe de travail «article 29» sur la protection des données (GT29) contrôlera la mise en œuvre des présentes lignes directrices et pourra les compléter s'il y a lieu.

II. Définitions

Le RGPD introduit des dispositions visant à garantir que le profilage et la prise de décision individuelle automatisée (qu'il s'agisse ou non de profilage) ne sont pas utilisés de manière à avoir des répercussions injustifiées sur les droits des personnes; par exemple:

- des exigences particulières en matière de transparence et de loyauté;
- des obligations accrues en matière de responsabilité;
- des bases juridiques spécifiées pour le traitement;
- le droit pour les particuliers de s'opposer au profilage et plus particulièrement au profilage à des fins de prospection; et
- si certaines conditions sont remplies, la nécessité de réaliser une analyse d'impact relative à la protection des données.

Le RGPD ne se concentre pas seulement sur les décisions prises à la suite d'un traitement automatisé ou d'un profilage. Il s'applique à la collecte de données pour la création de profils, ainsi qu'à l'application de ces profils aux particuliers.

A. Profilage

Dans son article 4, paragraphe 4, le RGPD définit le profilage comme:

> toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

Le profilage est composé de trois éléments:

- il doit s'agir d'une forme de traitement *automatisé*;
- il doit être effectué sur des *données à caractère personnel*; et
- l'objectif du profilage doit être d'*évaluer les aspects personnels* d'une personne physique.

L'article 4, paragraphe 4, fait référence à «toute forme de traitement automatisé» plutôt qu'à un traitement «exclusivement» automatisé (visé à l'article 22). Le profilage doit impliquer une certaine forme de traitement automatisé – bien que la participation humaine n'exclue pas nécessairement l'activité de la définition.

Le profilage est une procédure qui peut comporter une série de déductions statistiques. Il est souvent utilisé pour faire des prédictions au sujet des gens, en utilisant des données provenant de diverses sources pour déduire quelque chose sur une personne, en se fondant sur les qualités d'autres personnes qui semblent similaires sur le plan statistique.

Selon le RGPD, le profilage est un traitement automatisé de données à caractère personnel pour évaluer des aspects personnels, en particulier pour analyser *ou* faire des prédictions sur les particuliers. L'utilisation du mot «évaluer» suggère que le profilage implique une certaine forme d'appréciation ou de jugement à l'égard d'une personne.

Une simple classification des personnes en fonction de caractéristiques connues comme l'âge, le sexe et la taille ne conduit pas nécessairement au profilage. Cela dépendra de l'objectif de la classification. Par exemple, une entreprise peut souhaiter classer ses clients en fonction de leur âge ou de leur sexe à des fins statistiques et acquérir une vue d'ensemble de ses clients sans faire de prédictions ou tirer de conclusions au sujet d'une personne en particulier. Dans ce cas, le but n'est pas d'évaluer les caractéristiques individuelles et cela ne constitue donc pas du profilage.

Le RGPD s'inspire de la définition du profilage figurant dans la recommandation CM/Rec(2010)13[2] du Conseil de l'Europe (ci-après la «Recommandation»), mais n'est pas identique à celle-ci, étant donné que la Recommandation *exclut* les traitements qui ne comprennent pas d'inférence. Néanmoins, la Recommandation explique utilement que le profilage peut comporter trois étapes distinctes:

- une collecte de données;
- une analyse automatisée afin d'établir des corrélations;

[2] Conseil de l'Europe. La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage. Recommandation CM/Rec(2010)13 et exposé des motifs. Conseil de l'Europe, 23 novembre 2010. https://www.coe.int/t/dghl/standardsetting/cdcj/CDCJ%20Recommendations/CMRec(2010)13E_Profiling.pdf . Document consulté le 24 avril 2017.

- l'application de la corrélation à une personne pour déduire les caractéristiques du comportement actuel ou futur.

Les responsables du traitement qui effectuent le profilage devront s'assurer qu'ils satisfont aux exigences du RGPD lors de toutes les étapes susmentionnées.

D'une manière générale, le profilage consiste à recueillir des informations sur une personne (ou un groupe de personnes) et à évaluer leurs caractéristiques ou leurs comportements afin de les placer dans une certaine catégorie ou un certain groupe, notamment pour analyser et/ou faire des prédictions sur, par exemple:

- leur capacité à effectuer une tâche;
- leurs intérêts; ou
- leur comportement probable.

Exemple

Un courtier de données recueille des données auprès de différentes sources publiques et privées, soit pour le compte de ses clients, soit pour ses propres besoins. Il compile les données pour établir des profils sur les personnes concernées et les place dans des segments. Il vend ces informations aux entreprises qui souhaitent améliorer le ciblage de leurs biens et services. Le courtier de données effectue un profilage en plaçant une personne dans une certaine catégorie en fonction de ses intérêts.

L'existence ou non d'une décision individuelle automatisée, telle que définie à l'article 22, paragraphe 1, dépendra des circonstances.

B. Prise de décision automatisée

La prise de décision automatisée a une portée différente et peut partiellement chevaucher le profilage ou en résulter. La prise de décision exclusivement automatisée est la capacité de prendre des décisions par des moyens technologiques sans intervention humaine. Les décisions automatisées peuvent être fondées sur n'importe quel type de données, par exemple:

- les données fournies directement par les personnes concernées (comme les réponses à un questionnaire);
- les données observées au sujet des personnes (comme les données de localisation recueillies par l'intermédiaire d'une application);
- des données dérivées ou inférées, comme un profil de la personne qui a déjà été créé (p. ex. une cote de solvabilité).

Les décisions automatisées peuvent être prises avec ou sans profilage; le profilage peut se faire sans prendre de décisions automatisées. Toutefois, le profilage et la prise de décision automatisée ne sont pas nécessairement des activités distinctes. Quelque chose qui commence comme un simple processus décisionnel automatisé pourrait devenir un processus fondé sur le profilage, selon la façon dont les données sont utilisées.

Exemple

Imposer des amendes pour excès de vitesse sur la seule base des preuves fournies par les radars est un processus décisionnel automatisé qui n'implique pas nécessairement un profilage.

Toutefois, la décision serait fondée sur le profilage si les habitudes de la personne concernée au volant étaient surveillées au fil du temps. Par exemple, si le montant de l'amende infligée est le résultat d'une évaluation faisant intervenir d'autres facteurs, comme le fait de savoir si l'excès de vitesse est une récidive ou si le conducteur a commis récemment d'autres infractions au code de la route.

Les décisions qui ne sont pas exclusivement automatisées peuvent également inclure un profilage. Par exemple, avant d'accorder une hypothèque, une banque peut tenir compte de la cote de solvabilité de l'emprunteur, avec une intervention significative supplémentaire effectuée par des humains avant que toute décision ne soit appliquée à un individu.

C. Manière dont le RGPD aborde les concepts

Le profilage peut être utilisé de trois façons différentes:

i) un profilage général;
ii) une prise de décision fondée sur le profilage; et
iii) une prise de décision *exclusivement* automatisée, y compris le profilage, qui produit des effets juridiques ou affecte de manière significative de façon similaire la personne concernée (article 22, paragraphe 1).

La différence entre les points ii) et iii) est mieux illustrée par les deux exemples suivants présentant le cas d'une personne qui fait une demande de prêt en ligne:

- un être humain décide s'il accorde ou non le prêt sur la base d'un profil produit par des moyens purement automatisés (ii);
- un algorithme décide si le prêt est accordé et la décision est automatiquement transmise à la personne concernée, sans évaluation préalable et significative par un être humain (iii).

Les responsables du traitement peuvent effectuer un profilage et recourir à une prise de décision automatisée à condition de respecter tous les principes et de disposer d'une base légale pour le traitement. Des garanties et restrictions supplémentaires s'appliquent dans le cas d'une prise de décision exclusivement automatisée, y compris le profilage, visée à l'article 22, paragraphe 1.

Le chapitre III des présentes lignes directrices explique les dispositions du RGPD pour *tous* les profilages et *toutes* les prises de décisions individuelles automatisées. Cela comprend les processus décisionnels qui ne sont *pas* exclusivement automatisés.

Le chapitre IV des présentes lignes directrices explique les dispositions spécifiques qui *ne s'appliquent qu'à* la prise de décision individuelle automatisée, y compris le profilage[3]. Il existe une interdiction générale de ce type de traitement afin de tenir compte des risques potentiels pour les droits et les libertés des personnes.

[3] Telle que définie à l'article 22, paragraphe 1, du RGPD.

III. Dispositions générales sur le profilage et la prise de décision automatisée

Cet aperçu des dispositions s'applique à tous les profilages et à toutes les prises de décisions automatisées. Les dispositions spécifiques supplémentaires énoncées au chapitre IV s'appliquent si le traitement correspond à la définition de l'article 22, paragraphe 1.

A. Principes de la protection des données

Ces principes s'appliquent à tous les profilages et toutes les décisions automatisées concernant des données à caractère personnel[4]. Afin de garantir la conformité, les responsables du traitement doivent prendre en considération les éléments clés suivants:

1. Article 5, paragraphe 1, point a) - Licéité, loyauté et transparence

La transparence du traitement[5] est une exigence fondamentale du RGPD.

Le processus de profilage est souvent invisible pour la personne concernée. Il fonctionne en créant des données dérivées ou déduites sur les individus, c'est-à-dire de «nouvelles» données à caractère personnel qui n'ont pas été fournies directement par les personnes concernées elles-mêmes. Chacun possède un niveau de compréhension différent et pour certains, il peut être difficile de comprendre les techniques complexes intervenant dans le profilage et les processus décisionnels automatisés.

En vertu de l'article 12, paragraphe 1, le responsable du traitement doit fournir toute information concernant le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible[6].

Pour les données collectées directement auprès de la personne concernée, ces informations doivent être fournies au moment de la collecte (article 13); pour les données obtenues indirectement, les informations doivent être fournies dans les délais prévus à l'article 14, paragraphe 3.

Exemple

Certains assureurs proposent des tarifs et des services fondés sur le comportement au volant d'une personne. Les éléments pris en considération dans ces cas pourraient inclure la distance parcourue, le

[4] RGPD – Considérant 72 «Le profilage est soumis aux règles du présent règlement régissant le traitement des données à caractère personnel, par exemple le fondement juridique du traitement ou les principes en matière de protection des données.»

[5] Les lignes directrices du groupe de travail «article 29» sur la transparence couvrent de manière plus détaillée la transparence en général; voir les lignes directrices sur la transparence au titre du règlement (UE) 2016/679 (Guidelines on transparency under Regulation 2016/679) (wp260rev.01), 11 avril 2018http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[6] Bureau du Commissaire à l'information de l'Australie. Projet de consultation: le guide des mégadonnées et des principes australiens de protection de la vie privée (Guide to big data and the Australian Privacy Principles, 05/2016) dispose ce qui suit: «Les déclarations de confidentialité doivent communiquer les pratiques de traitement de l'information de façon claire et simple, mais aussi de façon exhaustive et suffisamment précise pour être bien comprises. *La technologie même qui permet une plus grande collecte de renseignements personnels offre également la possibilité de formuler des déclarations de confidentialité plus dynamiques, à plusieurs niveaux et axés sur l'utilisateur*». https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles. Document consulté le 24 avril 2017.

temps de conduite et le trajet suivi, ainsi que des prédictions fondées sur d'autres données recueillies par les capteurs dans une voiture (intelligente). Les données recueillies sont utilisées pour le profilage afin d'identifier les mauvais comportements au volant (accélération rapide, freinage brusque et excès de vitesse). Ces informations peuvent être recoupées avec d'autres sources (par exemple la météo, la circulation, le type de route) pour mieux comprendre le comportement du conducteur.

Le responsable du traitement doit s'assurer qu'il dispose d'une base légale pour ce type de traitement. Il doit également fournir à la personne concernée des informations sur les données collectées et, s'il y a lieu, sur l'existence d'une prise de décision automatisée visée à l'article 22, paragraphes 1 et 4, sur la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Les exigences spécifiques relatives à l'information et à l'accès aux données à caractère personnel sont examinées aux chapitres III (section D) et IV (section E).

Le traitement doit également être loyal et transparent.

Le profilage peut être déloyal et créer de la discrimination, par exemple en refusant aux personnes l'accès à un emploi, à un crédit ou à une assurance, ou en les ciblant avec des produits financiers excessivement risqués ou coûteux. L'exemple suivant, qui ne satisferait pas aux exigences de l'article 5, paragraphe 1, point a), illustre comment le profilage déloyal peut conduire à ce que certains consommateurs se voient proposer des offres moins attractives que d'autres.

Exemple

Un courtier de données vend à des sociétés financières des profils de consommateurs sans le consentement de ceux-ci ou sans connaître les données sous-jacentes. Les profils classent les consommateurs en catégories (avec des qualificatifs tels que «profil rural ayant du mal à joindre les deux bouts», «difficultés en milieu urbain-profil ethnique de deuxième génération», «débuts difficiles: jeunes parents célibataires») ou une «note», en mettant l'accent sur la vulnérabilité financière des consommateurs. Les sociétés financières proposent à ces consommateurs des prêts sur salaire et d'autres services financiers «non traditionnels» (prêts à taux élevé et autres produits financièrement risqués)[7].

2. Article 5, paragraphe 1, point b) – Traitement ultérieur et limitation des finalités

Le profilage peut impliquer l'utilisation de données à caractère personnel qui ont été collectées à l'origine à d'autres fins.

[7] Cet exemple est tiré de: Sénat des États-Unis, Comité du commerce, des sciences et des transports. Examen du secteur des courtiers de données: collecte, utilisation et vente de données sur les consommateurs à des fins de marketing (A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes), rapport du personnel pour le président Rockefeller, 18 décembre 2013. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf . Voir page ii du résumé et page 12 du corps du document en particulier. Document consulté le 21 juillet 2017.

Exemple

Certaines applications mobiles fournissent des services de localisation permettant à l'utilisateur de trouver des restaurants offrant des rabais à proximité de sa position. Toutefois, les données recueillies sont également utilisées pour établir un profil de la personne concernée à des fins de prospection – pour déterminer ses préférences alimentaires ou son mode de vie en général. La personne concernée s'attend à ce que ses données soient utilisées pour trouver des restaurants, mais pas pour recevoir des publicités pour la livraison de pizzas simplement parce que l'application a déterminé qu'elle rentre tard à la maison. Cette utilisation ultérieure des données de localisation peut ne pas être compatible avec les finalités pour lesquelles elles ont été collectées initialement et peut donc nécessiter le consentement de la personne concernée[8].

La compatibilité de ce traitement supplémentaire avec les finalités initiales pour lesquelles les données ont été collectées dépendra d'une série de facteurs[9], y compris les informations que le responsable du traitement a initialement fournies à la personne concernée. Ces facteurs sont reflétés dans le RGPD[10] et résumés ci-dessous:

- le lien entre les finalités pour lesquelles les données ont été collectées et les finalités du traitement ultérieur;
- le contexte dans lequel les données à caractère personnel ont été collectées et les attentes raisonnables des personnes concernées quant à leur utilisation ultérieure;
- la nature des données;
- l'impact du traitement ultérieur sur les personnes concernées; et
- les garanties appliquées par le responsable du traitement afin d'assurer un traitement loyal et d'éviter tout impact indu sur les personnes concernées.

3. Article 5, paragraphe 1, point c) – Minimisation des données

Les possibilités commerciales engendrées par le profilage, les coûts de stockage moins élevés et la capacité de traiter de grandes quantités d'informations peuvent encourager les organisations à collecter plus de données à caractère personnel qu'elles n'en ont réellement besoin, au cas où cela s'avérerait utile pour l'avenir. Les responsables du traitement doivent s'assurer qu'ils respectent le principe de minimisation des données, ainsi que les exigences des principes de limitation des finalités et de limitation de la durée de conservation.

Ils devraient être en mesure d'expliquer et de justifier clairement la nécessité de collecter et de conserver des données à caractère personnel, ou d'envisager d'utiliser des données agrégées, anonymisées ou (lorsque cela garantit une protection suffisante) pseudonymisées pour le profilage.

4. Article 5, paragraphe 1, point d) – Exactitude

[8] Il convient de noter que les dispositions du futur règlement «vie privée et communications électroniques» peuvent également s'appliquer.

[9] Comme souligné par le groupe de travail «article 29» sur la protection des données. Avis 03/2013 sur la limitation des finalités, 2 avril 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf . Document consulté le 24 avril 2017.

[10] Article 6, paragraphe 4, du RGPD.

Les responsables du traitement devraient tenir compte de l'exactitude à toutes les étapes du processus de profilage, en particulier lors de:

- la collecte de données;
- l'analyse des données;
- l'établissement du profil d'une personne; ou
- l'application d'un profil pour prendre une décision affectant la personne.

Si les données utilisées dans un processus automatisé de prise de décision ou de profilage sont inexactes, toute décision ou tout profil qui en résulte sera erroné. Les décisions peuvent être prises sur la base de données dépassées ou d'une interprétation incorrecte de données externes. Des inexactitudes peuvent conduire à des prédictions ou des déclarations inappropriées concernant, par exemple, le risque de santé, de crédit ou d'assurance d'une personne.

Même si les données brutes sont enregistrées avec exactitude, l'ensemble de données peut ne pas être entièrement représentatif ou les analyses peuvent contenir des biais cachés.

Les responsables du traitement doivent mettre en place des mesures solides pour vérifier et s'assurer en permanence que les données réutilisées ou obtenues indirectement sont exactes et à jour. Cela renforce l'importance de fournir des informations claires sur les données à caractère personnel traitées, afin que la personne concernée puisse corriger toute inexactitude et améliorer la qualité des données.

5. Article 5, paragraphe 1, point e) – Limitation de la conservation

Les algorithmes d'apprentissage automatique sont conçus pour traiter de grands volumes d'informations et établir des corrélations qui permettent aux organisations de produire des profils très complets et intimes des individus. Bien qu'il puisse y avoir des avantages à conserver les données dans le cas du profilage, puisqu'il y aura plus de données dont l'algorithme pourra s'inspirer, les responsables du traitement doivent respecter le principe de minimisation des données lorsqu'ils collectent des données à caractère personnel et veiller à ce qu'ils ne conservent ces données à caractère personnel que le temps nécessaire et proportionné aux finalités pour lesquelles ces données sont traitées.

La politique de conservation du responsable du traitement devrait tenir compte des droits et libertés des personnes concernées, conformément aux exigences de l'article 5, paragraphe 1, point e).

Le responsable du traitement doit également s'assurer que les données restent à jour tout au long de la période de conservation afin de réduire le risque d'inexactitudes[11].

B. Bases légales du traitement

La prise de décision automatisée visée à l'article 22, paragraphe 1, n'est autorisée que si l'une des exceptions décrites au chapitre IV (sections C et D) s'applique. Les bases légales suivantes applicables au traitement sont pertinentes pour tous les autres profilages et décisions individuelles automatisées.

1. Article 6, paragraphe 1, point a) – Consentement

[11] Autorité norvégienne de protection des données. La grande course aux données – Comment l'utilisation commerciale des données à caractère personnel remet en question la protection de la vie privée (The Great Data Race - How commercial use of personal data challenges privacy), rapport, novembre 2015. Datatilsynet https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/ Document consulté le 24 avril 2017.

Le consentement comme base du traitement est traité de manière générale dans les lignes directrices du GT29 sur le consentement[12]. Le consentement explicite est l'une des exceptions à l'interdiction de la prise de décision et du profilage automatisés définis à l'article 22, paragraphe 1.

Le profilage peut être opaque. Il s'appuie souvent sur des données dérivées ou déduites d'autres données, plutôt que sur des données fournies directement par la personne concernée.

Les responsables du traitement qui cherchent à se fonder sur le consentement pour procéder à un profilage devront démontrer que les personnes concernées comprennent exactement ce à quoi elles consentent, et se rappeler que le consentement n'est pas toujours une base appropriée pour le traitement[13]. Dans tous les cas, les personnes concernées devraient disposer de suffisamment d'informations pertinentes sur l'utilisation envisagée et les conséquences du traitement pour garantir que leur consentement représente un choix éclairé.

2. Article 6, paragraphe 1, point b – Nécessaire à l'exécution d'un contrat

Les responsables du traitement peuvent souhaiter utiliser le profilage et les processus décisionnels automatisés parce qu'ils:

- permettent une plus grande cohérence ou loyauté dans le processus de prise de décision (p. ex. en réduisant le risque d'erreur humaine, de discrimination et d'abus de pouvoir);
- réduisent le risque que les clients ne règlent pas les paiements pour des biens ou des services (par exemple en utilisant le référencement du crédit); ou
- leur permettent de prendre des décisions dans des délais plus courts et d'améliorer leur efficacité.

Indépendamment de ce qui précède, ces seules considérations ne suffisent pas à démontrer que ce type de traitement est *nécessaire* à l'exécution d'un contrat, en vertu de l'article 6, paragraphe 1, point b). Comme décrit dans l'avis du GT29 sur l'intérêt légitime[14], la nécessité doit être interprétée de manière restrictive.

Voici un exemple de profilage qui ne répondrait pas à la base de l'article 6, paragraphe 1, point b) pour le traitement.

Exemple

Un utilisateur achète des articles auprès d'un détaillant en ligne. Afin d'exécuter le contrat, le détaillant doit traiter les informations relatives à la carte de crédit de l'utilisateur à des fins de

[12] Groupe de travail «article 29» sur la protection des données. Lignes directrices sur le consentement au titre du règlement (UE) 2016/679 (Guidelines on Consent under Regulation 2016/679), WP259, 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Document consulté le 18 décembre 2017.

[13] Ibid.

[14] Avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE. Commission européenne, 9 avril 2014 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf. Document consulté le 24 avril 2017.

paiement et l'adresse de l'utilisateur pour livrer les marchandises. L'exécution du contrat ne dépend pas de l'établissement d'un profil des goûts et des choix de style de vie de l'utilisateur en fonction de ses visites sur le site web. Même si le profilage est spécifiquement mentionné dans les petits caractères du contrat, ce seul fait ne le rend pas «nécessaire» à l'exécution du contrat.

3. Article 6, paragraphe 1, point c) – Nécessaire au respect d'une obligation légale

Il peut se produire des cas où il y aura une obligation légale d'effectuer un profilage[15] – par exemple dans le cadre de la prévention de la fraude ou du blanchiment d'argent. L'avis du GT29 sur les intérêts légitimes[16] fournit des informations utiles sur cette base de traitement, y compris les garanties à appliquer.

4. Article 6, paragraphe 1, point d) – Nécessaire à la sauvegarde des intérêts vitaux

Cela couvre les situations dans lesquelles le traitement est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique.

Certains types de traitement peuvent servir des raisons importantes d'intérêt public ainsi que les intérêts vitaux de la personne concernée. Il peut s'agir, par exemple, du profilage nécessaire pour mettre au point des modèles permettant de prédire la propagation de maladies potentiellement mortelles ou dans des situations d'urgence humanitaire. Dans ces cas, toutefois, et en principe, le responsable du traitement ne peut se fonder sur des raisons d'intérêt vital que si aucune autre base juridique n'est disponible pour le traitement[17]. Si le traitement concerne des données à caractère personnel d'une catégorie particulière, le responsable du traitement devrait également s'assurer qu'elles satisfont aux exigences de l'article 9, paragraphe 2, point c).

5. Article 6, paragraphe 1, point e) – Nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

L'article 6, paragraphe 1, point e), pourrait constituer une base appropriée pour le profilage du secteur public dans certaines circonstances. La tâche ou la fonction doit avoir une base juridique claire.

6. Article 6, paragraphe 1, point f) – Nécessaire aux fins des intérêts légitimes[18] poursuivis par le responsable du traitement ou par un tiers

Le profilage est autorisé s'il est nécessaire aux fins des intérêts légitimes[19] poursuivis par le responsable du traitement ou par un tiers. Toutefois, l'article 6, paragraphe 1, point f), ne s'applique pas automatiquement au seul motif que le responsable du traitement ou un tiers a un intérêt légitime.

---

15 Considérants 41 et 45 du RGPD.

16 Page 19 de l'avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, groupe de travail «article 29» sur la protection des données. Commission européenne, 9 avril 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf. Document consulté le 24 avril 2017.

17 Considérant 46 du RGPD.

18 Les intérêts légitimes énumérés au considérant 47 du RGPD comprennent le traitement à des fins de prospection et le traitement strictement nécessaire à des fins de prévention de la fraude.

19 L'«intérêt légitime» du responsable du traitement ne peut pas rendre le profilage licite si le traitement relève de la définition de l'article 22, paragraphe 1.

Le responsable du traitement doit procéder à une mise en balance afin de déterminer si les intérêts ou les droits et libertés fondamentaux de la personne concernée prévalent sur ses propres intérêts.

Les éléments suivants sont particulièrement importants:

- le niveau de détail du profil (une personne concernée faisant l'objet d'un profil au sein d'une cohorte au sens large, comme les «personnes ayant un intérêt pour la littérature anglaise», ou segmentée et ciblée à un niveau granulaire);
- l'exhaustivité du profil (que le profil ne décrive qu'un petit aspect de la personne concernée ou qu'il brosse un tableau plus complet);
- l'impact du profilage (les effets sur la personne concernée); et
- les garanties visant à assurer la loyauté, la non-discrimination et l'exactitude du processus de profilage.

Bien que l'avis du GT29 sur les intérêts légitimes[20] se fonde sur l'article 7 de la directive 95/46/CE relative à la protection des données (ci-après la «directive»), il contient des exemples qui restent utiles et pertinents pour les responsables du traitement qui effectuent le profilage. Il suggère également qu'il serait difficile pour les responsables du traitement de justifier le recours à des intérêts légitimes comme base légale pour des pratiques intrusives de profilage et de suivi à des fins de marketing ou de publicité, par exemple celles qui impliquent le suivi d'individus sur plusieurs sites web, emplacements, dispositifs, services ou courtage de données.

Le responsable du traitement devrait également tenir compte de l'utilisation future ou de la combinaison de profils lors de l'évaluation de la validité du traitement en vertu de l'article 6, paragraphe 1, point f).

C. Article 9 – Catégories particulières de données

Les responsables du traitement ne peuvent traiter des données à caractère personnel d'une catégorie particulière que s'ils peuvent satisfaire à l'une des conditions énoncées à l'article 9, paragraphe 2, ainsi qu'à une condition de l'article 6. Cela comprend les données d'une catégorie particulière dérivées ou déduites de l'activité de profilage.

Le profilage peut engendrer des données d'une catégorie particulière par inférence à partir de données qui n'appartiennent pas à une catégorie particulière en soi, mais qui le deviennent lorsqu'elles sont combinées avec d'autres données. Par exemple, il peut être possible de déduire l'état de santé d'une personne à partir des historiques de ses achats d'aliments combinés à des données sur la qualité et la teneur énergétique des aliments.

Il est alors possible de découvrir des corrélations qui donnent des indications au sujet de la santé, des convictions politiques, des croyances religieuses ou de l'orientation sexuelle des individus, comme le démontre l'exemple suivant:

Exemple

[20] Groupe de travail «article 29» sur la protection des données. Avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE. Commission européenne, 9 avril 2014, page 47, exemples aux pages 59 et 60 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Document consulté le 24 avril 2017.

Une étude[21] a combiné les «J'aime» de Facebook avec des données d'enquête limitées et a constaté que les chercheurs ont prédit avec précision l'orientation sexuelle d'un utilisateur masculin dans 88 % des cas, l'origine ethnique de l'utilisateur dans 95 % des cas et si un utilisateur était chrétien ou musulman dans 82 % des cas.

Si des préférences et des caractéristiques sensibles sont déduites du profilage, le responsable du traitement doit s'assurer:

- que le traitement n'est pas incompatible avec la finalité initiale;
- qu'il a identifié une base légale pour le traitement des données d'une catégorie particulière; et
- qu'il informe la personne concernée du traitement.

La prise de décision automatisée telle que définie à l'article 22, paragraphe 1, qui est fondée sur des catégories particulières de données est couverte au chapitre IV (section D).

D. Droits de la personne concernée[22]

Le RGPD introduit des droits renforcés pour les personnes concernées et crée de nouvelles obligations pour les responsables du traitement.

Dans le contexte du profilage, ces droits sont opposables au responsable du traitement qui crée le profil et au responsable du traitement qui prend une décision automatisée au sujet d'une personne concernée (avec ou sans intervention humaine), si ces entités ne sont pas les mêmes.

Exemple

Un courtier de données entreprend le profilage de données à caractère personnel. Conformément à ses obligations en vertu des articles 13 et 14, il devrait informer la personne concernée du traitement, notamment de son intention de partager son profil avec d'autres organisations. Il devrait également présenter séparément les détails du droit d'opposition en vertu de l'article 21, paragraphe 1.

Le courtier de données partage le profil avec une autre société. Cette société utilise le profil pour envoyer des messages de prospection à la personne concernée.

La société doit informer l'individu [article 14, paragraphe 1, point c)] des raisons d'utiliser ce profil, et de la source d'où proviennent ces informations [article 14, paragraphe 2, point f)]. La société doit également informer la personne concernée de son droit de s'opposer au traitement, y compris au profilage, à des fins de prospection (article 21, paragraphe 2).

21

Michael Kosinski, David Stilwell et Thore Graepel. Les traits et attributs privés sont prévisibles à partir des enregistrements numériques du comportement humain (Private traits and attributes are predictable from digital records of human behaviour). Actes de l'Académie nationale des sciences des États-Unis d'Amérique, http://www.pnas.org/content/110/15/5802.full.pdf . Document consulté le 29 mars 2017.

22 Cette section est pertinente tant pour le profilage que pour la prise de décision automatisée. Pour la prise de décision automatisée en vertu de l'article 22, veuillez noter qu'il existe également des exigences supplémentaires telles que décrites au chapitre IV.

Le courtier de données et la société devraient permettre à la personne concernée d'accéder aux informations utilisées (article 15) pour rectifier toute information erronée (article 16) et, dans certaines circonstances, effacer le profil ou les données à caractère personnel utilisées pour la créer (article 17). La personne concernée devrait également être informée de son profil, par exemple dans quels «segments» ou «catégories» elle est placée. [23]

Si la société utilise le profil dans le cadre d'un processus décisionnel exclusivement automatisé ayant des effets juridiques sur la personne concernée ou l'affectant de manière significative de façon similaire, la société est le responsable du traitement soumis aux dispositions de l'article 22. (Cela n'exclut pas le courtier de données de l'article 22 si le traitement atteint le niveau requis.)

1. Articles 13 et 14 – Droit d'être informé

Compte tenu du principe fondamental de transparence qui sous-tend le RGPD, les responsables du traitement doivent veiller à expliquer clairement et simplement aux personnes concernées la manière dont fonctionne le profilage ou le processus décisionnel automatisé.

En particulier, lorsque le traitement implique une prise de décision fondée sur le profilage (indépendamment du fait qu'il relève ou non des dispositions de l'article 22), le fait que le traitement vise à la fois a) le profilage et b) la prise de décision fondée sur le profil généré doit être clairement indiqué à la personne concernée[24].

Le considérant 60 indique que la fourniture d'informations sur le profilage fait partie des obligations de transparence du responsable du traitement en vertu de l'article 5, paragraphe 1, point a). La personne concernée a le droit *d'être informée* par le responsable du traitement et, dans certaines circonstances, *de s'opposer* au «profilage», *indépendamment* du fait qu'il s'agisse ou non d'une prise de décision individuelle exclusivement automatisée fondée sur le profilage.

D'autres orientations sur la transparence en général sont disponibles dans les lignes directrices du GT29 sur la transparence dans le cadre du RGPD[25].

2. Article 15 — Droit d'accès

L'article 15 donne à la personne concernée le droit d'obtenir des précisions sur toutes les données à caractère personnel utilisées pour le profilage, y compris les catégories de données utilisées pour l'élaboration d'un profil.

[23] Autorité norvégienne de protection des données. La grande course aux données – Comment l'utilisation commerciale des données à caractère personnel remet en question la protection de la vie privée (The Great Data Race - How commercial use of personal data challenges privacy), rapport, novembre 2015. https://www.datatilsynet.no/English/Publications/The-Great-Data-Race/ Document consulté le 24 avril 2017.

[24] RGPD – Article 13, paragraphe 1, point c), et article 14, paragraphe 1, point c). L'article 13, paragraphe 2, point f), et l'article 14, paragraphe 2, point g), exigent que le responsable du traitement informe la personne concernée de l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4. Cela est expliqué plus en détail au chapitre IV.

[25] Groupe de travail «article 29» sur la protection des données. Lignes directrices sur la transparence au titre du règlement (UE) 2016/679 (Guidelines on transparency under Regulation 2016/679), WP260, 28 novembre 2017 http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850, consultées le 18 décembre 2017.

Outre les informations générales sur le traitement, le responsable du traitement est tenu, conformément à l'article 15, paragraphe 3, de mettre à disposition les données utilisées pour créer le profil, et de donner accès aux informations sur le profil et les segments dans lesquels la personne concernée a été placée.

Cela diffère du droit à la portabilité des données en vertu de l'article 20, en vertu duquel le responsable du traitement ne doit communiquer que les données fournies par la personne concernée ou observées par le responsable du traitement, et non le profil lui-même[26].

Le considérant 63 prévoit une certaine protection pour les responsables du traitement qui s'inquiètent de révéler des secrets d'affaires ou liés à la propriété intellectuelle, ce qui peut être particulièrement pertinent en ce qui concerne le profilage. Il indique que ce droit d'accès ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. Toutefois, les responsables du traitement ne peuvent pas invoquer la protection de leurs secrets d'affaires comme excuse pour refuser l'accès ou refuser de fournir des informations à la personne concernée

Le considérant 63 dispose que lorsque c'est possible, le responsable du traitement devrait pouvoir donner l'accès à distance à un système sécurisé permettant à la personne concernée d'accéder directement aux données à caractère personnel la concernant.

3. Article 16 – Droit de rectification, article 17 – Droit à l'effacement et article 18 – Droit à la limitation du traitement

Le profilage peut comporter un élément de prédiction, ce qui augmente le risque d'inexactitude. Les données saisies peuvent être inexactes ou non pertinentes, ou sorties de leur contexte. Il peut y avoir un problème avec l'algorithme utilisé pour établir les corrélations.

Le droit de rectification de l'article 16 pourrait s'appliquer lorsque, par exemple, une personne est placée dans une catégorie qui donne des indications sur sa capacité à accomplir une tâche, et que ce profil est fondé sur des informations incorrectes. Les personnes peuvent contester l'exactitude des données utilisées et tout groupement ou catégorie qui leur a été appliqué.

Les droits de rectification et à l'effacement[27] s'appliquent à la fois aux «données à caractère personnel saisies» (les données à caractère personnel utilisées pour créer le profil) et aux «données de sortie» (le profil lui-même ou la «note» attribuée à la personne).

L'article 16 prévoit également que la personne concernée a le droit de compléter les données à caractère personnel par des informations complémentaires.

Exemple

[26] Page 9, Lignes directrices du GT29 sur le droit à la portabilité des données (WP29 Guidelines on the Right to data portability), WP242 http://ec.europa.eu/newsroom/document.cfm?doc_id=45685. Consultées le 8 janvier 2018.

[27] RGPD– Article 17.

Le système informatique d'un cabinet médical local de chirurgie place une personne dans un groupe qui est le plus susceptible de contracter une maladie cardiaque. Ce «profil» n'est pas nécessairement inexact, même si elle ne souffre jamais d'une maladie cardiaque.
Le profil indique simplement qu'elle est *plus susceptible* de la contracter. C'est peut-être exact d'un point de vue statistique.

Néanmoins, la personne concernée a le droit, compte tenu de la finalité du traitement, de fournir une déclaration supplémentaire. Dans le scénario ci-dessus, cela pourrait se fonder, par exemple, sur un système informatique médical plus avancé (et un modèle statistique) tenant compte de données supplémentaires et effectuant des examens plus détaillés que celui du cabinet médical local avec des capacités plus limitées.

Le droit à la limitation du traitement (article 18) s'appliquera à n'importe quelle étape du processus de profilage.

4. Article 21 — Droit d'opposition

Le responsable du traitement doit porter *explicitement* à l'attention de la personne concernée les détails du droit d'opposition prévu à l'article 21, paragraphes 1 et 2, et les présenter clairement et séparément des autres informations (article 21, paragraphe 4).

En vertu de l'article 21, paragraphe 1, la personne concernée peut s'opposer au traitement (y compris au profilage) pour des raisons tenant à sa situation particulière. Les responsables du traitement sont spécifiquement tenus de prévoir ce droit dans tous les cas où le traitement est fondé sur l'article 6, paragraphe 1, point e) ou f).

Une fois que la personne concernée exerce ce droit, le responsable du traitement doit interrompre[28] (ou éviter de commencer) le processus de profilage, à moins qu'il puisse démontrer qu'il existe des motifs légitimes impérieux qui prévalent sur les intérêts et les droits et libertés de la personne concernée. Le responsable du traitement peut également être amené à effacer les données à caractère personnel pertinentes[29].

Le RGPD ne fournit aucune explication de ce qui serait considéré comme des motifs légitimes et impérieux[30]. Il se peut, par exemple, que le profilage soit bénéfique pour la société dans son ensemble (ou pour l'ensemble de la communauté) et pas seulement pour les intérêts commerciaux du responsable du traitement, comme le profilage destiné à prédire la propagation de maladies contagieuses.

Le responsable du traitement devrait:

- tenir compte de l'importance du profilage par rapport à son objectif particulier;

[28] RGPD – Article 18, paragraphe 1, point d).

[29] RGPD – Article 17, paragraphe 1, point c).

[30] Voir l'explication sur la légitimité, avis 6/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, groupe de travail «article 29» sur la protection des données. 9 avril 2014. Pages 24 à 26, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf . Document consulté le 24 avril 2017.

- examiner l'impact du profilage sur les intérêts, les droits et les libertés de la personne concernée – lequel devrait être limité au minimum nécessaire pour atteindre l'objectif; et
- effectuer une mise en balance.

Il doit toujours y avoir une mise en balance entre les intérêts concurrents du responsable du traitement et le fondement de l'opposition de la personne concernée (que ce soit pour des raisons personnelles, sociales ou professionnelles). Contrairement à la directive 95/46/CE, c'est au responsable du traitement plutôt qu'à la personne concernée qu'il incombe de prouver l'existence de motifs légitimes et impérieux.

Il ressort clairement du libellé de l'article 21 que le critère de mise en balance est différent de celui de l'article 6, paragraphe 1, point f). En d'autres termes, il ne suffit pas qu'un responsable du traitement démontre simplement que l'analyse de son intérêt légitime antérieur était correcte. Ce critère de mise en balance exige que l'intérêt légitime soit *impérieux*, ce qui implique un seuil plus élevé pour les objections majeures.

L'article 21, paragraphe 2 accorde un droit *inconditionnel* à la personne concernée de s'opposer au traitement de ses données à caractère personnel à des fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection[31]. Cela signifie qu'il n'est pas nécessaire de procéder à une mise en balance des intérêts; le responsable du traitement doit respecter les souhaits de la personne sans remettre en cause les motifs de l'objection. Le considérant 70 fournit un contexte supplémentaire à ce droit et indique qu'il peut être exercé à tout moment et sans frais.

IV. Dispositions spécifiques concernant la prise de décision exclusivement automatisée définie à l'article 22

L'article 22, paragraphe 1, dispose ce qui suit:

> La personne concernée a le droit de ne pas faire l'objet d'une décision fondée *exclusivement* sur un traitement automatisé, y compris le profilage, produisant des *effets juridiques* la concernant ou *l'affectant de manière significative de façon similaire*.

Le terme «droit» dans la disposition ne signifie pas que l'article 22, paragraphe 1, ne s'applique que lorsqu'il est activement invoqué par la personne concernée. L'article 22, paragraphe 1, établit une interdiction générale de prendre des décisions fondées exclusivement sur un traitement automatisé. Cette interdiction s'applique que la personne concernée prenne ou non une mesure concernant le traitement de ses données à caractère personnel.

En résumé, l'article 22 prévoit ce qui suit:

i) en principe, il existe une interdiction générale de prendre des décisions individuelles entièrement automatisées, y compris le profilage qui a un effet juridique ou un effet d'une importance similaire;
ii) toutefois, cette règle admet des exceptions;

[31] Conformément à l'article 12, paragraphe 2, les responsables du traitement qui collectent des données à caractère personnel auprès de personnes dans le but de les utiliser à des fins de prospection devraient, au moment de la collecte, envisager de proposer aux personnes concernées un moyen facile d'indiquer qu'elles ne souhaitent pas que leurs données à caractère personnel soient utilisées à des fins de prospection, plutôt que de leur demander d'exercer leur droit d'opposition à une occasion ultérieure.

iii) lorsque l'une de ces exceptions s'applique, des mesures doivent être mises en place pour sauvegarder les droits et libertés de la personne concernée ainsi que ses intérêts légitimes[32].

Cette interprétation renforce l'idée que la personne concernée a le contrôle de ses données à caractère personnel, ce qui est conforme aux principes fondamentaux du RGPD. Interpréter l'article 22 comme une interdiction plutôt que comme un droit à invoquer signifie que les personnes sont automatiquement protégées contre les effets potentiels de ce type de traitement. Le libellé de l'article suggère que telle en est l'intention et il est étayé par le considérant 71 qui indique ce qui suit:

> Toutefois, la prise de décision fondée sur un tel traitement, y compris le profilage, **devrait être permise** lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre [...] ou nécessaire à la conclusion ou à l'exécution d'un contrat [...], ou si la personne concernée a donné son consentement explicite.

Cela implique que le traitement au titre de l'article 22, paragraphe 1, n'est généralement pas autorisé[33].

Toutefois, l'interdiction prévue à l'article 22, paragraphe 1, *ne s'applique que* dans des circonstances spécifiques lorsqu'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, a un effet juridique sur une personne ou l'affecte de manière significative de façon similaire, comme expliqué plus en détail dans les lignes directrices. Même dans ces cas, il existe des exceptions définies qui permettent un tel traitement.

Les mesures de protection requises, examinées plus en détail ci-après, comprennent le droit d'être informé (abordé aux articles 13 et 14 – informations particulièrement utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues du traitement pour la personne concernée), et les garanties, telles que le droit d'obtenir une intervention humaine et le droit de contester la décision (abordés à l'article 22, paragraphe 3).

Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les personnes concernées, le responsable du traitement effectue une analyse d'impact relative à la protection des données.[34] Outre les autres risques liés au traitement, une analyse d'impact relative à la protection des données peut s'avérer particulièrement utile pour les responsables du traitement qui ne sont pas certains que les activités proposées relèvent de la définition de l'article 22, paragraphe 1, et, si une exception identifiée le permet, des mesures de sauvegarde qui doivent être appliquées.

A. «Décision fondée exclusivement sur un traitement automatisé»

[32] Le considérant 71 indique qu'en tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.

[33] D'autres commentaires sur l'interprétation de l'article 22 en tant qu'interdiction figurent à l'annexe 2.

[34] Groupe de travail «article 29» sur la protection des données, lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679. 4 avril 2017. Commission européenne. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Document consulté le 24 avril 2017.

L'article 22, paragraphe 1, fait référence aux décisions «fondées exclusivement» sur un traitement automatisé. Cela signifie qu'il n'y a pas d'intervention humaine dans le processus de décision.

Exemple

Un processus automatisé produit ce qui est en fait une recommandation au sujet d'une personne concernée. Si un être humain examine et tient compte d'autres facteurs dans la prise de décision finale, cette décision ne serait pas «fondée exclusivement» sur un traitement automatisé.

Le responsable du traitement ne peut pas contourner les dispositions de l'article 22 en créant une intervention humaine de toutes pièces. Par exemple, si quelqu'un applique systématiquement des profils générés automatiquement à des individus sans aucune influence réelle sur le résultat, il s'agirait quand même d'une décision fondée exclusivement sur un traitement automatisé.

Pour qu'il y ait intervention humaine, le responsable du traitement doit s'assurer que tout contrôle de la décision est significatif et ne constitue pas qu'un simple geste symbolique. Le contrôle devrait être effectué par une personne qui a l'autorité et la compétence pour modifier la décision. Dans le cadre de l'analyse, il convient de tenir compte de toutes les données pertinentes.

Dans le cadre de son analyse d'impact relative à la protection des données, le responsable du traitement devrait identifier et consigner le degré d'intervention humaine dans le processus de prise de décision et le stade auquel cela se produit.

B. «Produisant des effets juridiques à l'égard d'une personne physique» ou «l'affectant de manière significative de façon similaire»

Le RGPD reconnaît que la prise de décision automatisée, y compris le profilage, peut avoir de graves conséquences pour les personnes concernées. Le RGPD ne définit pas le terme «effets juridiques» ni l'expression «de manière significative de façon similaire», mais la formulation utilisée indique clairement que seuls les effets ayant une incidence grave seront couverts par l'article 22.

Décision «produisant des effets juridiques»

Un effet juridique exige que la décision, qui est fondée exclusivement sur un traitement automatisé, affecte les droits juridiques d'une personne, comme la liberté de s'associer avec d'autres personnes, de voter lors d'élections ou d'intenter une action en justice. Un effet juridique peut également affecter le statut juridique d'une personne ou ses droits en vertu d'un contrat. Parmi les exemples de ce type d'effet, il convient de mentionner les décisions automatisées au sujet d'une personne qui se traduisent par:

- l'annulation d'un contrat;
- le droit ou le refus d'un avantage social particulier accordé par la loi, comme l'allocation familiale ou l'allocation de logement;
- le refus d'admission dans un pays ou le refus de citoyenneté.

«l'affectant de manière significative de façon similaire»

Même si un processus décisionnel n'a pas d'effet sur les droits juridiques des personnes, il pourrait quand même relever du champ d'application de l'article 22 s'il produit un effet équivalent ou qui affecte la personne concernée de manière significative de façon similaire.

En d'autres termes, même s'il n'y a pas de changement dans ses droits ou obligations juridiques, la personne concernée pourrait quand même être suffisamment affectée pour exiger les protections prévues par cette disposition. Le RGPD ajoute l'expression «de façon similaire» (absente de l'article 15 de la directive 95/46/CE) à l'expression «l'affectant de manière significative». Par conséquent, le niveau d'*importance* doit être similaire à celui d'une décision produisant un effet juridique.

Le considérant 71 fournit les exemples typiques suivants: «le rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine».

Pour que le traitement des données affecte une personne de manière significative, les effets du traitement doivent être suffisamment conséquents ou importants pour être pris en considération. En d'autres termes, la décision doit être de nature à:

- affecter de manière significative la situation, le comportement ou les choix des personnes concernées;
- avoir un impact prolongé ou permanent sur la personne concernée; ou
- à l'extrême, entraîner l'exclusion ou la discrimination des personnes.

Même s'il est difficile d'être précis sur ce qui serait considéré comme suffisamment *significatif* pour atteindre le niveau requis, les décisions suivantes pourraient entrer dans cette catégorie:

- les décisions qui ont une incidence sur la situation financière d'une personne, comme son admissibilité à un crédit;
- les décisions qui affectent l'accès d'une personne aux services de santé;
- les décisions qui privent une personne d'une possibilité d'emploi ou qui la désavantagent gravement;
- les décisions qui affectent l'accès d'une personne à l'éducation, par exemple les admissions à l'université.

Cela nous amène également à la question de la publicité en ligne, qui s'appuie de plus en plus sur des outils automatisés et qui implique uniquement la prise de décision individuelle automatisée. Outre le respect des dispositions générales du RGPD, couvertes au chapitre III, les dispositions de la proposition de règlement «vie privée et communications électroniques» peuvent également être pertinentes. En outre, les enfants ont besoin d'une protection renforcée, comme nous le verrons plus loin au chapitre V.

Dans de nombreux cas typiques, la décision de présenter une publicité ciblée fondée sur le profilage, telle qu'une publicité pour un magasin de mode en ligne grand public basée sur un simple profil démographique, n'affectera pas les personnes concernées de façon similaire de manière significative : «les femmes de la région bruxelloise âgées de 25 à 35 ans qui sont susceptibles de s'intéresser à la mode et à certains articles d'habillement».

Toutefois, il se peut que ce soit le cas, selon les caractéristiques particulières de la situation, y compris en ce qui concerne:

- le caractère intrusif du processus de profilage, y compris le suivi des personnes sur différents sites web, appareils et services;
- les attentes et les souhaits des personnes concernées;
- la façon dont l'annonce est diffusée; ou
- le recours aux vulnérabilités connues des personnes concernées visées.

Un traitement qui pourrait avoir peu d'incidences sur les personnes en général peut en fait avoir un effet significatif à l'égard de certains groupes de la société, tels que les groupes minoritaires ou les

adultes vulnérables. Par exemple, une personne dont il est connu qu'elle éprouve des difficultés financières ou qui est susceptible d'éprouver de telles difficultés, et qui est régulièrement ciblée par des publicités pour des prêts à taux d'intérêt élevé, peut s'inscrire à ces offres et s'endetter davantage.

La prise de décision automatisée qui se traduit par des prix différentiels fondés sur des données à caractère personnel ou des caractéristiques personnelles pourrait également avoir un effet significatif si, par exemple, des prix prohibitifs empêchent effectivement une personne d'accéder à certains biens ou services.

La personne concernée pourrait également subir des effets l'affectant de manière significative de façon similaire, qui seraient déclenchés par les actions d'individus autres que celui auquel se rapporte la décision automatisée. Une illustration en est donnée ci-dessous.

Exemple

Hypothétiquement, une société émettrice de cartes de crédit pourrait réduire la limite de crédit d'un client, non pas en fonction de ses propres antécédents de remboursement, mais en fonction de critères de crédit non traditionnels, comme une analyse d'autres clients vivant dans la même région qui font leurs courses dans les mêmes magasins.

Cela pourrait signifier qu'une personne est privée d'opportunités en raison des actions de tiers.

Dans un contexte différent, l'utilisation de ces types de caractéristiques pourrait avoir l'avantage d'accorder du crédit à ceux qui n'ont pas d'antécédents de crédit conventionnels et qui, autrement, se seraient vu refuser cette possibilité.

C. Exceptions à l'interdiction

L'article 22, paragraphe 1, interdit de manière générale la prise de décision individuelle fondée exclusivement sur un traitement automatisé et produisant des effets juridiques ou affectant la personne concernée de manière significative de façon similaire, comme décrit ci-dessus.

Cela signifie que le responsable du traitement ne devrait pas entreprendre le traitement décrit à l'article 22, paragraphe 1, sauf si l'une des exceptions suivantes prévues à l'article 22, paragraphe 2, s'applique, lorsque la décision est:

a) nécessaire à la conclusion ou à l'exécution d'un contrat;
b) autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou
c) fondée sur le consentement explicite de la personne concernée.

Lorsque la prise de décision concerne des catégories particulières de données définies à l'article 9, paragraphe 1, le responsable du traitement doit également s'assurer qu'elles peuvent satisfaire aux exigences de l'article 22, paragraphe 4.

1. Exécution d'un contrat

Les responsables du traitement peuvent souhaiter utiliser des processus décisionnels exclusivement automatisés à des fins contractuelles parce qu'ils estiment que c'est la façon la plus appropriée

d'atteindre l'objectif. Il se peut que l'intervention humaine de routine soit parfois irréaliste sur le plan pratique ou impossible en raison de la quantité de données traitées.

Le responsable du traitement doit être en mesure de démontrer que ce type de traitement est nécessaire, en tenant compte du fait qu'une méthode plus respectueuse de la vie privée pourrait être adoptée. [35] S'il existe d'autres moyens efficaces et moins intrusifs pour atteindre le même but, alors le traitement ne serait pas «nécessaire».

La prise de décision automatisée décrite à l'article 22, paragraphe 1, peut également être nécessaire pour le traitement précontractuel.

Exemple

Une entreprise annonce un poste vacant. Dans la mesure où les postes au sein de l'entreprise en question sont très convoités, celle-ci reçoit des dizaines de milliers de candidatures. En raison du nombre exceptionnellement élevé de candidatures, l'entreprise peut considérer qu'il n'est pas possible d'identifier les candidats appropriés sans utiliser d'abord des moyens entièrement automatisés pour éliminer les candidatures non pertinentes. Dans ce cas, une prise de décision automatisée peut s'avérer nécessaire pour établir une liste restreinte de candidats possibles, avec l'intention de conclure un contrat avec une personne concernée.

Le chapitre III (section B) fournit davantage d'informations sur les contrats en tant que base légale pour le traitement.

2. Autorisée par le droit de l'Union ou le droit de l'État membre

La prise de décision automatisée, y compris le profilage, pourrait avoir lieu en vertu de l'article 22, paragraphe 2, point b), si le droit de l'Union ou de l'État membre en autorisait l'utilisation. La législation pertinente doit également prévoir des mesures appropriées pour sauvegarder les droits et libertés et les intérêts légitimes de la personne concernée.

Le considérant 71 indique que cela pourrait inclure l'utilisation de la prise de décision automatisée définie à l'article 22, paragraphe 1, aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale, ou d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement.

3. Consentement explicite

L'article 22 exige un consentement *explicite*. Le traitement qui relève de la définition de l'article 22, paragraphe 1, présente des risques importants en matière de protection des données, et un niveau élevé de contrôle individuel sur les données à caractère personnel est donc jugé approprié.

[35] Buttarelli, Giovanni. Guide pour l'évaluation de la nécessité des mesures limitant le droit fondamental à la protection des données à caractère personnel, Contrôleur européen de la protection des données, 11 avril 2017, https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_fr.pdf Consulté le 24 avril 2017.

Le «consentement explicite» n'est pas défini dans le RGPD. Les lignes directrices du GT29 sur le consentement[36] fournissent des orientations sur la façon dont cela doit être interprété.

Le chapitre III (section B) fournit davantage d'informations sur le consentement en général.

D. Catégories particulières de données à caractère personnel – Article 22, paragraphe 4

La prise de décision automatisée (décrite à l'article 22, paragraphe 1) qui implique des catégories particulières de données à caractère personnel n'est autorisée que dans les conditions cumulatives suivantes (article 22, paragraphe 4):

- il existe une exception applicable en vertu de l'article 22, paragraphe 2; et
- l'article 9, paragraphe 2, point a) ou g), s'applique.

Article 9, paragraphe 2, point a) – le consentement explicite de la personne concernée; ou

Article 9, paragraphe 2, point g) – traitement nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Dans les deux cas susmentionnés, le responsable du traitement doit mettre en place des mesures appropriées pour sauvegarder les droits et libertés de la personne concernée ainsi que ses intérêts légitimes.

E. Droits de la personne concernée[37]

1. Articles 13, paragraphe 2, point f), et article 14, paragraphe 2, point g) – Droit d'être informé

Compte tenu des risques et atteintes potentiels que le profilage visé à l'article 22 fait peser sur les droits des personnes concernées, les responsables du traitement devraient être particulièrement attentifs à leurs obligations en matière de transparence.

L'article 13, paragraphe 2, point f), et l'article 14, paragraphe 2, point g), exigent des responsables du traitement qu'ils fournissent des informations spécifiques et facilement accessibles sur la prise de décision automatisée fondée exclusivement sur un traitement automatisé, y compris le profilage, qui

[36] Groupe de travail «article 29» sur la protection des données. Lignes directrices sur le consentement au titre du règlement (UE) 2016/679 (Guidelines on Consent under Regulation 2016/679), WP259. 28 novembre 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849. Consultées le 18 décembre 2017.

[37] L'article 12 du RGPD prévoit les modalités applicables à l'exercice des droits de la personne concernée.

produit des effets juridiques ou affecte la personne concernée de manière significative de façon similaire[38].

Si le responsable du traitement prend des décisions automatisées au sens de l'article 22, paragraphe 1, il doit:

- dire à la personne concernée qu'il pratique ce type d'activité;
- fournir des informations utiles concernant la logique sous-jacente; et
- expliquer l'importance et les conséquences prévues du traitement.

La communication de ces informations aidera également les responsables du traitement à s'assurer qu'ils respectent certaines des garanties requises visées à l'article 22, paragraphe 3, et au considérant 71.

Si la prise de décision et le profilage automatisés ne satisfont pas à la définition de l'article 22, paragraphe 1, il est néanmoins de bonne pratique de fournir les informations ci-dessus. En tout état de cause, le responsable du traitement doit fournir à la personne concernée des informations suffisantes pour rendre le traitement loyal[39] et satisfaire à toutes les autres exigences en matière d'information prévues aux articles 13 et 14.

Informations utiles concernant la «logique sous-jacente»

En raison de la croissance et de la complexité de l'apprentissage automatique, il peut s'avérer difficile de comprendre le fonctionnement d'un processus décisionnel ou d'un profilage automatisé.

Le responsable du traitement devrait trouver des moyens simples d'informer la personne concernée de la raison d'être de la décision ou des critères sur lesquels elle est fondée. Le RGPD exige que le responsable du traitement fournisse des informations utiles sur la logique sous-jacente, mais pas nécessairement une explication complexe des algorithmes utilisés ou la divulgation de l'algorithme complet[40]. Les informations fournies doivent toutefois être suffisamment complètes pour que la personne concernée comprenne les raisons de la décision.

Exemple

Un responsable du traitement utilise la note de solvabilité pour évaluer et rejeter la demande de prêt d'une personne. La note peut avoir été fournie par une agence de référence de crédit ou calculée directement sur la base des informations détenues par le responsable du traitement.

Quelle que soit la source [et les informations sur la source doivent être fournies à la personne concernée en vertu de l'article 14, paragraphe 2, point f), lorsque les données à caractère personnel

[38] Voir l'article 22, paragraphes 1 et 4. Les lignes directrices du groupe de travail sur la transparence couvrent les exigences générales en matière d'information énoncées aux articles 13 et 14.

[39] Le considérant 60 du RGPD dispose que «le responsable du traitement devrait fournir à la personne concernée toute autre information nécessaire pour garantir un traitement équitable et transparent, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées. En outre, la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci.»

[40] La complexité ne peut excuser l'absence de fourniture d'informations à la personne concernée. Le considérant 58 dispose que le principes de transparence «vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne.»

n'ont pas été collectées auprès de la personne concernée], si le responsable du traitement se fonde sur cette note, il doit être en mesure de l'expliquer et d'en expliquer la raison à la personne concernée.

Le responsable du traitement explique que ce processus l'aide à prendre des décisions de prêt loyales et responsables. Il fournit des détails sur les principales caractéristiques prises en considération pour parvenir à la décision, la source de ces informations et leur pertinence. Cela peut inclure, par exemple:

- les informations fournies par la personne concernée dans le formulaire de demande;
- des informations sur la situation antérieure du compte, y compris tout arriéré de paiement; et
- les registres publics officiels tels que les registres de fraude et les registres d'insolvabilité.

Le responsable du traitement inclut également des informations pour informer la personne concernée que les méthodes de notation de la solvabilité utilisées sont régulièrement testées pour s'assurer qu'elles restent loyales, efficaces et impartiales.
Le responsable du traitement fournit des coordonnées de contact à la personne concernée afin que celle-ci puisse demander le réexamen de toute décision refusée, conformément aux dispositions de l'article 22, paragraphe 3.

«Importance» et «conséquences prévues»

Ces termes suggèrent que des informations doivent être fournies sur les traitements prévus ou futurs et sur la manière dont la prise de décision automatisée pourrait affecter la personne concernée[41]. Afin de rendre ces informations utiles et compréhensibles, des exemples réels et tangibles du type d'effets possibles devraient être donnés.

Dans un contexte numérique, les responsables du traitement pourraient être en mesure d'utiliser des outils supplémentaires pour illustrer ces effets.

Exemple

Une compagnie d'assurance utilise un processus décisionnel automatisé pour fixer les primes d'assurance-automobile en fonction du comportement des clients au volant. Pour illustrer l'importance et les conséquences prévues du traitement, elle explique que la conduite dangereuse peut entraîner une augmentation des primes d'assurance et fournit une application comparant les comportements de conducteurs fictifs, y compris ceux qui ont des habitudes dangereuses au volant comme l'accélération rapide et le freinage de dernière minute.

Elle utilise des graphiques pour donner des conseils sur la façon d'améliorer ces habitudes et, par conséquent, de réduire les primes d'assurance.

[41] Conseil de l'Europe. Projet de rapport explicatif sur la version modernisée de la Convention 108 du Conseil de l'Europe, paragraphe75: «Les personnes concernées ont le droit d'obtenir connaissance du raisonnement qui sous-tend le traitement de données, y compris les conséquences de ce raisonnement et les conclusions qui peuvent en avoir été tirées, en particulier lors de l'utilisation d'algorithmes pour une prise de décision automatisée, notamment dans le cadre du profilage. Par exemple, dans le cas d'un système d'évaluation de leur solvabilité par notation, les emprunteurs ont le droit d'obtenir connaissance de la logique sur laquelle repose le traitement de leurs données et qui aboutit à la décision d'octroi ou de refus du crédit, au lieu d'être simplement informés de la décision elle-même. La compréhension de ces éléments contribue à l'exercice effectif d'autres garanties essentielles comme le droit d'opposition et le droit de recours auprès de l'autorité compétente.» https://rm.coe.int/convention-pour-la-protection-des-personnes-a-l-egard-du-traitement-au/16806b6ec3 . Consultée le 24 avril 2017.

Les responsables du traitement peuvent utiliser des techniques visuelles similaires pour expliquer la manière dont une décision antérieure a été prise.

2. Article 15, paragraphe 1, point h) — Droit d'accès

L'article 15, paragraphe 1, point h), autorise les personnes concernées à disposer des mêmes informations concernant une prise de décision exclusivement automatisée, y compris un profilage, que celles requises en vertu de l'article 13, paragraphe 2, point f), et de l'article 14, paragraphe 2, point g), à savoir:

- l'existence d'une prise de décision automatisée, y compris un profilage;
- des informations utiles concernant la logique sous-jacente; et
- l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Le responsable du traitement devrait déjà avoir fourni ces informations à la personne concernée, conformément à ses obligations au titre de l'article 13[42].

L'article 15, paragraphe 1, point h), dispose que le responsable du traitement devrait fournir à la personne concernée des informations sur les *conséquences prévues* du traitement, plutôt qu'une explication d'une décision *particulière*. Le considérant 63 clarifie ce point en précisant que toute personne concernée devrait avoir le droit de se faire «communiquer» des informations sur le traitement automatique des données, y compris la logique sous-jacente et, *au moins* en cas de profilage, les conséquences d'un tel traitement.

En exerçant ses droits en vertu de l'article 15, la personne concernée peut prendre connaissance d'une décision prise à son égard, y compris une décision fondée sur un profilage.

Le responsable du traitement devrait fournir à la personne concernée des informations générales (notamment sur les facteurs pris en considération pour le processus décisionnel et sur leur «importance» respective à un niveau agrégé) qui lui sont également utiles pour contester la décision.

F. Établissement de garanties appropriées

Si la base applicable au traitement est l'article 22, paragraphe 2, point a) ou l'article 22, paragraphe 2, point c), l'article 22, paragraphe 3 exige que les responsables du traitement mettent en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes des personnes concernées. En vertu de l'article 22, paragraphe 2, point b), le droit de l'État membre ou de l'Union qui autorise le traitement doit également prévoir des mesures de sauvegarde appropriées.

Ces mesures devraient inclure au minimum un moyen permettant à la personne concernée d'obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision.

L'intervention humaine est un élément clé. Tout examen doit être effectué par une personne qui a l'autorité et la compétence appropriées pour modifier la décision. L'examinateur devrait procéder à une évaluation approfondie de toutes les données pertinentes, y compris toute information supplémentaire fournie par la personne concernée.

[42] L'article 12, paragraphe 3, du RGPD précise les délais de fourniture de ces informations.

Le considérant 71 souligne qu'*en tout état de cause*, les garanties appropriées devraient également comprendre:

> «[...] une information spécifique de la personne concernée ainsi que le droit [...] d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision.»

Le responsable du traitement doit fournir à la personne concernée un moyen simple d'exercer ces droits.

Cela souligne la nécessité d'assurer la transparence du traitement. La personne concernée ne pourra contester une décision ou exprimer son point de vue que si elle comprend parfaitement la manière dont la décision a été prise et sur quelle base. Les exigences de transparence sont examinées au chapitre IV (section E).

Des erreurs ou des biais dans les données recueillies ou partagées ou une erreur ou un biais dans le processus décisionnel automatisé peuvent avoir comme conséquences:

- des classifications incorrectes; et
- des évaluations fondées sur des projections imprécises; qui
- ont une incidence négative sur les individus.

Les responsables du traitement devraient procéder à des évaluations fréquentes des ensembles de données qu'ils traitent afin de vérifier s'il n'y a pas de biais, et élaborer des moyens de traiter tout élément préjudiciable, y compris toute dépendance excessive à l'égard des corrélations.
Les systèmes qui vérifient les algorithmes et les examens réguliers de l'exactitude et de la pertinence de la prise de décision automatisée, y compris le profilage, sont d'autres mesures utiles.

Les responsables du traitement devraient mettre en place des procédures et des mesures appropriées pour prévenir les erreurs, les inexactitudes[43] ou la discrimination sur la base de données de catégories particulières. Ces mesures devraient être utilisées sur une base cyclique; non seulement au stade de la conception, mais aussi en permanence, car le profilage est appliqué aux individus. Les résultats de ces mesures devraient être pris en considération dans la conception du système.

D'autres exemples de mesures de sauvegarde appropriées sont disponibles dans la section Recommandations

V. Enfants et profilage

Le RGPD instaure des obligations supplémentaires pour les responsables du traitement des données lorsqu'ils traitent des données à caractère personnel relatives aux enfants.

L'article 22 lui-même ne fait aucune distinction selon que le traitement concerne des adultes ou des enfants. Toutefois, le considérant 71 indique que les décisions exclusivement automatisées, y compris le profilage, produisant des effets juridiques ou affectant la personne concernée de manière

[43] Le considérant 71 du RGPD indique ce qui suit:
«Afin d'assurer un traitement équitable et transparent à l'égard de la personne concernée, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées, le responsable du traitement devrait utiliser des procédures mathématiques ou statistiques adéquates aux fins du profilage, appliquer les mesures techniques et organisationnelles appropriées pour faire en sorte, en particulier, que les facteurs qui entraînent des erreurs dans les données à caractère personnel soient corrigés et que le risques d'erreur soit réduit au minimum, [...].»

significative de façon similaire, ne devraient pas s'appliquer aux enfants[44]. Étant donné que cette formulation n'est pas reflétée dans l'article lui-même, le GT29 estime qu'il ne s'agit pas d'une interdiction absolue de ce type de traitement à l'égard des enfants. Toutefois, à la lumière de ce considérant, le GT29 recommande aux responsables du traitement de ne pas invoquer, en principe, les exceptions prévues à l'article 22, paragraphe 2, pour le justifier.

Il peut néanmoins y avoir des circonstances dans lesquelles il est nécessaire que les responsables du traitement prennent des décisions exclusivement automatisées, y compris le profilage, produisant des effets juridiques ou affectant les enfants de manière significative de façon similaire, par exemple pour protéger leur bien-être. Dans un tel cas, le traitement peut être effectué sur la base des exceptions visées à l'article 22, paragraphe 2, points a), b) ou c), selon le cas.

Dans ces cas, des garanties appropriées doivent être en place, comme l'exigent l'article 22, paragraphe 2, point b), et l'article 22, paragraphe 3, et elles doivent donc être adaptées aux enfants. Le responsable du traitement doit veiller à ce que ces garanties soient efficaces pour protéger les droits, les libertés et les intérêts légitimes des enfants dont les données sont traitées.

La nécessité d'une protection spécifique pour les enfants est reflétée dans le considérant 38, qui dispose ce qui suit:

> «Les enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel. Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins *de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant*.»

L'article 22 n'empêche pas les responsables du traitement de prendre des décisions exclusivement automatisées concernant les enfants, si la décision ne produit pas d'effet juridique ou n'affecte pas l'enfant de manière significative de façon similaire. Cependant, une prise de décision exclusivement automatisée qui influence les choix et le comportement d'un enfant pourrait potentiellement produire un effet juridique ou l'affecter de manière significative de façon similaire, selon la nature des choix et des comportements en question.

Dans la mesure où les enfants représentent un groupe plus vulnérable de la société, les organisations devraient, en général, s'abstenir de les profiler à des fins de marketing[45]. Les enfants peuvent être particulièrement vulnérables dans l'environnement en ligne et plus facilement influencés par la publicité comportementale. Par exemple, dans les jeux en ligne, le profilage peut être utilisé pour cibler les joueurs qui, selon l'algorithme, sont plus susceptibles de dépenser de l'argent dans le jeu et pour fournir des publicités plus personnalisées. L'âge et la maturité de l'enfant peuvent affecter sa

[44] Considérant 71 – «Cette mesure ne devrait pas concerner un enfant.»

[45] L'avis 02/2013 du GT29 sur les applications destinées aux dispositifs intelligents (WP202), adopté le 27 février 2013, dans sa section 3.10 consacrée aux enfants, précise à la page 26 que les responsables du traitement des données ne doivent pas traiter les données des enfants à des fins de publicité comportementale, ni directement ni indirectement, car l'enfant n'est pas en mesure d'en comprendre la finalité et cela dépasse donc les limites du traitement licite.

capacité à comprendre la motivation qui sous-tend ce type de marketing ou les conséquences qui en découlent[46].

L'article 40, paragraphe 2, point g, fait explicitement référence à l'élaboration de codes de conduite prévoyant des garanties pour les enfants; il est également possible de compléter des codes existants[47].

VI. Analyses d'impact relatives à la protection des données et délégué à la protection des données

La responsabilité est un domaine important et une exigence explicite dans le cadre du RGPD. [48]

En tant qu'outil clé de responsabilisation, une analyse d'impact relative à la protection des données permet au responsable du traitement d'évaluer les risques associés à la prise de décision automatisée, y compris le profilage. Il s'agit d'une façon de montrer que des mesures appropriées ont été mises en place pour faire face à ces risques et démontrer la conformité avec le RGPD.

L'article 35, paragraphe 3, point a), souligne la nécessité pour le responsable du traitement d'effectuer une analyse d'impact relative à la protection des données dans les cas suivants:

> *l'évaluation systématique et approfondie* d'aspects personnels concernant des personnes physiques, qui est *fondée sur* un traitement automatisé, *y compris* le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;

L'article 35, paragraphe 3, point a), fait référence aux évaluations, y compris le profilage et les décisions qui sont «fondées» sur un traitement automatisé, plutôt que sur un traitement «exclusivement» automatisé. Cela signifie que l'article 35, paragraphe 3, point a), s'appliquera dans le cas d'une prise de décision, y compris un profilage, produisant des effets juridiques ou affectant les personnes concernées de manière significative de façon similaire, qui *n'est pas* entièrement automatisée, ainsi que d'une prise de décision exclusivement automatisée définie à l'article 22, paragraphe 1.

Si le responsable du traitement envisage un «modèle» dans lequel il prend des décisions *exclusivement* automatisées ayant une *forte incidence* sur les personnes concernées sur la base de profils établis à leur sujet et qu'il *ne peut* se fonder sur le consentement de ces personnes, sur un contrat conclu avec elles ou sur une loi l'autorisant, le responsable du traitement ne devrait pas poursuivre la procédure.

Le responsable du traitement peut toujours envisager un «modèle» de prise de décision fondé sur le profilage, en augmentant sensiblement le niveau d'intervention humaine, de sorte que le modèle *n'est plus un processus décisionnel entièrement automatisé*, bien que le traitement puisse encore présenter

---

[46] Une étude de l'UE sur l'impact du marketing par l'intermédiaire des médias sociaux, des jeux en ligne et des applications mobiles sur le comportement des enfants a montré que les pratiques de marketing ont une incidence manifeste sur le comportement des enfants. Cette étude s'est fondée sur des enfants âgés de 6 à 12 ans.

[47] Un exemple de code de conduite en matière de marketing auprès des enfants est celui produit par la FEDMA, mémorandum explicatif, disponible à l'adresse: http://www.oecd.org/sti/ieconomy/2091875.pdf Consulté le 15 mai 2017. Voir en particulier: «6.2 Les agents de marketing ciblant les enfants, ou pour lesquels les enfants sont susceptibles de constituer une partie de leur public, ne devraient pas exploiter la crédulité, la loyauté, la vulnérabilité ou le manque d'expérience des enfants; 6.8.5 Les agents de marketing ne devraient pas subordonner l'accès d'un enfant à un site web à la collecte de renseignements personnels détaillés. En particulier, des mesures incitatives spéciales telles que des offres de prix et des jeux ne devraient pas être utilisées pour inciter les enfants à divulguer des informations personnelles détaillées» (traduction libre).

[48] Comme l'exige l'article 5, paragraphe 2, du RGPD.

des risques pour les droits et libertés fondamentaux des personnes concernées. Si tel est le cas, le responsable du traitement doit s'assurer qu'il peut faire face à ces risques et satisfaire aux exigences décrites au chapitre III des présentes lignes directrices.

Une analyse d'impact relative à la protection des données peut également s'avérer utile pour permettre au responsable du traitement de définir les mesures qu'il introduira pour faire face aux risques liés à la protection des données concernées par le traitement. Ces mesures[49] pourraient notamment consister à:

- informer la personne concernée de l'existence et de la logique sous-jacente du processus décisionnel automatisé;
- expliquer l'importance et les conséquences prévues du traitement pour la personne concernée;
- fournir à la personne concernée les moyens de s'opposer à la décision; et à
- permettre à la personne concernée d'exprimer son point de vue.

D'autres activités de profilage peuvent justifier une analyse d'impact relative à la protection des données, selon les particularités du cas. Les responsables du traitement peuvent consulter les lignes directrices du GT29 sur les analyses d'impact relatives à la protection des données[50] pour de plus amples renseignements et pour déterminer la nécessité d'effectuer une analyse d'impact relative à la protection des données.

Une exigence supplémentaire en matière de responsabilité est la désignation d'un délégué à la protection des données (DPD), lorsque le profilage et/ou la prise de décision automatisée constituent une activité de base du responsable du traitement et exigent un suivi régulier et systématique à grande échelle des personnes concernées [article 37, paragraphe 1, point b)][51].

[49] Reflétant les exigences de l'article 13, paragraphe 2, point f), de l'article 14, paragraphe 2, point g), et de l'article 22, paragraphe 3.

[50] Groupe de travail «article 29» sur la protection des données. Groupe de travail «article 29», lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679. 4 avril 2017. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Consultées le 24 avril 2017.

[51] Groupe de travail «article 29» sur la protection des données. Lignes directrices concernant les délégués à la protection des données (DPD). 5 avril 2017; http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 Consultées le 22 janvier 2018.

ANNEXE 1 – Recommandations de bonnes pratiques

Les recommandations de bonnes pratiques suivantes aideront les responsables du traitement des données à satisfaire aux exigences des dispositions du RGPD sur le profilage et la prise de décision automatisée[52].

Article	Objet	Recommandation
5, paragraphe 1, point a), 12, 13, 14	Droit à l'information	Les responsables du traitement devraient consulter les lignes directrices du GT29 sur la transparence (WP260) pour les exigences générales en matière de transparence. Outre les exigences générales, lorsque le responsable du traitement traite des données au sens de l'article 22, il doit fournir des informations utiles concernant la logique sous-jacente. Au lieu de fournir une explication mathématique complexe sur le fonctionnement des algorithmes ou de l'apprentissage automatique, le responsable du traitement devrait envisager d'utiliser des moyens clairs et complets pour fournir les informations à la personne concernée, par exemple: • les catégories de données qui ont été ou seront utilisées dans le processus de profilage ou de prise de décision; • les raisons pour lesquelles ces catégories sont jugées pertinentes; • la façon dont tout profil utilisé dans le processus décisionnel automatisé est établi, y compris les statistiques utilisées dans l'analyse; • les raisons pour lesquelles ce profil est pertinent pour le processus décisionnel automatisé; et • la manière dont il est utilisé aux fins d'une décision au sujet de la personne concernée. Ces informations seront généralement plus pertinentes pour la personne concernée et contribueront à la transparence du traitement. Les responsables du traitement peuvent envisager des techniques de visualisation et des techniques interactives pour faciliter la transparence algorithmique[53].

[52] Les responsables du traitement doivent également s'assurer qu'ils ont mis en place des procédures solides pour garantir qu'ils peuvent remplir les obligations qui leur incombent en vertu des articles 15 à 22 dans les délais prévus par le RGPD.

[53] Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0 (Commissariat à l'information - Mégadonnées, intelligence artificielle, apprentissage automatique et protection des données version 2.0), mars 2017. Page 87, paragraphe 194, mars 2017. https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf Document consulté le 24 avril 2017.

article 6, paragraphe 1, point a)	Consentement comme base du traitement	Si les responsables du traitement se fondent sur le consentement comme base du traitement, ils devraient consulter les lignes directrices du GT29 sur le consentement (WP259).
15	Droit d'accès	Les responsables du traitement peuvent envisager de mettre en place un mécanisme permettant aux personnes concernées de vérifier leur profil, y compris les détails des informations et des sources utilisées pour l'établir.
16	Droit de rectification	Les responsables du traitement qui donnent aux personnes concernées l'accès à leur profil dans le cadre de leurs droits au titre de l'article 15 devraient leur donner la possibilité de mettre à jour ou de corriger toute inexactitude concernant leurs données ou leur profil. Cela peut également aider les responsables du traitement à remplir leurs obligations au titre de l'article 5, paragraphe 1, point d). Les responsables du traitement pourraient envisager d'introduire des outils de gestion des préférences en ligne tels qu'un tableau de bord sur la protection de la vie privée. Cela donnerait aux personnes concernées la possibilité de gérer l'utilisation de leurs informations dans un certain nombre de services différents – ce qui leur permettrait de modifier les paramètres, de mettre à jour leurs données à caractère personnel et d'examiner ou de modifier leur profil pour corriger toute inexactitude.
21, paragraphes 1 et 2	Droit d'opposition	Le droit d'opposition visé à l'article 21, paragraphes 1 et 2, doit être explicitement porté à l'attention de la personne concernée et présenté clairement et séparément de toute autre information (article 21, paragraphe 4). Les responsables du traitement doivent s'assurer que ce droit est affiché clairement sur leur site web ou dans toute documentation pertinente et qu'il n'est pas dissimulé dans d'autres modalités et conditions.
22 et considérant 71	Garanties appropriées	La liste suivante, bien que non exhaustive, fournit quelques suggestions de bonnes pratiques dont les responsables du traitement doivent tenir compte lorsqu'ils prennent une décision fondée exclusivement sur un traitement automatisé, y compris le profilage (visée à l'article 22, paragraphe 1): • des contrôles réguliers d'assurance qualité de leurs systèmes pour veiller à ce que les personnes soient traitées équitablement et ne fassent pas l'objet de discriminations, que ce soit sur la base de catégories particulières de données à caractère personnel ou autrement; • l'audit algorithmique, qui consiste à tester les algorithmes utilisés et développés par les systèmes d'apprentissage automatique pour prouver qu'ils

		fonctionnent réellement comme prévu et qu'ils ne produisent pas de résultats discriminatoires, erronés ou injustifiés; • pour les audits effectués par un «tiers» indépendant (lorsque la prise de décision fondée sur le profilage a une forte incidence sur les personnes concernées), fournir à l'auditeur toute information nécessaire sur le fonctionnement de l'algorithme ou du système d'apprentissage automatique; • obtenir des garanties contractuelles pour les algorithmes de tiers que l'audit et les tests ont été effectués et que l'algorithme est conforme aux normes convenues; • des mesures spécifiques de minimisation des données afin de prévoir des périodes de conservation clairement définies pour les profils et pour toutes les données à caractère personnel utilisées lors de la création ou de l'application des profils; • l'utilisation de techniques d'anonymisation ou de pseudonymisation dans le contexte du profilage; • les moyens de permettre à la personne concernée d'exprimer son point de vue et de contester la décision; et • un mécanisme d'intervention humaine dans des cas précis, par exemple en fournissant un lien vers une procédure de recours au moment où la décision automatisée est transmise à la personne concernée, avec des délais convenus pour l'examen du dossier et un point de contact désigné pour toute question. Les responsables du traitement peuvent également envisager des possibilités telles que: • des mécanismes de certification des opérations de traitement; • des codes de conduite pour les processus d'audit recourant à un apprentissage automatique; • des comités d'examen éthique pour évaluer les inconvénients et les avantages potentiels pour la société liés à des applications particulières dans le domaine du profilage.

ANNEXE 2 – Principales dispositions du RGPD

Principales dispositions du RGPD qui font référence au profilage et à la prise de décision automatisée en général

Article	Considérant	Remarques
3, paragraphe 2, point b)	**24**	Le suivi du comportement des personnes concernées, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. **Considérant 24** «[...] suivies sur internet, [...] l'utilisation [...] de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, *afin notamment de prendre des décisions* la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.»
4, paragraphe 4	**30**	Définition du profilage à l'**article 4, paragraphe 4** **Considérant 30** «des identifiants en ligne tels que des adresses IP et des témoins de connexion («cookies») ou d'autres identifiants, par exemple des étiquettes d'identification par radiofréquence [...] peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, *peuvent servir à créer des profils de personnes physiques et à identifier ces personnes*.»
5 et 6	**72**	**Considérant 72**: «Le profilage est soumis aux règles du présent règlement régissant le traitement des données à caractère personnel, par exemple le fondement juridique du traitement **(article 6)** ou les principes en matière de protection des données **(article 5)**.»
8	**38**	Utilisation des données à caractère personnel d'enfants à des fins de profilage. **Considérant 38:** « Les enfants méritent une protection spécifique [...] notamment, [...] à l'utilisation de données à caractère personnel relatives aux enfants à des fins de [...] création de profils de personnalité ou d'utilisateur.»
13 et 14	**60**	Droit d'être informé **Considérant 60**: «En outre, la personne concernée *devrait être informée de l'existence d'un profilage et des conséquences de celui-ci*.»
15	**63**	Droits d'accès **Considérant 63:** «le droit de connaître et de se faire communiquer [...] les finalités du traitement des données à caractère personnel, [...] et les conséquences que ce traitement pourrait avoir, *au moins* en cas de profilage.»
21, paragraphes 1, 2 et 3	**70**	Droit de s'opposer au profilage **Considérant 70** «[...] le droit [...] de s'opposer à ce traitement, y compris le profilage dans la mesure où il est lié à une telle prospection.»
23	**73**	**Considérant 73:** «Des limitations à certains principes spécifiques [...] au droit d'opposition, aux décisions fondées sur le profilage [...] peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique [...]» afin de sauvegarder des objectifs spécifiques d'intérêt public général.

38

35, paragraphe 3, point a)	**91**	Une analyse d'impact relative à la protection des données est requise dans le cas de «l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est *fondée* sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire;» **Cette disposition couvre la prise de décision, y compris le profilage, qui n'est pas exclusivement automatisée.**

Principales dispositions du RGPD qui font référence à la prise de décision exclusivement automatisée définie à l'article 22

Article	Considérant	Remarques
13, paragraphe 2, point f), et **14, paragraphe 2, point g)**	**61**	Droit d'être informé au sujet: • de l'existence d'un processus décisionnel automatisé en vertu de l'**article 22, paragraphes 1 et 4**; • des informations utiles concernant la logique sous-jacente; • de l'importance et des conséquences prévues de ce traitement.
15, point h)		Droits d'accès spécifiques aux informations concernant l'existence d'une prise de décision automatisée, y compris un profilage.
22, paragraphe 1	**71**	Interdiction de prendre des décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, qui produisent des effets juridiques ou affectent la personne concernée de manière significative de façon similaire. En plus de l'explication fournie dans le corps des lignes directrices, les points suivants développent la raison d'être de l'article 22 en tant qu'interdiction: • Bien que le chapitre III traite des droits de la personne concernée, les dispositions des articles 12 à 22 ne concernent pas exclusivement l'exercice *actif* des droits. Certains droits sont *passifs*; ils ne portent pas tous sur des situations dans lesquelles la personne concernée prend une mesure, c'est-à-dire qu'elle formule une demande, une plainte ou une exigence quelconque. Les articles 15 à 18 et 20 et 21 concernent l'exercice actif des droits de la personne concernée, mais les articles 13 et 14 concernent les devoirs que le responsable du traitement doit remplir, sans aucune intervention active de la personne concernée. Ainsi, l'inclusion de l'article 22 dans ce chapitre ne signifie pas en soi qu'il s'agit d'un droit d'opposition; • L'article 12, paragraphe 2, mentionne «l'exercice des droits conférés à la personne concernée au titre des articles 15 à 22»; mais cela ne signifie pas que l'article 22, paragraphe 1, lui-même doit être interprété comme un droit. Il *existe* un droit actif au titre de l'article 22, mais il fait partie des garanties qui doivent être appliquées dans les cas où la prise de décision automatisée est autorisée [article 22,

		paragraphe 2, points a) à c)] - le droit d'obtenir une intervention humaine, d'exprimer son point de vue et de contester la décision. Il ne s'applique que dans ces cas, car il est interdit d'effectuer le traitement décrit à l'article 22, paragraphe 1, sur d'autres bases; • L'article 22 se trouve dans une section du RGPD appelée «Droit d'opposition **et** prise de décision individuelle automatisée», ce qui implique que l'article 22 n'est *pas* un droit d'opposition comme l'article 21. Cela est encore renforcé par l'absence, à l'article 22, d'une obligation d'information explicite équivalente à celle qui figure à l'article 21, paragraphe 4; • Si l'article 22 devait être interprété comme un droit d'opposition, l'exception prévue à l'article 22, paragraphe 2, point c), n'aurait pas beaucoup de sens. L'exception prévoit que la prise de décision automatisée peut encore avoir lieu si la personne concernée a donné son consentement explicite (voir ci-dessous). Cela serait contradictoire, car une personne concernée ne peut pas s'opposer et consentir au même traitement; • Une objection signifierait qu'une intervention humaine doit avoir lieu. Les exceptions visées à l'article 22, paragraphe 2, points a) et c), prévalent sur la règle principale de l'article 22, paragraphe 1, mais uniquement tant qu'une intervention humaine est à la disposition de la personne concernée, conformément à l'article 22, paragraphe 3. Étant donné que la personne concernée a déjà demandé une intervention humaine (par son opposition), l'article 22, paragraphe 2, points a) et c), serait automatiquement contourné dans tous les cas, le rendant ainsi dénué de sens dans les faits. **Considérant 71**: «Ce type de traitement inclut le "profilage" qui consiste en toute forme de traitement automatisé de données à caractère personnel visant à évaluer les aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des aspects concernant le rendement au travail de la personne concernée, sa situation économique, sa santé, ses préférences ou centres d'intérêt personnels, sa fiabilité ou son comportement, ou sa localisation et ses déplacements [...].» «*Cette mesure ne devrait pas concerner un enfant.*»
22, paragraphe 2, points a) à c)	**71**	L'**article 22, paragraphe 2**, lève l'interdiction de traitement sur la base de **a)** l'exécution ou la conclusion d'un contrat, **b)** du droit de l'Union ou de l'État membre, ou **c)** du consentement explicite. Le **considérant 71** fournit un complément d'information sur l'**article 22, paragraphe 2, point b)**, et indique que le traitement visé à l'**article 22, paragraphe 1**: «[...] devrait être permise lorsqu'elle est expressément autorisée par le droit de l'Union ou le droit d'un État membre auquel le responsable du traitement est soumis, y compris aux fins de contrôler et de prévenir les fraudes et l'évasion fiscale conformément aux règles, normes et recommandations des

40

		institutions de l'Union ou des organes de contrôle nationaux, et d'assurer la sécurité et la fiabilité d'un service fourni par le responsable du traitement [...].»
22, paragraphe 3	**71**	**L'article 22, paragraphe 3, et le considérant 71** précisent également que même dans les cas visés à l'**article 22, paragraphe 2, points a) et c)**, le traitement devrait faire l'objet de garanties appropriées. **Considérant 71:** «qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision. Cette mesure ne devrait pas concerner un enfant.»
23	**73**	**Considérant 73:** «Des limitations à certains principes spécifiques [...] au droit d'opposition, aux décisions fondées sur le profilage [...] peuvent être imposées par le droit de l'Union ou le droit d'un État membre, dans la mesure nécessaire et proportionnée dans une société démocratique [...]» afin de sauvegarder des objectifs spécifiques d'intérêt public général.
35, paragraphe 3, point a)	**91**	Exigences concernant la réalisation d'une analyse d'impact relative à la protection des données
47, paragraphe 2, point e)		Les règles d'entreprise contraignantes visées à l'**article 47, paragraphe 1**, devraient préciser au moins «le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conformément à l'**article 22**».

ANNEXE 3 - Lectures complémentaires

Les présentes lignes directrices tiennent compte des documents suivants:

- GT29, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation (Document d'orientation sur les éléments essentiels d'une définition et d'une disposition sur le profilage dans le règlement général de l'UE sur la protection des données), adopté le 13 mai 2013;
- GT29, avis 2/2010 sur la publicité comportementale en ligne , WP171;
- GT29, avis 03/2013 sur la limitation des finalités, WP 203;
- GT29, avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, WP217
- GT29, Statement on the role of a risk-based approach to data protection legal frameworks (Déclaration sur le rôle d'une approche fondée sur les risques dans les cadres juridiques de protection des données), WP218;
- GT29, avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, WP223;
- GT29, Lignes directrices concernant les délégués à la protection des données (DPD), WP243;

41

- GT29, Lignes directrices sur la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant, WP244;
- GT29, Lignes directrices sur le consentement,WP259
- GT29, Lignes directrices sur la transparence, WP260
- Conseil de l'Europe. Recommandation CM/Rec(2010)13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage;
- Conseil de l'Europe. Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées, janvier 2017
- Information Commissioner's Office – Big data, artificial intelligence, machine learning and data protection version 2.0 (Commissariat à l'information - Mégadonnées, intelligence artificielle, apprentissage automatique et protection des données version 2.0), mars 2017
- Bureau du Commissaire à l'information de l'Australie - Consultation draft: Guide to big data and the Australian Privacy Principles (Projet de consultation: le guide des mégadonnées et des principes australiens de protection de la vie privée), mai 2016
- Contrôleur européen de la protection des données (EDPS), avis 7/2015 – Relever les défis des données massives, 19 novembre 2015
- Datatilsynet – Big Data – privacy principles under pressure (Mégadonnées - les principes de protection de la vie privée sous pression), septembre 2013
- Conseil de l'Europe. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel - Projet de rapport explicatif sur la version modernisée de la Convention 108 du Conseil de l'Europe, août 2016
- Datatilsynet – The Great Data Race – How commercial utilisation of personal data challenges privacy (La grande course aux données – Comment l'utilisation commerciale des données à caractère personnel remet en question la protection de la vie privée). Rapport, novembre 2015.
- Contrôleur européen de la protection des données – Évaluer la nécessité de mesures qui limitent le droit fondamental à la protection des données à caractère personnel: une boîte à outils (Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit).
- Comité mixte des autorités européennes de surveillance. Joint Committee Discussion Paper on the use of Big Data by financial institutions (Document de discussion du Comité mixte sur l'utilisation des mégdonnées par les institutions financières), 2016-86. https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf.
- Commission de la protection de la vie privée. Rapport Big Data https://www.autoriteprotectiondonnees.be/rapport-big-data.
- Sénat des États-Unis, Comité du commerce, des sciences et des transports. Examen du secteur des courtiers de données: collecte, utilisation et vente de données sur les consommateurs à des fins de marketing (A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes), rapport du personnel pour le président Rockefeller, 18 décembre 2013. https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf
- Lilian Edwards & Michael Veale. Slave to the Algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for (Esclave de l'algorithme? Pourquoi un «droit à une explication» n'est probablement pas le remède que vous recherchez). Document de recherche, publié le 24 mai 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855
- NYTimes.com. Showing the Algorithms behind New York City Services (Présentation des algorithmes qui sous-tendent les services de la ville de New York). https://mobile.nytimes.com/2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html?referer=https://t.co/6uUVVjOIXx?amp=1. Document consulté le 24 août 2017.
- Conseil de l'Europe. Recommandation CM/Rec(2018)x du Comité des Ministres aux États membres sur des lignes directrices à l'intention des États membres en vue de respecter, protéger et

assurer les droits de l'enfant dans l'environnement numérique (projet révisé, 25 juillet 2017). https://www.coe.int/en/web/children/-/call-for-consultation-guidelines-for-member-states-to-promote-protect-and-fulfil-children-s-rights-in-the-digital-environment?inheritRedirect=true&redirect=%2Fen%2Fweb%2Fchildren . Document consulté le 31 août 2017.

- Unicef. Privacy, protection of personal information and reputation rights (Protection de la vie privée, protection des renseignements personnels et droit à la réputation). Discussion paper series: Children's Rights and Business in a Digital World. https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf. Document consulté le 31 août 2017.
- Chambre des Lords. Growing up with the internet (Grandir avec internet.). Comité spécial des communications, 2e rapport des sessions 2016-2017. https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm. Consulté le 31 août 2017.
- Sandra Wachter, Brent Mittelstadt et Luciano Floridi. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation (Pourquoi le règlement général sur la protection des données ne prévoit pas de droit à l'explication de la prise de décision automatisée.), 28 décembre 2016. https://www.turing.ac.uk/research_projects/data-ethics-group-deg/ . Document consulté le 13 décembre 2017.
- Sandra Wachter, Brent Mittelstadt et Chris Russell. Counterfactual explanations Without Opening the Black Box: Automated Decisions and the GDPR (Raisonnements contrefactuels sans ouvrir la boîte noire: décisions automatisées et RGPD), 6 octobre2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3063289. Document consulté le 13 décembre 2017.
- Gouvernement australien. Better Practice Guide, Automated Assistance in Administrative Decision-Making. Six steps methodology, plus summary of checklist points Part 7 (Guide des bonnes pratiques, Aide automatisée à la prise de décisions administratives. Méthodologie en six étapes et résumé des points de la liste de contrôle - Partie 7), février 2007. https://www.oaic.gov.au/images/documents/migrated/migrated/betterpracticeguide.pdf. Document consulté le 9 janvier 2018.

Lignes directrices sur la mise en œuvre et la fixation des amendes administratives (WP253)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP 253

Lignes directrices sur l'application et la fixation des amendes administratives aux fins du règlement (UE) 2016/679

Adoptées le 3 octobre 2017

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant chargé de la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (droits fondamentaux et citoyenneté de l'Union) de la direction générale Justice et consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 03/075.

Site web: http://ec.europa.eu/justice/data-protection/index_fr.htm

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

Table des matières:

I. Introduction

L'Union européenne a mené à bien une réforme approfondie de la réglementation relative à la protection des données en Europe. Cette réforme repose sur plusieurs piliers (éléments clés): des règles cohérentes, des procédures simplifiées, des actions coordonnées, la participation des utilisateurs, une information plus efficace et des pouvoirs renforcés d'application des règles.

Les responsables du traitement et les sous-traitants sont plus que jamais chargés de veiller à la protection effective des données à caractère personnel des individus. Les autorités de contrôle sont investies de pouvoirs pour garantir que les principes du règlement général sur la protection des données (ci-après le «règlement») ainsi que les droits des personnes concernées sont respectés conformément à l'esprit et à la lettre du règlement.

L'application cohérente des règles relatives à la protection des données est essentielle à un régime harmonisé de protection des données. Les amendes administratives sont au cœur du nouveau régime d'application introduit par le règlement. Elles constituent un élément efficace de la panoplie dont les autorités de contrôle disposent pour faire respecter la réglementation, parallèlement aux autres mesures prévues par l'article 58.

Le présent document vise à aider les autorités de contrôle, auxquelles il est destiné, à améliorer l'application du règlement et à mieux le faire respecter. Il reflète leur compréhension commune des dispositions de l'article 83 du règlement ainsi que son interaction avec les articles 58 et 70 et les considérants correspondants.

En particulier, l'article 70, paragraphe 1, point e), prévoit que le comité européen de la protection des données (ci-après le «CEPD») est habilité à publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente du présent règlement. L'article 70, paragraphe 1, point k), précise la disposition pour ce qui est des lignes directrices concernant la fixation des amendes administratives.

Les présentes lignes directrices ne sont pas exhaustives et ne fournissent pas d'explications sur les différences entre les systèmes administratifs, civils ou pénaux lors de l'imposition de sanctions administratives en général.

Afin d'assurer une approche cohérente de l'imposition des amendes administratives, qui reflète de manière adéquate l'ensemble des principes énoncés dans les présentes lignes directrices, le CEPD a convenu d'une définition commune des critères d'évaluation visés à l'article 83, paragraphe 2, du règlement. Le CEPD et chaque autorité de contrôle conviennent donc d'utiliser les présentes lignes directrices dans le cadre d'une approche commune.

II. Principes

Dès qu'une violation du règlement a été établie sur la base de l'évaluation des faits de l'espèce, l'autorité de contrôle compétente doit définir la ou les mesures correctives les plus adéquates pour remédier à la violation. Les dispositions de l'article 58, paragraphe 2, points b à j[1], énoncent les instruments que les autorités de contrôle peuvent utiliser pour remédier aux cas de non-conformité dus à un responsable du traitement ou un sous-traitant. Lorsqu'elles exercent ces pouvoirs, les autorités de contrôle doivent respecter les principes suivants:

1. La violation du règlement devrait entraîner l'imposition de «sanctions équivalentes».

La notion d'«équivalence» est essentielle pour déterminer la portée de l'obligation qui incombe aux autorités de contrôle de veiller à être cohérentes lorsqu'elles exercent leur pouvoir d'adopter des mesures correctives conformément à l'article 58, paragraphe 2, de manière générale, et lorsqu'elles infligent des amendes administratives en particulier[2].

Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, ***le niveau de protection [...] devrait être équivalent*** *dans tous les États membres* (considérant 10). Le considérant 11 précise qu'un niveau équivalent de protection des données à caractère personnel dans l'ensemble de l'Union exige, entre autres, «*dans les États membres, des pouvoirs équivalents de surveillance et de contrôle du respect des règles relatives à la protection des données à caractère personnel et des sanctions équivalentes pour les violations*». En outre, des sanctions équivalentes dans l'ensemble des États membres ainsi qu'une coopération efficace entre les autorités de contrôle des différents États membres sont considérées comme une manière «*d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur*», conformément au considérant 13 du règlement.

Le règlement offre une base plus solide que la directive 95/46/CE pour assurer un niveau plus élevé de cohérence, puisqu'il est directement applicable dans les États membres. Si les autorités de contrôle agissent en «totale indépendance» (article 52) à l'égard des gouvernements, des responsables du traitement ou des sous-traitants, elles sont tenues de coopérer «*en vue d'assurer une application cohérente du présent règlement et des mesures prises pour en assurer le respect*» [article 57, paragraphe 1, point g)].

Le règlement appelle à une plus grande cohérence que la directive 95/46/CE lorsque des sanctions sont infligées. Dans les cas transfrontaliers, la cohérence sera garantie essentiellement par le mécanisme de coopération (guichet unique) et, dans une certaine mesure, par le mécanisme de contrôle de la cohérence décrit par le nouveau règlement.

Dans les cas nationaux couverts par le règlement, les autorités de contrôle appliqueront les présentes lignes directrices dans un esprit de coopération, conformément à l'article 57, paragraphe 1, point g), et

[1] L'article 58, paragraphe 2, point a), prévoit que des avertissements peuvent être adressés lorsque «les opérations de traitement [...] sont susceptibles de violer les dispositions du présent règlement». Autrement dit, dans le cas couvert par la disposition, la violation du règlement n'a pas encore eu lieu.

[2] Même lorsque le système juridique de certains pays de l'Union ne permet pas l'imposition d'amendes administratives comme le règlement le prévoit, une telle application des règles dans ces États membres doit avoir un effet équivalent aux amendes administratives infligées par les autorités de contrôle (considérant 151). Les juridictions sont tenues par le règlement mais pas par les présentes lignes directrices du CEPD.

à l'article 63, en vue d'assurer une application cohérente du règlement et des mesures prises pour en assurer le respect. Bien que les autorités de contrôle restent libres de choisir les mesures correctives présentées à l'article 58, paragraphe 2, elles doivent éviter d'appliquer des mesures correctives différentes à des cas similaires.

Il en va de même lorsque ces mesures correctives prennent la forme d'amendes.

2. Comme toutes les mesures correctives choisies par les autorités de contrôle, les amendes administratives devraient être «effectives, proportionnées et dissuasives».

Comme toutes les mesures correctives en général, les amendes administratives devraient répondre de manière adéquate à la nature, à la gravité et aux conséquences de la violation, et les autorités de contrôle doivent apprécier l'ensemble des faits de l'espèce d'une manière cohérente et objectivement justifiée. L'appréciation du caractère effectif, proportionné et dissuasif dans chaque cas devra également prendre en considération l'objectif poursuivi par la mesure corrective retenue, à savoir de restaurer le respect des règles ou de sanctionner un comportement illicite (ou les deux).

Les autorités de contrôle devraient déterminer une mesure corrective qui soit «*effective, proportionnée et dissuasive*» (article 83, paragraphe 1), tant dans les cas nationaux (article 55) que dans les cas impliquant un traitement transfrontalier de données à caractère personnel (tel que défini à l'article 4, paragraphe 23).

Les présentes lignes directrices reconnaissent le fait que les législations nationales peuvent fixer des exigences supplémentaires pour la procédure coercitive devant être suivie par les autorités de contrôle. Ces exigences peuvent comprendre, par exemple, l'envoi de notifications, les exigences de formes, les délais pour la présentation d'observations, le recours, l'exécution des règles et le paiement[3].

Ces exigences ne devraient toutefois pas porter atteinte, dans la pratique, au caractère effectif, proportionné ou dissuasif des mesures.

La pratique émergente au sein des autorités de contrôle en matière de protection des données, mais aussi les enseignements tirés d'autres secteurs réglementés préciseront la notion de caractère effectif, proportionné ou dissuasif, de même que la jurisprudence des juridictions appelées à interpréter ces principes.

Pour infliger des amendes effectives, proportionnées et dissuasives, les autorités de contrôle s'en remettront à la définition de la notion d'entreprise fournie par la CJUE aux fins de l'application des articles 101 et 102 du traité FUE, à savoir que la notion d'entreprise **doit s'entendre** comme une unité économique pouvant être formée par la société mère et toutes les filiales concernées. Conformément au droit et à la jurisprudence de l'Union[4], il y a lieu d'entendre par entreprise l'unité économique engagée dans des activités commerciales ou économiques, quelle que soit la personne morale impliquée (considérant 150).

[3] Par exemple, le cadre constitutionnel et le projet de loi sur la protection des données en Irlande prévoient qu'une décision formelle est prise sur l'établissement de la violation et que celle-ci est communiquée aux parties concernées avant l'évaluation de la sévérité de la ou des sanctions. La décision sur l'établissement de la violation ne peut être modifiée pendant l'évaluation de la sévérité de la ou des sanctions.

[4] Dans sa jurisprudence, la Cour de justice en donne la définition suivante: «la notion d'entreprise comprend toute entité exerçant une activité économique, indépendamment du statut juridique de cette entité et de son mode de financement» (arrêt Höfner et Elsner, ECLI:EU:C:1991:161, point 21). Une entreprise «doit être comprise comme désignant une unité économique même si, du point de vue juridique, cette unité économique est constituée de plusieurs personnes physiques ou morales» (arrêt Confederación Española de Empresarios de Estaciones de Servicio, ECLI:EU:C:2006:784, point 40).

3. L'autorité de contrôle compétente appréciera «chaque cas d'espèce»

Les amendes administratives peuvent être infligées pour répondre à toute une série de violations. L'article 83 du règlement prévoit une approche harmonisée des violations des obligations explicitement énumérées aux paragraphes 4 à 6. La législation d'un État membre peut étendre l'application de l'article 83 aux autorités et organismes publics établis dans cet État membre. En outre, la législation des États membres peut permettre ou même rendre obligatoire l'imposition d'une amende en cas de violation d'autres dispositions que celles visées à l'article 83, paragraphes 4 à 6.

Le règlement exige que chaque cas d'espèce soit apprécié[5]. L'article 83, paragraphe 2, est le point de départ d'une telle appréciation individuelle. Ce paragraphe énonce que «[p]*our décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants* (...)». Par conséquent, et compte tenu également du considérant 148[6], l'autorité de contrôle est tenue de choisir la ou les mesures les plus adéquates. Dans les cas mentionnés à l'article 83, paragraphes 4 à 6, ce choix **doit** prendre en considération l'ensemble des mesures correctives, et notamment l'imposition de l'amende administrative appropriée, que ce soit parallèlement à une mesure corrective au titre de l'article 58, paragraphe 2, ou de manière autonome.

Les amendes sont un instrument important que les autorités de contrôle devraient utiliser dans les circonstances appropriées. Les autorités de contrôle sont encouragées à adopter une approche mûrement réfléchie et équilibrée lorsqu'elles appliquent des mesures correctives afin de réagir à la violation d'une manière tant effective et dissuasive que proportionnée. Il ne s'agit pas de considérer les amendes comme un recours ultime ni de craindre de les imposer, mais, en revanche, elles ne doivent pas non plus être utilisées de telle manière que leur efficacité s'en trouverait amoindrie.

[5] Outre l'application des critères prévus à l'article 83, d'autres dispositions sous-tendent cette approche, notamment:

- le considérant 141 («*L'enquête faisant suite à une réclamation devrait être menée, sous contrôle juridictionnel, dans la mesure appropriée au cas d'espèce.*»);
- le considérant 129 («*Les pouvoirs des autorités de contrôle devraient être exercés conformément aux garanties procédurales appropriées prévues par le droit de l'Union et le droit des États membres, d'une manière impartiale et équitable et dans un délai raisonnable. Toute mesure devrait notamment être appropriée, nécessaire et proportionnée en vue de garantir le respect du présent règlement, compte tenu des circonstances de l'espèce...»);*
- l'article 57, paragraphe 1, point f) («*traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association, conformément à l'article 80, examine l'objet de la réclamation, dans la mesure nécessaire...;*»).

[6] *Afin de renforcer l'application des règles du présent règlement, des sanctions y compris des amendes administratives devraient être infligées pour toute violation du présent règlement, en complément ou à la place des mesures appropriées imposées par l'autorité de contrôle en vertu du présent règlement. En cas de violation mineure ou si l'amende susceptible d'être imposée constitue une charge disproportionnée pour une personne physique, un rappel à l'ordre peut être adressé plutôt qu'une amende. Il convient toutefois de tenir dûment compte de la nature, de la gravité et de la durée de la violation, du caractère intentionnel de la violation et des mesures prises pour atténuer le dommage subi, du degré de responsabilité ou de toute violation pertinente commise précédemment, de la manière dont l'autorité de contrôle a eu connaissance de la violation, du respect des mesures ordonnées à l'encontre du responsable du traitement ou du sous-traitant, de l'application d'un code de conduite, et de toute autre circonstance aggravante ou atténuante. L'application de sanctions y compris d'amendes administratives devrait faire l'objet de garanties procédurales appropriées conformément aux principes généraux du droit de l'Union et de la Charte, y compris le droit à une protection juridictionnelle effective et à une procédure régulière.*»

Dans les cas où l'article 65 du règlement reconnaît sa compétence, le CEPD adopte une décision contraignante dans les litiges entre autorités qui concernent en particulier l'établissement d'une violation. Lorsque l'objection pertinente et motivée soulève la question de la conformité de la mesure corrective avec le RGPD, la décision du CEPD examine également la manière dont les principes d'efficacité, de proportionnalité et de dissuasion sont respectés par l'amende administrative proposée dans le projet de décision de l'autorité de contrôle compétente. Les lignes directrices distinctes que le CEPD formulera sur l'application de l'article 65 du règlement apporteront plus de précisions sur le type de décision devant être prise par le CEPD.

4. Une approche harmonisée des amendes administratives dans le domaine de la protection des données requiert la participation active des autorités de contrôle et des échanges d'informations entre elles

Les présentes lignes directrices reconnaissent le fait que le pouvoir d'infliger des amendes représente, pour certaines autorités de contrôle nationales, une nouveauté dans le domaine de la protection des données et qu'il soulève de nombreuses questions de ressources, d'organisation et de procédure. Ainsi, les décisions par lesquelles les autorités de contrôle exercent le pouvoir d'infliger des amendes qui leur a été confié pourront être attaquées devant les juridictions nationales.

Les autorités de contrôle coopèrent entre elles et, le cas échéant, avec la Commission européenne au travers des mécanismes de coopération prévus par le règlement afin de favoriser les échanges d'informations formels et informels, notamment lors d'ateliers. Cette coopération devrait se concentrer sur leur expérience et leur pratique dans l'exercice du pouvoir d'infliger des amendes, le but ultime étant d'atteindre une plus grande cohérence.

Ce partage proactif d'informations, parallèlement à la jurisprudence émergente sur l'exercice de ce pouvoir, pourrait donner lieu à une révision des principes ou de certains points des présentes lignes directrices.

III. Critères d'évaluation visés à l'article 83, paragraphe 2

L'article 83, paragraphe 2, contient une liste de critères que les autorités de contrôle sont censées appliquer lorsqu'elles apprécient l'opportunité d'infliger une amende ainsi que le montant de celle-ci. Il n'est pas recommandé d'effectuer une évaluation répétée des mêmes critères, mais une évaluation qui tienne compte de l'ensemble des circonstances de chaque cas d'espèce, conformément à l'article 83[7].

Les conclusions établies au premier stade de l'évaluation peuvent être utilisées à la seconde étape relative au montant de l'amende, afin d'éviter de devoir effectuer une deuxième évaluation sur la base des mêmes critères.

Les lignes directrices de la présente section visent à aider les autorités de contrôle à interpréter les faits de l'espèce à la lumière des critères énoncés à l'article 83, paragraphe 2.

a) la nature, la gravité et la durée de l'infraction

Presque toutes les obligations qui incombent aux responsables du traitement et aux sous-traitants en vertu du règlement sont classées en fonction de leur **nature** dans les dispositions de l'article 83, paragraphes 4 à 6. En fixant deux montants maximaux différents pour l'amende administrative (10 et 20 millions d'euros), le règlement indique déjà que la violation de certaines dispositions du règlement peut être plus grave que celle d'autres dispositions. Lorsqu'elle évalue les faits de l'espèce à la lumière des critères généraux contenus à l'article 83, paragraphe 2, l'autorité de contrôle compétente peut toutefois considérer que, dans le cas d'espèce, la nécessité de réagir par une mesure corrective sous la forme d'une amende est plus ou moins élevée. Lorsqu'une amende est choisie comme mesure corrective appropriée ou qu'elle figure parmi de telles mesures, le système par paliers prévu par le règlement (article 83, paragraphes 4 à 6) est appliqué pour déterminer l'amende maximale pouvant être infligée en fonction de la nature de la violation en question.

Le considérant 148 introduit la notion de «violations mineures». Ces violations peuvent porter sur une ou plusieurs dispositions du règlement, énumérées à l'article 83, paragraphe 4 ou 5. L'évaluation des critères énoncés à l'article 83, paragraphe 2, peut toutefois amener l'autorité de contrôle à considérer que, dans les circonstances concrètes de l'espèce, la violation n'engendre pas un risque important pour les droits des personnes concernées, par exemple, et qu'elle n'affecte pas l'essence de l'obligation en question. Dans de tels cas, l'amende est parfois (mais pas toujours) remplacée par un rappel à l'ordre.

Le considérant 148 ne fait pas obligation à l'autorité de contrôle de remplacer d'office l'amende par un rappel à l'ordre dans le cas d'une violation mineure («*un rappel à l'ordre peut être adressé plutôt qu'une amende*»), mais il lui laisse la possibilité de le faire après une évaluation concrète de toutes les circonstances de l'espèce.

Le considérant 148 offre la même possibilité de remplacer une amende par un rappel à l'ordre lorsque le responsable du traitement est une personne physique et que l'amende susceptible de lui être infligée constituerait une charge disproportionnée. Le principe est que l'autorité de contrôle doit évaluer si, compte tenu des circonstances du cas d'espèce, l'imposition d'une amende est nécessaire. Si elle tranche en faveur de l'imposition d'une amende, l'autorité de contrôle doit alors également évaluer si cette amende constituerait une charge disproportionnée pour une personne physique.

[7] En raison des règles de procédure nationales qui découlent, dans certains pays, d'exigences constitutionnelles, l'évaluation de la sanction à infliger peut être effectuée séparément après l'évaluation de la question de savoir si une violation a été commise. Le contenu et le degré de précision d'un projet de décision adopté par l'autorité de contrôle principale dans ces pays peuvent s'en trouver limités.

Le règlement n'attribue pas un taux d'amende précis à chaque violation, mais se borne à les plafonner (montant maximal). Cela peut indiquer que la violation des obligations énoncées à l'article 83, paragraphe 4, est moins grave que la violation de celles énumérées à l'article 83, paragraphe 5. La réaction effective, proportionnée et dissuasive à une violation de l'article 83, paragraphe 5, dépendra néanmoins des circonstances de l'espèce.

Il convient de noter que les violations du règlement qui, par leur nature, pourraient relever de la catégorie allant «jusqu'à 10 millions d'euros ou jusqu'à 2 % du chiffre d'affaires annuel mondial total», visée à l'article 83, paragraphe 4, pourraient finalement relever d'une catégorie de niveau supérieur (20 millions d'euros) dans certaines circonstances. Cela pourrait être le cas lorsque ces violations ont fait précédemment l'objet d'une injonction[8] de l'autorité de contrôle que le responsable du traitement ou le sous-traitant n'a pas respectée[9] (article 83, paragraphe 6). Les dispositions de la législation nationale peuvent, dans la pratique, affecter cette évaluation[10]. La nature de la violation, mais aussi «*la portée ou [...] la finalité du traitement concerné, ainsi que [le] nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi*» donneront une indication de la **gravité** de la violation. La survenance de plusieurs violations différentes commises simultanément dans un cas particulier implique que l'autorité de contrôle a la possibilité d'infliger les amendes administratives à un niveau qui rend celles-ci efficaces, proportionnées et dissuasives, dans les limites de la violation la plus grave. Par conséquent, si une violation des articles 8 et 12 a été constatée, l'autorité de contrôle a la possibilité d'appliquer les mesures correctives visées à l'article 83, paragraphe 5, qui correspondent à la catégorie de la violation la plus grave, à savoir celle de l'article 12. La fourniture, à ce stade, d'informations plus détaillées dépasserait le cadre des présentes lignes directrices (des calculs détaillés pourraient en effet faire l'objet d'une éventuelle version ultérieure).

[8] Les injonctions visées à l'article 58, paragraphe 2, sont les suivantes:

- ordonner au responsable du traitement ou au sous-traitant de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits en application du présent règlement;
- ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé;
- ordonner au responsable du traitement de communiquer à la personne concernée une violation de données à caractère personnel;
- imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement;
- ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement en application des articles 16, 17 et 18 et la notification de ces mesures aux destinataires auxquels les données à caractère personnel ont été divulguées en application de l'article 17, paragraphe 2, et de l'article 19;
- ordonner à l'organisme de certification de retirer une certification délivrée en application des articles 42 et 43, ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus satisfaites;
- ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

[9] L'application de l'article 83, paragraphe 6, doit nécessairement tenir compte du droit de procédure national. La législation nationale détermine la manière dont une injonction est émise et notifiée ainsi que le moment à partir duquel elle entre en vigueur. Elle détermine également si un délai peut être accordé pour la mise en conformité. En particulier, l'effet d'un recours sur la force exécutoire d'une injonction devrait être pris en considération.

[10] Les dispositions législatives relatives à la prescription peuvent avoir pour effet qu'une injonction précédente de l'autorité de contrôle ne puisse plus être prise en considération en raison du laps de temps qui s'est écoulé depuis qu'elle a été émise. Dans certaines juridictions, les règles prévoient qu'à l'expiration de la période de prescription concernant une injonction, aucune amende ne peut être infligée pour le non-respect de cette injonction au titre de l'article 83, paragraphe 6. Il incombe à chaque autorité de contrôle dans chaque juridiction de déterminer comment elle sera affectée par ces dispositions.

Les facteurs ci-dessous devraient être évalués en combinaison avec, par exemple, le nombre de personnes concernées et les effets possibles sur celles-ci.

Le **nombre** de personnes concernées devrait être évalué afin de déterminer si le fait est isolé ou s'il est révélateur d'une violation plus systématique ou de l'absence de routines adéquates. Cela ne veut pas dire que des faits isolés ne devraient pas donner lieu à l'application des règles, étant donné qu'ils peuvent tout de même affecter de nombreuses personnes concernées. En fonction des circonstances de l'espèce, ce nombre se rapportera, par exemple, au nombre total de déclarants dans la base de données en cause, au nombre d'utilisateurs d'un service, au nombre de clients ou à la population du pays, le cas échéant.

La **finalité** du traitement doit également être évaluée. L'avis du groupe de travail «article 29» relatif à la limitation des finalités[11] a déjà analysé les deux grands éléments fondateurs de ce principe de la législation sur la protection des données: la spécification des finalités et l'utilisation compatible. Lorsqu'elles apprécient la finalité du traitement dans le contexte de l'article 83, paragraphe 2, les autorités de contrôle devraient se demander dans quelle mesure le traitement respecte les deux éléments clés de ce principe[12]. Dans certaines situations, l'autorité de contrôle peut estimer nécessaire de procéder à une analyse plus approfondie de la finalité du traitement en tant que tel dans l'analyse visée à l'article 83, paragraphe 2.

Si les personnes concernées ont subi un **dommage**, le niveau du dommage doit être pris en considération. Le traitement de données à caractère personnel peut engendrer des risques pour les droits et les libertés de l'individu, comme l'exprime le considérant 75:

> «*Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral, en particulier: lorsque le traitement peut donner lieu à une discrimination, à un vol ou une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, à un renversement non autorisé du processus de pseudonymisation ou à tout autre dommage économique ou social important; lorsque les personnes concernées pourraient être privées de leurs droits et libertés ou empêchées d'exercer le contrôle sur leurs données à caractère personnel; lorsque le traitement concerne des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, la religion ou les convictions philosophiques, l'appartenance syndicale, ainsi que des données génétiques, des données concernant la santé ou des données concernant la vie sexuelle ou des données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes; lorsque des aspects personnels sont évalués, notamment dans le cadre de l'analyse ou de la prédiction d'éléments concernant le rendement au travail, la situation économique, la santé, les préférences ou centres d'intérêt personnels, la fiabilité ou le comportement, la localisation ou les déplacements, en vue de créer ou d'utiliser des profils individuels; lorsque le traitement porte sur des données à caractère personnel relatives à des personnes physiques vulnérables, en particulier les enfants; ou lorsque le traitement porte sur un volume important de données à caractère personnel et touche un nombre important de personnes concernées.*»

[11] WP 203, avis 03/2013 sur la limitation des finalités, consultable à la page: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Voir également WP 217, avis 6/2014 sur la notion d'intérêt légitime du responsable du traitement au titre de l'article 7, page 24, sur la question: «Qu'est-ce qui fait qu'un intérêt est "légitime" ou "illégitime"?»

Si des dommages ont été subis ou sont susceptibles de l'être en raison d'une violation du règlement, l'autorité de contrôle devrait en tenir compte dans le choix de la mesure corrective, même si elle n'est pas elle-même compétente pour octroyer le dédommagement correspondant au préjudice subi.

L'imposition d'une amende ne dépend pas de la capacité de l'autorité de contrôle à établir un lien de cause à effet entre la violation et le préjudice matériel (voir, par exemple, l'article 83, paragraphe 6).

La **durée** de la violation peut être indicative, par exemple:

a) d'un acte intentionnel de la part du responsable du traitement ou

b) d'une omission de prendre les mesures préventives appropriées ou

c) d'une incapacité à mettre en place les mesures techniques et organisationnelles requises.

b) le fait que la violation a été commise délibérément ou par négligence

En général, l'«intention» comprend à la fois la connaissance et la volonté en rapport avec les caractéristiques d'une infraction, tandis que «non délibérément» signifie qu'il n'y a pas eu d'intention de commettre la violation, bien que le responsable du traitement ou le sous-traitant n'ait pas respecté l'obligation de diligence qui lui incombe en vertu de la législation.

Il est généralement admis que les violations commises délibérément, qui manifestent un mépris pour les dispositions législatives, sont plus graves que les violations commises non délibérément et que, par conséquent, elles sont davantage susceptibles de justifier l'application d'une amende administrative. Les conclusions pertinentes concernant la volonté ou la négligence seront tirées sur la base des éléments objectifs de comportement déduits des faits de l'espèce. En outre, la jurisprudence et les pratiques émergentes dans le domaine de la protection des données résultant de l'application du règlement fourniront des exemples de circonstances indiquant des seuils plus précis pour apprécier si la violation a été commise ou non de manière délibérée.

Les circonstances qui dénotent une violation délibérée peuvent être un traitement illicite autorisé explicitement par la haute direction du responsable du traitement, ou contre l'avis du délégué à la protection des données ou au mépris des politiques existantes, par exemple le fait d'obtenir et de traiter des données concernant les salariés d'un concurrent dans l'intention de discréditer celui-ci sur le marché.

Voici d'autres exemples:

- la modification de données à caractère personnel dans le but de donner faussement l'impression que des objectifs ont été atteints – cela s'est vu dans le contexte des objectifs concernant les listes d'attente dans les hôpitaux;
- la vente de données à caractère personnel à des fins de commercialisation, c'est-à-dire le fait de vendre des données comme si la personne concernée avait donné son consentement préalable sans vérifier son avis à ce sujet ou en passant outre celui-ci.

D'autres circonstances, comme le fait de ne pas lire et de ne pas respecter les politiques existantes, les erreurs humaines ou le fait de ne pas vérifier la présence de données à caractère personnel dans les informations publiées, de ne pas appliquer à temps les mises à jour techniques ou de ne pas adopter de politiques (au lieu de s'abstenir uniquement de les appliquer) peuvent dénoter une négligence.

Les entreprises devraient veiller à mettre en place des structures et des ressources adaptées à la nature et à la complexité de leurs activités. En conséquence, les responsables du traitement et les sous-traitants ne peuvent se prévaloir d'un manque de ressources pour justifier des violations de la législation relative à la protection des données. D'après le règlement, les routines et la documentation des activités de traitement s'inspirent d'une approche basée sur le risque.

Il existe des zones grises qui influenceront la prise de décisions quant à l'opportunité d'imposer une mesure corrective. Il se peut que l'autorité doive procéder à une enquête plus poussée afin d'établir les faits de l'espèce et garantir que toutes les circonstances propres à chaque cas d'espèce ont été suffisamment prises en considération.

c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées

Les responsables du traitement et les sous-traitants sont tenus de mettre en œuvre les mesures techniques et organisationnelles afin de garantir un niveau de sécurité adapté au risque, d'effectuer des analyses d'impact relatives à la protection des données et d'atténuer les risques pour les droits et les libertés des personnes résultant du traitement des données à caractère personnel. Toutefois, lorsqu'une violation a lieu et que la personne concernée subit un dommage, la partie responsable devrait faire tout ce qui est en son pouvoir pour réduire les conséquences de la violation pour la personne concernée. Un tel comportement responsable (ou son absence) devrait être pris en compte par l'autorité de contrôle lorsqu'elle choisit la ou les mesures correctives et lorsqu'elle évalue la sanction à infliger dans le cas d'espèce.

Bien que les facteurs aggravants et atténuants soient particulièrement adaptés pour calculer avec précision le montant de l'amende en fonction des circonstances particulières de l'espèce, leur rôle dans le choix de la mesure corrective appropriée ne devrait pas être sous-estimé. Dans les cas où l'évaluation basée sur d'autres critères laisse des doutes à l'autorité de contrôle quant à l'opportunité d'une amende administrative, qu'il s'agisse d'une mesure corrective unique ou d'une mesure combinée à celles visées à l'article 58, ces circonstances aggravantes ou atténuantes peuvent aider à choisir les mesures appropriées en faisant pencher la balance vers celle qui paraît la plus efficace, la plus proportionnée et la plus dissuasive dans le cas concerné.

Cette disposition vise à évaluer le degré de responsabilité du responsable du traitement après que la violation a été commise. Il se peut qu'elle couvre des cas où le responsable du traitement ou le sous-traitant n'a manifestement pas adopté une attitude irresponsable ou négligente, mais où il a fait tout son possible pour corriger son comportement lorsqu'il a pris conscience de la violation.

L'expérience dans le domaine réglementaire accumulée par les autorités de contrôle dans le cadre de la directive 95/46/CE a montré précédemment qu'il peut être approprié de faire preuve d'une certaine flexibilité à l'égard des responsables du traitement ou des sous-traitants qui ont reconnu avoir commis une violation et pris des mesures pour remédier à leur comportement ou en limiter les conséquences. Ces mesures peuvent, par exemple, prendre les formes suivantes (elles ne justifieront toutefois pas une approche plus flexible dans chaque cas):

- la prise de contact avec d'autres responsables du traitement ou sous-traitants susceptibles d'avoir été impliqués dans un élargissement du traitement, par exemple lorsque des données ont été partagées par erreur avec des tiers;
- les mesures prises en temps utile par le responsable du traitement ou le sous-traitant pour empêcher que la violation se poursuive ou qu'elle atteigne un niveau ou un stade tel que ses conséquences auraient été beaucoup plus graves.

d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en œuvre en vertu des articles 25 et 32

Par comparaison avec la directive 95/46/CE sur la protection des données, le règlement responsabilise beaucoup plus le responsable du traitement.

Le degré de responsabilité du responsable du traitement ou du sous-traitant peut être évalué, dans le contexte de l'application d'une mesure corrective appropriée, à partir des questions suivantes:

- le responsable du traitement a-t-il mis en œuvre des mesures techniques suivant les principes de protection des données dès la conception ou par défaut (article 25)?
- le responsable du traitement a-t-il mis en œuvre des mesures organisationnelles qui donnent effet aux principes de protection des données dès la conception et par défaut (article 25) à tous les niveaux de l'organisation?
- le responsable du traitement ou le sous-traitant a-t-il mis en œuvre un niveau approprié de sécurité (article 32)?
- les routines ou politiques pertinentes en matière de protection des données sont-elles connues et appliquées au niveau approprié de la direction au sein de l'organisation? (article 24)

Les articles 25 et 32 du règlement imposent aux responsables du traitement de tenir compte «*de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques*». Ces dispositions instaurent une obligation de moyens plutôt qu'une obligation de résultat, c'est-à-dire que le responsable du traitement doit effectuer les évaluations nécessaires et tirer les conclusions appropriées. La question à laquelle l'autorité de contrôle doit répondre est de savoir dans quelle mesure le responsable du traitement «a fait ce qui pouvait être attendu de lui» compte tenu de la nature, de la finalité ou de l'ampleur du traitement considéré à la lumière des obligations qui lui incombent en vertu du règlement.

Lors de cette évaluation, il convient de tenir dûment compte de toute procédure ou méthode relevant des «bonnes pratiques», lorsqu'elles existent et qu'elles s'appliquent. Il importe également de tenir compte des normes de l'industrie ainsi que des codes de conduite dans le domaine ou le métier concerné. Les codes de conduite pourraient donner une indication de ce qui constitue une pratique courante dans le domaine et du niveau de connaissance des différentes façons de faire face aux problèmes de sécurité habituels liés au traitement.

Si les bonnes pratiques devraient être l'idéal à poursuivre dans l'absolu, les circonstances particulières de chaque cas d'espèce doivent être prises en considération pour évaluer le degré de responsabilité.

e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant

Ce critère vise à évaluer les antécédents de l'entité qui a commis la violation. Les autorités de contrôle devraient être conscientes du fait que cette évaluation peut avoir une portée assez large parce que tout type de violation du règlement, même si elle est de nature différente de celle examinée dans ce cadre par l'autorité de contrôle, pourrait être «pertinente» pour l'évaluation, étant donné qu'elle pourrait donner une indication du niveau général de méconnaissance ou de non-observation des règles en matière de protection des données.

L'autorité de contrôle devrait évaluer les questions suivantes:

- le responsable du traitement ou le sous-traitant a-t-il déjà commis la même violation?
- le responsable du traitement ou le sous-traitant a-t-il violé le règlement de la même manière? (par exemple, à la suite d'une mauvaise connaissance des routines existantes au sein de l'organisation ou d'une évaluation inappropriée des risques, parce qu'il n'a pas répondu en temps voulu aux demandes de la personne concernée ou qu'il a pris un retard injustifié pour répondre aux demandes, etc.)

f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs

L'article 83, paragraphe 2, prévoit qu'il peut être tenu «dûment compte» du degré de coopération pour décider d'infliger ou non une amende administrative ainsi que du montant de celle-ci. Le règlement n'apporte pas de réponse précise à la question de savoir comment il convient de tenir compte des efforts des responsables du traitement ou des sous-traitants pour remédier à une violation déjà établie par l'autorité de contrôle. En outre, il est clair que les critères seraient normalement appliqués lors du calcul du montant de l'amende à infliger.

Toutefois, lorsque l'intervention du responsable du traitement a eu pour effet d'empêcher des conséquences négatives pour les droits des personnes ou de les limiter, son intervention peut également être prise en considération lors du choix d'une mesure corrective proportionnée au cas d'espèce.

La question suivante donne un exemple de cas où la coopération avec l'autorité de contrôle est susceptible d'être prise en considération:

- l'entité a-t-elle réagi d'une manière particulière aux demandes de l'autorité de contrôle pendant la phase d'enquête dans ce cas spécifique, de telle sorte que les incidences sur les droits des personnes concernées ont été considérablement limitées?

Cela dit, il ne serait pas approprié d'accorder une attention supplémentaire à la coopération déjà requise par la loi, par exemple lorsque l'entité est de toute façon tenue de permettre à l'autorité de contrôle d'accéder à ses locaux pour mener ses audits ou ses inspections.

g) les catégories de données à caractère personnel concernées par la violation

Voici quelques exemples de questions clés auxquelles l'autorité de contrôle pourrait estimer nécessaire de répondre, le cas échéant:

- La violation concerne-t-elle le traitement des catégories particulières de données visées aux articles 9 et 10 du règlement?
- Les données sont-elles directement ou indirectement identifiables?

- Le traitement implique-t-il des données dont la diffusion pourrait causer à la personne concernée un dommage immédiat ou une souffrance (qui ne relèvent pas de la catégorie visée aux articles 9 ou 10)?
- Les données sont-elles directement disponibles, sans protections techniques, ou sont-elles cryptées[13]?

h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation

Une autorité de contrôle pourrait être informée de la violation à la suite d'une enquête, de plaintes, d'articles de presse, de dénonciations anonymes ou d'une notification par le responsable du traitement. Le règlement fait obligation au responsable du traitement de signaler à l'autorité de contrôle les violations de données à caractère personnel. Lorsque le responsable du traitement ne fait que remplir cette obligation, le respect de celle-ci ne peut être considéré comme un facteur atténuant. De même, l'autorité de contrôle peut considérer qu'un responsable du traitement ou un sous-traitant qui a fait preuve de négligence en ne notifiant pas la violation, ou en ne la notifiant pas de manière détaillée en raison de son incapacité à évaluer adéquatement l'ampleur de la violation, mérite une sanction plus lourde, c'est-à-dire qu'il est peu probable qu'elle considère cette violation comme étant mineure.

i) lorsque des mesures visées à l'article 58, paragraphe 2, ont été précédemment ordonnées à l'encontre du responsable du traitement ou du sous-traitant concerné pour le même objet, le respect de ces mesures

Il se peut qu'une autorité de contrôle ait déjà un responsable du traitement ou un sous-traitant dans le collimateur s'il a déjà commis une violation et après des échanges nourris avec le délégué à la protection des données, s'il existe. L'autorité de contrôle tiendra dès lors compte des échanges antérieurs.

Contrairement au critère décrit au point e), ce critère d'évaluation ne vise qu'à rappeler aux autorités de contrôle qu'elles doivent se référer aux mesures qu'elles ont elles-mêmes prises précédemment à l'égard du même responsable du traitement ou sous-traitant «*concernant le même objet*»

j) l'application de codes de conduite approuvés en application de l'article 40 ou de mécanismes de certification approuvés en application de l'article 42

Les autorités de contrôle ont le devoir de «*[contrôler] l'application du présent règlement et [de veiller] au respect de celui-ci*» [article 57, paragraphe 1, point a)]. L'application d'un code de conduite approuvé peut être utilisée par le responsable du traitement ou le sous-traitant pour démontrer le respect de la réglementation, conformément à l'article 24, paragraphe 3, l'article 28, paragraphe 5, ou l'article 32, paragraphe 3.

En cas de violation de l'une des dispositions du règlement, l'application d'un code de conduite approuvé pourrait donner à l'autorité de contrôle une indication de la nécessité réelle d'intervenir sous la forme d'une amende administrative efficace, proportionnée et dissuasive ou sous la forme d'autres mesures correctives. D'après l'article 40, paragraphe 4, les codes de conduite approuvés comprendront «*les mécanismes permettant à l'organisme [de contrôle] de procéder au contrôle obligatoire du respect de ses dispositions*».

Lorsque le responsable du traitement ou le sous-traitant applique un code de conduite approuvé, l'autorité de contrôle peut se contenter du fait que la communauté chargée d'administrer le code prend

[13] Le fait que la violation ne concerne que des données indirectement identifiables ou même pseudonymes ou cryptées ne devrait pas toujours être considéré comme un facteur atténuant assimilable à une «prime». Pour ces violations, une évaluation globale des autres critères pourrait faire pencher modérément ou fortement la balance en faveur de l'imposition d'une amende.

IV. Conclusions

Les réflexions sur les questions telles que celles exposées à la section précédente aideront les autorités de contrôle à établir, à partir des faits pertinents de l'espèce, les critères les plus utiles pour décider d'infliger ou non une amende administrative appropriée en plus ou à la place des autres mesures prévues à l'article 58. Compte tenu du contexte qui se dégage d'une telle évaluation, l'autorité de contrôle déterminera la mesure corrective la plus efficace, la plus proportionnée et la plus dissuasive pour réagir à la violation.

L'article 58 donne quelques orientations quant aux mesures qu'une autorité de contrôle peut choisir, étant donné que les mesures correctives sont en soi de nature différente et qu'elles visent essentiellement à atteindre des finalités différentes. Certaines mesures visées à l'article 58 peuvent même se cumuler et constituer ainsi une action régulatrice basée sur plusieurs mesures correctives.

Il n'est pas toujours nécessaire de compléter la mesure par une autre mesure corrective. Par exemple, l'efficacité et le caractère dissuasif de l'intervention de l'autorité de contrôle, qui prend dûment en compte ce qui est proportionné dans le cas d'espèce, peuvent être garantis uniquement par l'amende.

Fondamentalement, les autorités doivent rétablir le respect de la réglementation en recourant à toutes les mesures correctives dont elles disposent. Les autorités de contrôle devront également choisir la voie la plus appropriée à leur action régulatrice. Celle-ci peut comprendre par exemple des sanctions pénales (lorsqu'elles sont disponibles au niveau national).

La pratique consistant à infliger des amendes administratives de manière cohérente dans toute l'Union européenne est en pleine évolution. Des mesures devraient être prises conjointement par les autorités de contrôle pour améliorer en permanence la cohérence. Elles peuvent prendre la forme d'échanges réguliers lors d'ateliers de traitement de cas ou d'autres événements permettant la comparaison de cas tirés des niveaux infranational, national et transnational. La création d'un sous-groupe permanent rattaché à un département compétent du CEPD est recommandée pour soutenir cette activité permanente.

Lignes directrices sur le consentement (WP259)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR
WP259 rév.01

Groupe de travail «Article 29»
Lignes directrices sur le consentement au sens du règlement 2016/679

Adoptées le 28 novembre 2017
Version révisée et adoptée le 10 avril 2018

LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU

TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013

Site web: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Sommaire

1. Introduction

Les présentes lignes directrices fournissent une analyse approfondie de la notion de consentement dans le règlement 2016/679, également connu sous le nom de règlement général sur la protection des données (ci-après le «RGPD»). Le concept de consentement tel qu'utilisé jusqu'à présent dans la directive sur la protection des données (ci-après la «directive 95/46/CE») et dans la directive «vie privée et communications électroniques» a évolué. Le RGPD apporte des clarifications et des précisions complémentaires sur les conditions d'obtention et de démonstration d'un consentement valable. Les présentes lignes directrices se concentrent sur ces modifications afin de fournir des orientations pratiques visant à assurer le respect du RGPD, en s'inspirant de l'avis 15/2011 sur le consentement. Il incombe aux responsables du traitement d'innover afin de trouver de nouvelles solutions qui fonctionnent selon les paramètres de la loi et favorisent davantage la protection des données à caractère personnel ainsi que les intérêts des personnes concernées.

Le consentement demeure l'une des six bases juridiques permettant de traiter des données à caractère personnel, telles qu'énumérées à l'article 6 du RGPD[1]. Lorsqu'il entreprend des activités qui impliquent le traitement de données à caractère personnel, le responsable du traitement doit toujours prendre le temps d'examiner quelle serait la base juridique appropriée pour le traitement envisagé.

En général, le consentement ne constitue une base juridique appropriée que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou de la possibilité de les refuser sans subir de préjudice. Lorsqu'il sollicite un consentement, le responsable du traitement a l'obligation d'évaluer si celui-ci satisfera à toutes les conditions d'obtention d'un consentement valable. S'il a été obtenu dans le plein respect du RGPD, le consentement est un outil qui confère aux personnes concernées un contrôle sur le traitement éventuel de leurs données à caractère personnel. Dans le cas contraire, le contrôle de la personne concernée devient illusoire et le consentement ne constituera pas une base valable pour le traitement des données, rendant de ce fait l'activité de traitement illicite[2].

Les avis existants du groupe de travail «Article 29» (ci-après le «G29») sur le consentement[3] restent pertinents lorsqu'ils sont en phase avec le nouveau cadre juridique, dès lors que le RGPD codifie certaines des orientations et des bonnes pratiques générales du G29 et que la plupart des principaux éléments du consentement restent identiques en vertu du RGPD. Aussi le G29 développe-t-il et complète-t-il dans le présent document ses avis précédents relatifs à des thématiques spécifiques comprenant des références au consentement au sens de la directive 95/46/CE plutôt que de les remplacer.

[1] L'article 9 du RGPD fournit une liste de dérogations possibles à l'interdiction de traiter les catégories particulières de données à caractère personnel. L'une des exceptions citées est lorsque la personne concernée donne son consentement explicite au traitement des données.
[2] Voir également l'avis 15/2011 sur la définition du consentement (CP 187), p. 6-9 et/ou l'avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (WP 217), p. 10, 11, 14 et 15.
[3] Principalement l'avis 15/2011 sur la définition du consentement (WP 187).

Comme indiqué dans l'avis 15/2011 sur la définition du consentement, l'invitation à accepter le traitement de données devrait être régie par des conditions strictes, dès lors qu'elle concerne les droits fondamentaux des personnes concernées et que le responsable du traitement souhaite procéder à un traitement qui serait illicite sans le consentement de la personne concernée[4]. Le rôle essentiel du consentement est souligné par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. En outre, l'obtention d'un consentement n'annule pas ou ne diminue pas de quelque façon que ce soit l'obligation imposée au responsable du traitement de respecter les principes relatifs au traitement énoncés dans le RGPD, notamment dans son article 5 concernant la loyauté, la nécessité, la proportionnalité ainsi que la qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de la personne concernée, cela ne justifie pas la collecte de données excessives au regard d'une finalité spécifique de traitement, ce qui serait foncièrement abusif[5].

Dans le même temps, le G29 est conscient de la révision de la directive «vie privée et communications électroniques» (2002/58/CE). La notion de consentement telle que présentée dans le projet de règlement «vie privée et communications électroniques» reste liée à la notion de consentement au sens du RGPD[6]. En vertu de ce nouvel instrument, les entreprises nécessiteront probablement le consentement des personnes concernées pour la plupart de leurs messages commerciaux en ligne et de leurs appels commerciaux, ainsi que pour leurs méthodes de suivi en ligne, y compris moyennant l'utilisation de cookies, d'applications ou d'autres logiciels. Le G29 a déjà fourni des recommandations et des orientations au législateur européen concernant la proposition de règlement «vie privée et communications électroniques»[7].

Concernant la directive «vie privée et communications électroniques» existante, le G29 note que les références faites à la directive 95/46/CE abrogée s'entendent comme faites au RGPD[8]. Ceci s'applique également aux références faites au consentement dans l'actuelle directive 2002/58/CE, dès lors que le règlement «vie privée et communications électroniques» ne sera pas (encore) entré en vigueur le 25 mai 2018. Selon l'article 95 du RGPD, aucune obligation supplémentaire concernant le traitement de données dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications ne sera imposée dans la mesure où la directive «vie privée et communications électroniques» impose des obligations spécifiques ayant le même objectif. Le G29 note que les exigences relatives au consentement imposées par le RGPD ne sont pas considérées comme des «obligations supplémentaires», mais plutôt comme des conditions préalables essentielles au traitement licite. Aussi les conditions d'obtention d'un consentement valable établies par le RGPD sont-elles applicables dans les situations tombant dans le champ d'application de la directive «vie privée et communications électroniques».

[4] Avis 15/2011 sur la définition du consentement (WP 187), p. 9.
[5] Voir également l'avis 15/2011 sur la définition du consentement (WP 187) et l'article 5 du RGPD.
[6] Selon l'article 9 de la proposition de règlement «vie privée et communications électroniques», la définition et les conditions du consentement figurant à l'article 4, paragraphe 11, et à l'article 7 du RGPD s'appliquent.
[7] Voir l'avis 03/2016 sur l'évaluation et la révision de la directive «vie privée et communications électroniques» (WP 240).
[8] Voir l'article 94 du RGPD.

2. Le consentement dans l'article 4, paragraphe 11, du RGPD

L'article 4, paragraphe 11, du RGPD définit le consentement comme suit: *«toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.»*

Le concept fondamental de consentement reste identique à celui de la directive 95/46/CE; et le consentement constitue l'une des bases juridiques sur lesquelles tout traitement de données à caractère personnel doit être fondé conformément à l'article 6 du RGPD[9]. Outre la définition révisée de l'article 4, paragraphe 11, le RGPD fournit des orientations complémentaires dans son article 7 et dans ses considérants 32, 33, 42 et 43 quant à la façon dont le responsable du traitement doit agir afin de respecter les principaux éléments de l'exigence de consentement.

Enfin, l'introduction de dispositions et de considérants spécifiques sur le retrait du consentement confirme que le consentement devrait être une décision réversible et qu'un certain degré de contrôle par la personne concernée demeure.

3. Éléments d'un consentement valable

L'article 4, paragraphe 11, du RGPD stipule que le consentement de la personne concernée signifie toute:

- manifestation de volonté libre,
- spécifique,
- éclairée et
- univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Les sections suivantes analysent dans quelle mesure la formulation de l'article 4, paragraphe 11, exige des responsables du traitement de modifier leurs demandes/formulaires de consentement afin de se conformer au RGPD[10].

[9] Le consentement était défini par la directive 95/46/CE comme «*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*» qui doit être «*indubitablement donné*» afin de rendre le traitement des données à caractère personnel légitime (article 7, point a), de la directive 95/46/CE). Voir l'avis 15/2011 du G29 sur la définition du consentement (WP 187) pour des exemples d'adéquation du consentement en tant que base juridique. Dans cet avis, le G29 a fourni des orientations afin de distinguer les cas où le consentement est une base juridique appropriée de ceux où les intérêts légitimes (avec une éventuelle possibilité de refus) constituent une base suffisante, ou encore lorsqu'une relation contractuelle serait recommandée. Voir également l'avis 06/2014 du G29, paragraphe III.1.2, p. 15 et suivantes. Le consentement explicite constitue également l'une des exceptions à l'interdiction de traitement portant sur des catégories particulières de données: voir l'article 9 du RGPD.

[10] Pour des orientations concernant les activités de traitement en cours basées sur le consentement au sens de la directive 95/46/CE, voir le chapitre 7 du présent document ainsi que le considérant 171 du RGPD.

3.1. Manifestation de volonté libre[11]

L'adjectif «libre» implique un choix et un contrôle réel pour les personnes concernées. En règle générale, le RGPD dispose que si la personne concernée n'est pas véritablement en mesure d'exercer un choix, se sent contrainte de consentir ou subira des conséquences négatives importantes si elle ne donne pas son consentement, le consentement n'est pas valable[12]. Si le consentement est présenté comme une partie non négociable des conditions générales, l'on considère qu'il n'a pas été donné librement. Le consentement ne sera par conséquent pas considéré comme étant donné librement si la personne concernée n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice[13]. La notion de déséquilibre entre le responsable du traitement et la personne concernée est également prise en compte par le RGPD.

Au moment de déterminer si le consentement est donné librement, il y a également lieu de tenir compte de la situation spécifique de l'intégration du consentement dans un contrat ou de son association à la fourniture d'un service, comme décrit à l'article 7, paragraphe 4. L'article 7, paragraphe 4, a été rédigé de façon non exhaustive par l'usage des termes «entre autres», ce qui signifie qu'une série d'autres situations peut tomber sous le coup de cette disposition. En termes généraux, toute pression ou influence inappropriée exercée sur la personne concernée (pouvant se manifester de différentes façons) l'empêchant d'exercer sa volonté rendra le consentement non valable.

> [Exemple 1]
> Une application mobile d'édition de photos demande à ses utilisateurs d'activer leur localisation GPS afin de pouvoir utiliser ses services. L'application indique également à ses utilisateurs qu'elle utilisera les données collectées à des fins de publicité comportementale. Ni la géolocalisation, ni la publicité comportementale en ligne ne sont nécessaires à la fourniture de services d'édition de photos et toutes deux dépassent de ce fait la fourniture du service de base proposé. Dès lors que les utilisateurs ne peuvent pas utiliser l'application sans consentir à ces finalités, le consentement ne peut pas être considéré comme donné librement.

3.1.1. Déséquilibre des rapports de force

Le considérant 43[14] indique clairement qu'il n'est pas probable que des **autorités publiques** puissent se fonder sur le consentement pour le traitement de données à caractère personnel, dès lors

[11] Dans plusieurs avis, le groupe de travail «Article 29» a exploré les limites du consentement dans des situations où il ne peut être donné librement. C'était notamment le cas de l'avis 15/2011 sur la définition du consentement (WP 187), du document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (WP 131), de l'avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel (WP 48), du deuxième avis 4/2009 sur le traitement de données par l'Agence mondiale antidopage (deuxième avis 4/2009 sur le standard international de l'Agence mondiale antidopage (AMA) sur la protection de la vie privée et des renseignements personnels, sur les dispositions y afférentes du Code de l'AMA et sur d'autres questions concernant la vie privée dans le contexte de la lutte contre le dopage dans le sport menée par l'AMA et des organisations antidopage (nationales) (WP 162)).

[12] Voir l'avis 15/2011 sur la définition du consentement (WP 187), p. 14.

[13] Voir les considérants 42 et 43 du RGPD et l'avis 15/2011 du G29 sur la définition du consentement, adopté le 13 juillet 2011 (WP 187), p. 14.

[14] Le considérant 43 du RGPD prévoit que: *«Pour garantir que le consentement est donné librement, il convient que celui-ci ne constitue pas un fondement juridique valable pour le traitement de données à caractère personnel dans un cas particulier lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière. [...]»*

que lorsque le responsable du traitement est une autorité publique, il existe souvent un déséquilibre manifeste des rapports de force entre le responsable du traitement et la personne concernée. Il est également clair que dans la plupart des cas, la personne concernée n'aura pas de solution alternative réaliste à l'acceptation du traitement (et des conditions de traitement) de ce type de responsable du traitement. Le G29 considère qu'il existe d'autres bases juridiques en principe plus adaptées aux activités des autorités publiques[15].

Sans préjudice de ces considérations générales, le cadre juridique du RGPD n'exclut pas entièrement le recours au consentement en tant que base juridique du traitement de données par des autorités publiques. Les exemples suivants démontrent que le recours au consentement peut être approprié dans certaines circonstances.

> [Exemple 2] Une municipalité locale prévoit des travaux d'entretien de la voirie. Dès lors que les travaux de voirie pourraient perturber la circulation pendant un certain temps, la municipalité offre à ses citoyens la possibilité de s'inscrire sur une liste d'adresses électroniques afin d'être informés de l'état d'avancement des travaux et des retards prévus. La municipalité indique clairement qu'il n'y a aucune obligation de participation et demande le consentement des personnes concernées pour pouvoir utiliser leurs adresses électroniques (exclusivement) à cette fin. Les citoyens qui ne donnent pas leur consentement ne seront en aucun cas privés d'un service de base de la municipalité ou de l'exercice d'un quelconque droit, et sont donc libres de donner ou de refuser leur consentement à ce traitement de leurs données. Toutes les informations sur les travaux de voirie seront également disponibles sur le site Internet de la municipalité.
>
> [Exemple 3] Une propriétaire foncière nécessite certains permis de la part de sa municipalité locale et de l'administration provinciale dans laquelle se situe sa municipalité. Les deux entités publiques ont besoin des mêmes informations afin de délivrer ces permis, mais n'ont pas accès à leurs bases de données respectives. Elles demandent donc les mêmes informations à la propriétaire foncière, qui envoie ses données séparément à ces deux entités publiques. La municipalité et l'administration provinciale demandent son consentement pour fusionner leurs dossiers afin d'éviter une duplication des procédures et de la correspondance. Elles lui assurent que c'est entièrement facultatif et que les demandes de permis seront de toute façon traitées séparément si elle décide de ne pas donner son consentement à la fusion de ses données. La propriétaire foncière peut librement donner son consentement aux autorités concernant la fusion des dossiers.
>
> [Exemple 4] Une école publique demande le consentement de ses étudiants pour utiliser leurs photographies dans une revue étudiante imprimée. Le consentement serait ici le fruit d'un véritable choix dès lors que les étudiants ne se verront pas privés de tout enseignement ou de tout service et pourraient refuser l'utilisation de ces photographies sans aucun préjudice[16].

Un déséquilibre des rapports de force peut également avoir lieu dans le cadre des relations de **travail**[17]. Au vu de la dépendance résultant de la relation employeur/employé, il est peu probable que la personne concernée soit en mesure de refuser de donner son consentement à son employeur concernant le traitement de ses données sans craindre ou encourir des conséquences négatives suite à ce refus. Il est ainsi peu probable qu'un employé soit en mesure de répondre librement à une

[15] Voir l'article 6 du RGPD, notamment le paragraphe 1, points c) et e).
[16] Aux fins de cet exemple, une école publique signifie une école financée par l'État ou un établissement scolaire considéré comme une autorité publique ou un organisme public par le droit national.
[17] Voir également l'article 88 du RGPD, qui souligne la nécessité de protéger les intérêts spécifiques des employés et introduit la possibilité de dérogations dans la législation des États membres. Voir également le considérant 155.

demande de consentement de la part de son employeur visant à activer des systèmes de surveillance, tels que des caméras de surveillance, sur le lieu de travail, ou à remplir des formulaires d'évaluation, sans se sentir obligé de consentir[18]. Aussi le G29 considère-t-il problématique que les employeurs traitent les données à caractère personnel de leurs employés actuels ou potentiels en se fondant sur leur consentement, dès lors qu'il est peu probable que celui-ci soit donné librement. Pour la majorité de ces traitements de données au travail, la base juridique ne peut et ne devrait pas être le consentement des employés (article 6, paragraphe 1, point a)) en raison de la nature de la relation employeur/employé[19].

Cela ne signifie toutefois pas que les employeurs ne peuvent jamais avoir recours au consentement en tant que base juridique pour le traitement de données. Il peut exister des situations où l'employeur est en mesure de démontrer que le consentement est de facto donné librement. Vu le déséquilibre des rapports de force entre un employeur et les membres de son personnel, les employés ne peuvent donner librement leur consentement que dans des situations exceptionnelles, lorsqu'absolument aucune conséquence négative ne résultera de leur refus de donner leur consentement[20].

> [Exemple 5]
> Une équipe de tournage va filmer dans un bureau. L'employeur demande le consentement de tous les employés travaillant dans la zone concernée à être filmés, dès lors qu'ils pourraient apparaître en arrière-plan de la vidéo. Ceux qui ne souhaitent pas être filmés ne sont pénalisés en aucune façon, et disposeront de bureaux équivalents ailleurs dans le bâtiment pendant toute la durée du tournage.

Les déséquilibres de rapports de force ne se limitent pas aux autorités publiques et aux employeurs, ils peuvent également avoir lieu dans d'autres situations. Comme souligné par le G29 dans plusieurs avis, le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes (par ex. coûts supplémentaires importants) si elle ne donne pas son consentement. Le consentement ne sera pas libre lorsque tout élément de contrainte, de pression ou d'incapacité d'exercer un véritable choix sera présent.

3.1.2. Conditionnalité

L'article 7, paragraphe 4, du RGPD joue un rôle crucial au moment de déterminer si le consentement est donné librement[21].

---

[18] Voir l'avis 15/2011 sur la définition du consentement (WP 187), p. 14-16, l'avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel (WP 48), chapitre 10, le document de travail concernant la surveillance des communications électroniques sur le lieu de travail (WP 55), paragraphe 4.2, et l'avis 2/2017 sur le traitement des données au travail (WP 249), paragraphe 6.2.
[19] Voir l'avis 2/2017 sur le traitement des données au travail, pages 6-7.
[20] Voir également l'avis 2/2017 sur le traitement des données au travail, paragraphe 6.2.
[21] Article 7, paragraphe 4, du RGPD: «*Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.*» Voir également le considérant 43 du RGPD, qui prévoit que: «*[...] Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un*

L'article 7, paragraphe 4, du RGPD indique entre autres que le «couplage» du consentement à l'acceptation de conditions générales et la «subordination» de la fourniture d'un contrat ou d'un service à une demande de consentement au traitement de données à caractère personnel non nécessaires à l'exécution dudit contrat ou service ne sont en aucun cas souhaitables. Le consentement est présumé ne pas avoir été donné librement s'il a été donné dans une telle situation (considérant 43). L'article 7, paragraphe 4, cherche à garantir que la finalité du traitement des données à caractère personnel ne soit pas dissimulée ou associée à la fourniture d'un contrat ou d'un service pour lequel ces données à caractère personnel ne sont pas nécessaires. Ce faisant, le RGPD veille à ce que le traitement de données à caractère personnel pour lequel le consentement est sollicité ne puisse pas devenir directement ou indirectement la contre-performance d'un contrat. Ces deux bases juridiques du traitement de données à caractère personnel, à savoir le consentement et le contrat, ne peuvent pas être fusionnées et amalgamées.

L'obligation de consentir au traitement de données à caractère personnel autres que celles strictement nécessaires limite le choix de la personne concernée et fait obstacle au consentement libre. Dès lors que la législation sur la protection des données vise à protéger les droits fondamentaux, le contrôle d'un individu sur ses données à caractère personnel est considéré comme essentiel, et il semble évident que le consentement au traitement de données à caractère personnel non nécessaires ne peut pas être considéré comme une condition sine qua non de l'exécution d'un contrat ou de la fourniture d'un service.

Lorsqu'une demande de consentement est liée à l'exécution d'un contrat par le responsable du traitement, une personne concernée ne souhaitant pas autoriser le traitement de ses données à caractère personnel par le responsable du traitement risque ainsi de voir les services sollicités lui être refusés.

Afin d'évaluer si une telle situation de couplage ou de subordination a lieu, il est important de déterminer le champ d'application du contrat et les données qui seraient nécessaires à l'exécution dudit contrat.
Selon l'avis 06/2014 du G29, la locution «nécessaire à l'exécution d'un contrat» doit être interprétée de façon restrictive. Le traitement doit être nécessaire pour exécuter le contrat conclu avec chacune des personnes concernées. Cela peut par exemple inclure le traitement de l'adresse de la personne concernée afin que des biens achetés en ligne puissent être livrés, ou le traitement des informations de carte de crédit afin de permettre le paiement. Dans le contexte du travail, ce principe peut par exemple autoriser le traitement des informations liées au salaire et au compte bancaire afin de pouvoir verser les salaires[22]. Il doit exister un lien direct et objectif entre le traitement des données et l'objectif d'exécution du contrat.

---

contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.»

[22] Pour plus d'informations et d'exemples, voir l'avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, adopté par le G29 le 9 avril 2014, p. 18-19. (WP 217).

Si un responsable du traitement cherche à traiter des données qui sont effectivement nécessaires à l'exécution d'un contrat, le consentement n'est alors pas la base juridique appropriée[23].

L'article 7, paragraphe 4, n'est pertinent que lorsque les données requises ne sont **pas** nécessaires à l'exécution d'un contrat (y compris la fourniture d'un service) et que l'exécution dudit contrat est conditionnée à l'obtention desdites données sur la base du consentement. Inversement, si le traitement **est** nécessaire à l'exécution du contrat (y compris la fourniture d'un service), l'article 7, paragraphe 4, ne s'applique pas.

> [Exemple 6]
> Une banque demande le consentement de ses clients afin de permettre à de tierces parties d'utiliser leurs informations de paiement à des fins de commercialisation directe. Ce traitement n'est pas nécessaire à l'exécution du contrat avec le client et à la fourniture de services de compte bancaire ordinaires. Si le refus du client de donner son consentement à cette finalité de traitement entraînerait le déni de services bancaires, la fermeture du compte bancaire, ou, selon le cas, une augmentation des frais, le consentement ne peut être donné librement.

Le choix du législateur de souligner, entre autres, la conditionnalité en tant que présomption de l'absence de liberté de consentement démontre qu'il convient d'évaluer soigneusement l'existence d'une telle conditionnalité. La locution «tenir le plus grand compte» utilisée dans l'article 7, paragraphe 4, suggère que le responsable du traitement doit être particulièrement prudent lorsqu'un contrat (qui pourrait inclure la fourniture d'un service) intègre une sollicitation de consentement au traitement de données à caractère personnel.

Dès lors que la formulation de l'article 7, paragraphe 4, n'est pas absolue, il pourrait exister un nombre très limité de cas où cette conditionnalité ne rendrait pas le consentement non valable. Toutefois, le terme «présumé» du considérant 43 indique clairement que de tels cas seront hautement exceptionnels.

En tout état de cause, la charge de la preuve repose sur le responsable du traitement en vertu de l'article 7, paragraphe 4[24]. Cette règle spécifique reflète le principe général de responsabilité omniprésent dans le RGPD. Toutefois, lorsque l'article 7, paragraphe 4, s'applique, il sera plus difficile pour le responsable du traitement de prouver que le consentement a été donné librement par la personne concernée[25].

---

[23] La base juridique appropriée pourrait alors être l'article 6, paragraphe 1, point b) (contrat).
[24] Voir également l'article 7, paragraphe 1, du RGPD qui stipule que le responsable du traitement doit démontrer que le consentement de la personne concernée a été donné librement.
[25] Dans une certaine mesure, l'introduction de ce paragraphe est une codification des orientations existantes du G29. Comme décrit dans l'avis 15/2011, lorsqu'une personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement – en raison de la nature de la relation ou de circonstances particulières – l'on peut être porté à croire que la liberté de consentement est limitée (par ex. dans une relation de travail ou si la collecte des données est effectuée par une autorité publique). Avec l'entrée en vigueur de l'article 7, paragraphe 4, il sera plus difficile pour le responsable du traitement de prouver que le consentement a été donné librement par la personne concernée. Cf. avis 15/2011 sur la définition du consentement (WP 187), p. 14-18.

Le responsable du traitement pourrait avancer que son organisation offre un véritable choix aux personnes concernées si celles-ci peuvent choisir entre un service qui inclut le consentement à l'utilisation de données à caractère personnel à des fins complémentaires et un service équivalent proposé par le même responsable du traitement n'impliquant pas de consentir au traitement de données à caractère personnel à des fins complémentaires. Dans la mesure où il existe la possibilité que le responsable du traitement exécute le contrat ou fournisse le service sans que la personne concernée ne consente aux autres utilisations des données en question, le service n'est pas conditionné. Les deux services doivent cependant être réellement équivalents.

Le G29 considère que le consentement ne peut pas être considéré comme donné librement si un responsable du traitement avance qu'il existe un choix entre son service comprenant le consentement à l'utilisation de données à caractère personnel à des fins complémentaires et un service équivalent proposé par un autre responsable du traitement. Dans un tel cas, la liberté de choix dépendrait de ce que d'autres acteurs du marché font et de si la personne concernée trouve les services de l'autre responsable du traitement réellement équivalents. Cela impliquerait en outre une obligation pour les responsables du traitement de surveiller l'évolution du marché afin de s'assurer que le consentement à leurs activités de traitement est toujours valable, dès lors qu'un concurrent pourrait modifier ultérieurement ses services. Aussi le recours à cet argument implique-t-il que le consentement n'est pas conforme au RGPD.

3.1.3. Nécessité de détailler le consentement

Un service peut impliquer de multiples opérations de traitement à différentes fins. Dans de tels cas, les personnes concernées devraient être libres de choisir quelles finalités elles acceptent, plutôt que de devoir consentir à un ensemble de finalités de traitement. En vertu du RGPD, plusieurs consentements pourraient être nécessaires avant de pouvoir fournir un service dans un cas donné.

Le considérant 43 précise que le consentement est présumé ne pas avoir été donné librement si le processus/la procédure d'obtention du consentement ne permet pas aux personnes concernées de donner un consentement distinct à différentes opérations de traitement des données à caractère personnel (par ex. uniquement pour certaines opérations de traitement et pas pour d'autres) bien que cela soit approprié dans le cas d'espèce. Le considérant 32 stipule que «*Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles*».

Si le responsable du traitement a regroupé plusieurs finalités de traitement et n'a pas cherché à obtenir un consentement distinct pour chaque finalité, la liberté est limitée. Cette nécessité de détailler le consentement est étroitement liée à la nécessité que le consentement soit spécifique, comme décrit à la rubrique 3.2 ci-après. Afin de se conformer aux conditions d'obtention d'un consentement valable lorsque le traitement des données est effectué pour différentes finalités, il convient de détailler le consentement, c.-à-d. de différencier ses différentes finalités et d'obtenir un consentement pour chacune d'entre elles.

[Exemple 7]
Dans la même demande de consentement, un détaillant demande le consentement de ses clients à l'utilisation de leurs données afin de leur envoyer des communications commerciales par courrier électronique et de

partager leurs informations avec d'autres entreprises au sein du même groupe. Ce consentement n'est pas détaillé dès lors qu'il n'y a pas de consentement différencié pour ces deux finalités distinctes et le consentement ne sera donc pas valable. Dans ce cas, un consentement spécifique devrait être obtenu pour envoyer les coordonnées de la personne concernée aux partenaires commerciaux. Un tel consentement spécifique sera jugé valable pour chaque partenaire (voir également la rubrique 3.3.1) dont l'identité a été fournie à la personne concernée au moment de l'obtention de son consentement, à condition que les données leur soient envoyées pour la même finalité (dans cet exemple: une finalité commerciale).

3.1.4. Préjudice

Le responsable du traitement doit démontrer qu'il est possible de refuser ou de retirer son consentement sans subir de préjudice (considérant 42). Par exemple, le responsable du traitement doit prouver que le retrait du consentement n'engendre pas de frais pour la personne concernée et qu'il n'y a donc pas de désavantage évident pour ceux qui retirent leur consentement.

D'autres exemples de préjudice sont la tromperie, l'intimidation, la coercition ou toute conséquence négative importante si la personne concernée refuse de donner son consentement. Le responsable du traitement devrait être en mesure de prouver que la personne concernée dispose d'une véritable liberté de choix concernant la décision de donner ou non son consentement et qu'il est possible de retirer son consentement sans subir de préjudice.

Si un responsable du traitement est en mesure de démontrer qu'un service inclut la possibilité de retirer son consentement sans subir de conséquences négatives, c'est-à-dire sans que la qualité du service ne soit amoindrie au détriment de l'utilisateur, cela peut constituer la preuve que le consentement a été donné librement. Le RGPD n'exclut pas tous les incitants, mais il appartiendra au responsable du traitement de démontrer que le consentement a bien été donné librement en toutes circonstances.

[Exemple 8]
Lorsqu'une utilisatrice télécharge une application mobile de la catégorie «mode de vie», celle-ci sollicite son consentement pour accéder à l'accéléromètre du téléphone. Cet accès n'est pas nécessaire au fonctionnement de l'application, mais est utile pour le responsable du traitement qui souhaite en savoir plus sur les mouvements et les niveaux d'activité de ses utilisateurs. Lorsque l'utilisatrice retire ultérieurement son consentement, elle découvre que l'application ne fonctionne plus que de manière restreinte. Il s'agit d'un exemple de préjudice au sens du considérant 42, ce qui signifie que le consentement n'a jamais été obtenu de façon valable (et le responsable doit de ce fait supprimer toutes les données à caractère personnel concernant les mouvements des utilisateurs collectées de cette manière).

[Exemple 9]
Une personne concernée s'inscrit à un bulletin d'informations d'une enseigne de mode avec des réductions générales. Le détaillant demande le consentement de la personne concernée pour collecter davantage de données sur ses préférences en matière de shopping afin d'adapter ses offres à ses préférences en fonction de son historique d'achat ou d'un questionnaire rempli sur une base volontaire. Si la personne concernée retire ultérieurement son consentement, elle recevra à nouveau des réductions non personnalisées. Il ne s'agit pas ici d'un préjudice, dès lors que seul l'incitant autorisé aura été perdu.

[Exemple 10]
Une revue de mode donne la possibilité à ses lecteurs d'acheter de nouveaux produits de maquillage avant leur lancement officiel.

Les produits seront bientôt disponibles sur le marché, mais les lecteurs de cette revue bénéficient d'une avant-première exclusive sur ces produits. Afin de profiter de cet avantage, les lecteurs doivent donner leur adresse postale et consentir à leur inscription sur la liste de diffusion de la revue. L'adresse postale est nécessaire pour l'expédition et la liste de diffusion est utilisée pour l'envoi d'offres commerciales pour des produits tels que des cosmétiques ou des t-shirts tout au long de l'année.
L'entreprise explique que les données sur la liste de diffusion ne seront utilisées que pour l'envoi de produits et de dépliants publicitaires par la revue elle-même et ne seront en aucun partagées avec d'autres organisations.
Si le lecteur ne souhaite pas révéler son adresse à cette fin, il ne subira aucun préjudice dès lors que les produits lui seront toujours accessibles.

3.2. Spécifique

L'article 6, paragraphe 1, point a), confirme que le consentement de la personne concernée doit être donné en lien avec «une ou plusieurs finalités spécifiques» et que la personne concernée a un choix concernant chacune de ces finalités[26]. L'exigence selon laquelle le consentement doit être «*spécifique*» vise à garantir un certain degré de contrôle utilisateur et de transparence pour la personne concernée. Cette exigence n'a pas été modifiée par le RGPD et reste étroitement liée à l'exigence selon laquelle le consentement doit être «éclairé». Parallèlement, elle doit être interprétée conformément à l'exigence selon laquelle le consentement doit être «détaillé» pour être considéré comme étant «libre»[27]. Pour résumer, afin de se conformer au caractère «spécifique» du consentement, le responsable du traitement doit garantir:

(i) la spécification des finalités en tant que garantie contre tout détournement d'usage,
(ii) le caractère détaillé des demandes de consentement, et
(iii) la séparation claire des informations liées à l'obtention du consentement au traitement des données et des informations concernant d'autres sujets.

Ad. i): Conformément à l'article 5, paragraphe 1, point b), du RGPD, l'obtention d'un consentement valable est toujours précédée de la détermination d'une finalité déterminée, explicite et légitime pour l'activité de traitement envisagée[28]. Combinée à la notion de limitation de la finalité de l'article 5, paragraphe 1, point b), la nécessité d'obtenir un consentement spécifique sert de garantie contre l'élargissement ou l'estompement progressif des fins auxquelles les données sont traitées après qu'une personne concernée a donné son consentement à la collecte initiale de ses données. Ce phénomène, également connu sous le terme de détournement d'usage, constitue un risque pour les personnes concernées dès lors qu'il peut entraîner une utilisation imprévue de leurs données à caractère personnel par le responsable du traitement ou par de tierces parties ainsi que l'affaiblissement du contrôle exercé par la personne concernée.

[26] Des orientations complémentaires concernant la détermination des «finalités» peuvent être trouvées dans l'avis 3/2013 sur la limitation de la finalité (WP 203).
[27] Le considérant 43 du RGPD prévoit qu'un consentement distinct pour différentes opérations de traitement sera nécessaire chaque fois que cela est approprié. Des possibilités de consentement détaillé devraient être prévues afin de permettre aux personnes concernées de donner un consentement distinct à des fins distinctes.
[28] Voir l'avis 3/2013 du G29 sur la limitation de la finalité (WP 203), p. 16: «*Pour ces raisons, les finalités vagues ou générales, telles que des fins d'"amélioration de l'expérience utilisateur", des "fins commerciales", des "fins de sécurité informatique" ou des fins de "recherches futures", ne satisferont généralement pas – si pas davantage détaillées – au critère d'être "spécifiques".*»

Si le responsable du traitement se fonde sur l'article 6, paragraphe 1, point a), la personne concernée doit toujours donner son consentement pour une finalité de traitement spécifique[29]. Conformément au concept de *limitation de la finalité*, à l'article 5, paragraphe 1, point b) et au considérant 32, le consentement peut couvrir différentes opérations dans la mesure où ces opérations partagent la même finalité. Il va sans dire qu'un consentement spécifique ne peut être obtenu que lorsque les personnes concernées sont spécifiquement informées des finalités prévues du traitement des données les concernant.

Sans préjudice des dispositions relatives à la compatibilité des finalités, le consentement doit être spécifique à la finalité. Les personnes concernées donneront leur consentement en sachant qu'elles en possèdent le contrôle et que leurs données ne seront traitées qu'à ces fins spécifiques. Si un responsable du traitement traite des données en se fondant sur le consentement et souhaite traiter les données à une autre finalité, il doit solliciter un consentement complémentaire pour cette autre finalité à moins qu'une autre base juridique ne reflète mieux la situation.

> [Exemple 11] Un réseau de télévision par câble collecte les données à caractère personnel de ses abonnés en se fondant sur leur consentement afin de leur proposer, en fonction de leurs habitudes de visionnement, des suggestions personnalisées de nouveaux films qui pourraient les intéresser. Après un certain temps, le réseau décide qu'il souhaiterait permettre à de tierces parties d'envoyer (ou d'afficher) des publicités ciblées en fonction des habitudes de visionnement des abonnés. Au vu de cette nouvelle finalité, un nouveau consentement sera nécessaire.

Ad. ii): Les mécanismes de consentement ne doivent pas être détaillés uniquement afin de satisfaire à l'exigence selon laquelle le consentement doit être «libre», mais également à l'exigence selon laquelle il doit être «spécifique». Cela signifie qu'un responsable du traitement qui sollicite le consentement pour diverses finalités spécifiques devrait prévoir un consentement distinct pour chaque finalité afin que les utilisateurs puissent donner un consentement spécifique à des finalités spécifiques.

Ad. iii): Enfin, le responsable des données devrait accompagner chacune des demandes de consentement distinctes d'informations spécifiques concernant les données traitées pour chaque finalité afin que les personnes concernées soient conscientes de l'incidence de leur choix. Les personnes concernées pourront ainsi donner leur consentement spécifique. Cette problématique est liée à l'exigence selon laquelle les responsables du traitement doivent fournir des informations claires, telle que décrite à la rubrique 3.3 ci-après.

3.3. Éclairée

Le RGPD renforce l'exigence selon laquelle le consentement doit être éclairé. Conformément à l'article 5 du RGPD, l'exigence de transparence, étroitement liée aux principes de loyauté et de licéité, en est l'un des principes fondamentaux. Fournir des informations aux personnes concernées avant d'obtenir leur consentement est indispensable afin de leur permettre de prendre des décisions en toute connaissance de cause, de comprendre ce à quoi ils consentent et, par exemple, d'exercer leur droit de retirer leur consentement. Si le responsable du traitement ne fournit pas d'informations

[29] Ceci est conforme à l'avis 15/2011 du G29 sur la définition du consentement (WP 187), par exemple p. 19.

accessibles, le contrôle utilisateur devient illusoire et le consentement ne constituera pas une base valable pour le traitement.

Si un responsable du traitement ne respecte pas les exigences relatives à l'obtention d'un consentement éclairé, ce consentement ne sera pas valable et ledit responsable du traitement pourrait se trouver dans une situation d'infraction à l'article 6 du RGPD.

3.3.1. Exigences minimales de contenu pour que le consentement soit «éclairé»

Pour que le consentement soit éclairé, il est nécessaire d'informer la personne concernée de certains éléments cruciaux pour opérer un choix. Aussi le G29 est-il d'avis qu'au moins les informations suivantes sont nécessaires afin d'obtenir un consentement valable:

(i) l'identité du responsable du traitement, [30]
(ii) la finalité de chacune des opérations de traitement pour lesquelles le consentement est sollicité[31],
(iii) les (types de) données collectées et utilisées, [32]
(iv) l'existence du droit de retirer son consentement[33],
(v) des informations concernant l'utilisation des données pour la prise de décision automatisée conformément à l'article 22, paragraphe 2, point c)[34], le cas échéant, et
(vi) des informations sur les risques éventuels liés à la transmission des données en raison de l'absence de décision d'adéquation et de garanties appropriées telles que décrites à l'article 46[35].

Concernant les points (i) et (iii), le G29 signale que si le consentement sollicité servira de base à plusieurs responsables (conjoints) du traitement ou si les données seront transférées à, ou traitées par, d'autres responsables qui souhaitent se fonder sur le consentement original, ces organisations devraient toutes être nommées. Les sous-traitants ne doivent pas impérativement être nommés en vertu des exigences en matière de consentement, bien que pour se conformer aux articles 13 et 14 du RGPD, les responsables du traitement devront fournir une liste complète des destinataires ou des catégories de destinataires, y compris des sous-traitants. Pour conclure, le G29 signale qu'en fonction des circonstances et du contexte de chaque cas, plus d'informations peuvent être nécessaires afin que la personne concernée puisse réellement comprendre les opérations de traitement envisagées.

3.3.2. Comment fournir des informations

[30] Voir également le considérant 42 du RGPD: «*[...] Pour que le consentement soit éclairé, la personne concernée devrait connaître au moins l'identité du responsable du traitement et les finalités du traitement auquel sont destinées les données à caractère personnel. [...]*».
[31] Voir à nouveau le considérant 42 du RGPD.
[32] Voir également l'avis 15/2011 du G29 sur la définition du consentement (WP 187), p. 21-22.
[33] Voir l'article 7, paragraphe 3, du RGPD.
[34] Voir également les lignes directrices du G29 sur les décisions individuelles automatisées et le profilage au titre du règlement 2016/679 (WP 251), paragraphe IV.B, p. 20 et suivantes.
[35] Conformément à l'article 49, paragraphe 1, point a), des informations spécifiques relatives à l'absence des garanties décrites à l'article 46 sont requises lorsqu'un consentement explicite est sollicité. Voir également l'avis 15/2011 du G29 sur la définition du consentement (WP 187), p. 21.

Le RGPD ne stipule pas la forme sous laquelle les informations doivent être fournies afin de satisfaire à l'exigence du consentement éclairé. Cela signifie que les informations valables peuvent être présentées de diverses façons, par exemple sous la forme de communications écrites ou verbales ou de messages audio ou vidéo. Le RGPD fixe toutefois différentes exigences en matière de consentement éclairé, notamment dans son article 7, paragraphe 2, et dans son considérant 32. Cela entraîne une amélioration du niveau de clarté et d'accessibilité des informations.

En sollicitant un consentement, les responsables du traitement devraient s'assurer d'utiliser systématiquement des termes clairs et simples. Cela signifie qu'un message devrait être facilement compréhensible pour l'homme de la rue et pas uniquement pour les avocats. Les responsables du traitement ne peuvent pas utiliser de longues politiques de confidentialité difficiles à comprendre ou des énoncés riches en jargon juridique. Le consentement doit être clair et se distinguer des autres questions, et doit être présenté sous une forme compréhensible et aisément accessible. Cette exigence signifie essentiellement que les informations nécessaires à une prise de décision éclairée concernant le consentement ne peuvent être cachées dans des conditions générales[36].

Un responsable du traitement doit s'assurer que le consentement est fourni sur la base d'informations qui permettent aux personnes concernées d'identifier facilement qui est le responsable des données et de comprendre ce à quoi elles consentent. Le responsable du traitement doit clairement décrire la finalité du traitement des données pour lequel le consentement est sollicité[37].

D'autres orientations spécifiques sur l'accessibilité ont été fournies dans les lignes directrices du G29 sur la transparence. Si le consentement doit être donné par voie électronique, la sollicitation doit être claire et concise. Des informations superposées ou détaillées peuvent être un moyen adéquat de gérer la double obligation que celles-ci soient précises et complètes d'un côté, et compréhensibles d'un autre.

Un responsable du traitement doit évaluer quel type de public fournit des données à caractère personnel à son organisation. Par exemple, si le public cible comprend des mineurs, il convient que le responsable du traitement s'assure que les informations soient compréhensibles pour ceux-ci[38]. Après avoir identifié leur public, les responsables du traitement doivent déterminer quelles informations devraient être fournies et, consécutivement, comment lesdites informations seront présentées aux personnes concernées.

L'article 7, paragraphe 2, traite des déclarations de consentement écrites préformulées concernant également d'autres questions. Lorsque le consentement est requis dans le cadre d'un contrat (papier), la demande de consentement devrait être présentée sous une forme qui la distingue clairement des autres questions. Si le contrat papier comprend de nombreux aspects qui ne sont pas

[36] La déclaration de consentement doit être désignée comme telle. Les énoncés de type «Je suis conscient(e) que...» ne satisfont pas à l'exigence selon laquelle les termes utilisés doivent être clairs.
[37] Voir l'article 4, paragraphe 11, et l'article 7, paragraphe 2, du RGPD.
[38] Voir également le considérant 58 concernant les informations compréhensibles pour les enfants.

liés à la question du consentement à l'utilisation de données à caractère personnel, la question du consentement devrait être traitée sous une forme qui se distingue clairement, ou dans le cadre d'un document distinct. De même, si le consentement est sollicité par voie électronique, la demande de consentement doit être séparée et distincte, elle ne peut être simplement un paragraphe dans les conditions générales, conformément au considérant 32[39]. Afin de s'adapter à de petits écrans ou à des situations où il y a peu d'espace pour les informations, une présentation superposée des informations peut être envisagée, le cas échéant, afin d'éviter toute perturbation excessive de l'expérience utilisateur ou de la conception du produit.

Un responsable du traitement qui se fonde sur le consentement de la personne concernée doit également respecter les différentes obligations en matière d'information énoncées aux articles 13 et 14 afin d'être conforme au RGPD. En pratique, le respect des obligations en matière d'information et de l'exigence selon laquelle le consentement doit être éclairé pourrait entraîner une approche intégrée dans de nombreux cas. Toutefois, cette rubrique est rédigée étant entendu qu'un consentement «éclairé» valable est possible même lorsque tous les éléments des articles 13 et/ou 14 ne sont pas mentionnés lors du processus d'obtention du consentement (ces points devraient bien évidemment être mentionnés ailleurs, par exemple dans l'avis de confidentialité d'une entreprise). Le G29 a publié d'autres lignes directrices sur l'exigence de la transparence.

[Exemple 12]
L'entreprise X est un responsable du traitement qui a reçu des plaintes concernant le manque de clarté des finalités du traitement des données pour lesquelles le consentement a été demandé aux personnes concernées. L'entreprise considère nécessaire de vérifier si les informations de sa demande de consentement sont compréhensibles pour les personnes concernées. X organise des panels volontaires constitués de catégories spécifiques de clients et présente de nouvelles mises à jour de ses informations de consentement à ces audiences tests avant de les communiquer à l'extérieur. La sélection du panel respecte le principe d'indépendance et se fait sur la base de critères assurant un résultat représentatif et non biaisé. Les membres du panel reçoivent un questionnaire et indiquent ce qu'ils ont compris de ces informations et comment ils les évalueraient sur les plans de l'intelligibilité et de la pertinence. Le responsable du traitement poursuit ces tests jusqu'à ce que le panel indique que les informations sont compréhensibles. X établit un rapport du test et le tient à disposition à des fins de référence ultérieure. Cet exemple montre l'une des possibilités dont dispose X pour démontrer que les personnes concernées reçoivent des informations claires avant de consentir au traitement de leurs données à caractère personnel par ses soins.

[Exemple 13]
Une entreprise procède au traitement de données en se fondant sur le consentement. L'entreprise utilise un avis de confidentialité superposé qui inclut une demande de consentement. L'entreprise communique toutes les informations de base concernant le responsable du traitement et les activités de traitement des données envisagées[40]. Toutefois, l'entreprise n'indique pas comment son délégué à la protection des données peut être contacté dans le premier niveau d'informations de son avis de confidentialité. Afin de disposer d'une base

[39] Voir également le considérant 42 et la directive 93/13/CE, notamment son article 5 (termes clairs et compréhensibles et en cas de doute, l'interprétation la plus favorable au consommateur prévaudra) et son article 6 (invalidité des clauses abusives, le contrat continue à exister sans ces clauses s'il reste pertinent, faute de quoi le contrat ne sera plus valable).
[40] Il convient de noter que lorsque l'identité du responsable du traitement ou les finalités du traitement ne sont pas apparentes dans le premier niveau d'informations de l'avis de confidentialité superposé (et se trouvent dans des niveaux inférieurs), il sera difficile pour le responsable du traitement de démontrer que la personne concernée a donné un consentement éclairé, à moins que le responsable du traitement ne soit en mesure de démontrer que la personne concernée en question a accédé à ces informations avant de donner son consentement.

juridique valable au sens de l'article 6, ce responsable du traitement a obtenu un consentement «éclairé» valable, même si les coordonnées du délégué à la protection des données n'ont pas été communiquées à la personne concernée (dans le premier niveau d'informations) conformément à l'article 13, paragraphe 1, point b) ou à l'article 14, paragraphe 1, point b) du RGPD.

3.4. Univoque

Le RGPD établit clairement que le consentement nécessite une déclaration de la part de la personne concernée ou un acte positif clair, ce qui signifie qu'il doit toujours être donné par une déclaration ou un geste actif. Il doit être évident que la personne concernée a consenti au traitement en question.

L'article 2, point h), de la directive 95/46/CE décrit le consentement comme une «manifestation de volonté par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement». L'article 4, paragraphe 11, du RGPD développe cette définition en précisant qu'un consentement valable nécessite une manifestation de volonté *univoque*, par une *déclaration ou par un acte positif clair*, conformément à de précédentes orientations publiées par le G29.

Un «acte positif clair» signifie que la personne concernée doit avoir posé un acte délibéré afin de donner son consentement au traitement spécifique[41]. Le considérant 32 établit des orientations complémentaires à cet égard. Le consentement peut être recueilli au moyen d'une déclaration écrite ou orale (enregistrée), y compris par voie électronique.

Peut-être la façon la plus littérale de satisfaire au critère d'une «déclaration écrite» est-elle de s'assurer que la personne concernée rédige une lettre ou un courrier électronique expliquant au responsable du traitement ce à quoi elle consent. Cela est cependant rarement réaliste. Les déclarations écrites peuvent adopter de nombreuses tailles et formes qui pourraient être conformes au RGPD.

Sans préjudice du droit des contrats (national) existant, le consentement peut être obtenu moyennant une déclaration orale enregistrée, bien qu'il convienne que la personne concernée ait pris bonne note des informations à sa disposition avant sa déclaration de consentement. Le recours à des cases cochées par défaut n'est pas valable en vertu du RGPD. Le silence ou l'inactivité de la personne concernée, ainsi que le simple fait qu'elle continue à utiliser un service, ne peuvent être considérés comme une indication active de choix.

[41] Voir le document de travail des services de la Commission, analyse d'impact, annexe 2, p. 20 et p. 105-106: «*Comme le souligne également l'avis du G29 sur le consentement, il semble essentiel de préciser que l'obtention d'un consentement valable impose de recourir à des mécanismes qui ne laissent aucun doute sur l'intention de la personne concernée de consentir au traitement, tout en expliquant que – dans le contexte de l'environnement en ligne – l'utilisation d'options par défaut, que la personne concernée doit modifier pour refuser le traitement («consentement fondé sur le silence»), ne constitue pas, en soi, un consentement indubitable. Cela conférerait aux individus un plus grand contrôle sur leurs propres données lorsque le traitement est fondé sur leur consentement. Quant à l'incidence sur le responsable du traitement, celle-ci serait faible dès lors que cette mesure ne fait que clarifier et expliciter les implications de l'actuelle directive concernant les conditions d'un consentement valable de la part de la personne concernée. Dans la mesure où la notion de consentement «explicite» clarifierait – en remplaçant la notion de consentement «indubitable» – les modalités et la qualité du consentement et où elle ne vise pas à accroître le nombre de cas et de situations où le consentement (explicite) devrait être utilisé comme base du traitement, l'incidence de cette mesure sur les responsables du traitement ne devrait pas être majeure.*»

[Exemple 14]
Lors de l'installation d'un logiciel, celui-ci demande le consentement de la personne concernée afin d'utiliser des rapports d'erreur non anonymes afin d'améliorer le logiciel. Un avis de confidentialité superposé fournissant les informations nécessaires accompagne la demande de consentement. En cochant activement la case stipulant «Je consens», l'utilisateur est en mesure de poser un «acte positif clair» afin de donner son consentement au traitement.

Un responsable du traitement doit également être conscient que le consentement ne peut être obtenu moyennant la même action que lorsqu'une personne concernée accepte un contrat ou les conditions générales d'un service. L'acceptation globale des conditions générales ne peut être considérée comme un acte positif clair visant à donner son consentement à l'utilisation de données à caractère personnel. Le RGPD n'autorise pas les responsables du traitement à proposer des cases cochées par défaut ou des options de refus nécessitant une action de la personne concernée pour signaler son refus (par exemple des «cases de refus»)[42].

Lorsque le consentement est donné à la suite d'une demande introduite par voie électronique, la demande de consentement ne devrait pas *inutilement* perturber l'utilisation du service pour lequel il est accordé[43]. Un acte positif clair par lequel une personne concernée donne son consentement peut être nécessaire lorsqu'une méthode moins perturbante ou dérangeante entraînerait une certaine ambiguïté. Il peut ainsi être nécessaire qu'une demande de consentement interrompe l'expérience d'utilisation jusqu'à un certain point afin que cette demande soit effective.

Toutefois, les responsables du traitement conservent la liberté de développer un mode de consentement qui convienne à leur organisation dans le respect des exigences du RGPD. À cet égard, les mouvements physiques peuvent être qualifiés d'actes positifs clairs conformes au RGPD.

Les responsables du traitement devraient élaborer des mécanismes de consentement clairs pour les personnes concernées. Ils doivent éviter toute ambiguïté et s'assurer que l'acte par lequel le consentement est accordé puisse se distinguer de tout autre acte. Aussi la simple poursuite de l'utilisation ordinaire d'un site Internet n'est-elle pas un comportement qui permet de supposer une manifestation de volonté de la part de la personne concernée visant à donner son accord à une opération de traitement envisagée.

[Exemple 15]
Faire glisser une barre sur un écran, agiter la main devant une caméra intelligente, faire tourner un smartphone dans le sens des aiguilles d'une montre ou pour former un huit sont différentes possibilités permettant d'indiquer son consentement, pour autant que des informations claires soient fournies et qu'il soit clair que le mouvement en question signifie que la personne concernée accepte une demande spécifique (par ex. «En faisant glisser cette barre vers la gauche, vous consentez à l'utilisation de l'information X à une fin Y. Veuillez répéter le mouvement pour confirmer»). Le responsable du traitement doit être en mesure de démontrer que le consentement a été obtenu de cette façon et les personnes concernées doivent être en mesure de retirer leur consentement aussi facilement qu'elles l'ont donné.

[42] Voir l'article 7, paragraphe 2. Voir également le document de travail n° 02/2013 sur le recueil du consentement pour le dépôt de cookies (WP 208), p. 4-7.
[43] Voir le considérant 32 du RGPD.

[Exemple 16]
Faire défiler une page ou naviguer sur un site Internet ne satisfait pas à l'exigence d'un acte positif clair. La raison en est que la notification indiquant qu'en continuant à faire défiler la page, l'utilisateur donne son consentement peut être difficile à distinguer et/ou peut être manquée lorsqu'une personne concernée fait rapidement défiler de longs textes, et qu'une telle action n'est pas suffisamment univoque.

Dans le contexte numérique, de nombreux services nécessitent des données à caractère personnel afin de fonctionner. Les utilisateurs reçoivent ainsi chaque jour de nombreuses demandes de consentement auxquelles elles doivent répondre par un clic ou en balayant leur écran. Cela peut mener à une certaine lassitude: lorsque trop souvent rencontré, l'effet d'avertissement des mécanismes de consentement diminue.

Il en résulte une situation où les informations de consentement cessent d'être lues. Cela constitue un grand risque pour les personnes concernées, dès lors que le consentement est généralement demandé pour des actions qui seraient illicites sans ce consentement. Le RGPD impose aux responsables du traitement de développer des solutions à ce problème.

Un exemple fréquemment mentionné de solution à ce problème dans un environnement en ligne est l'obtention du consentement des utilisateurs d'Internet moyennant les paramètres de leur navigateur. De tels paramètres devraient être développés conformément aux conditions d'un consentement valable établies par le RGPD, telles que la nécessité que le consentement soit distinct pour chacune des finalités envisagées et que les informations fournies nomment les responsables du traitement.

En tout état de cause, le consentement doit toujours être obtenu avant que le responsable du traitement ne commence à traiter les données à caractère personnel pour lesquelles un consentement est nécessaire. Le G29 a à maintes reprises considéré dans ses avis précédents que le consentement devrait être donné préalablement à l'activité de traitement[44]. Bien que le RGPD n'indique pas littéralement dans son article 4, paragraphe 11, que le consentement doit être donné préalablement à l'activité de traitement, il le laisse cependant clairement entendre. Le titre de l'article 6, paragraphe 1, et la formule «a consenti» utilisée dans l'article 6, paragraphe 1, point a), étayent cette interprétation. Il ressort logiquement de l'article 6 et du considérant 40 qu'une base juridique valable doit exister avant le début du traitement des données. Le consentement devrait donc être donné préalablement à l'activité de traitement. En principe, il peut être suffisant de ne demander le consentement de la personne concernée qu'une seule fois. Les responsables du traitement doivent toutefois obtenir un nouveau consentement spécifique si les finalités du traitement des données changent après l'obtention du consentement ou si une finalité supplémentaire est envisagée.

4. Obtention d'un consentement explicite

Le consentement explicite est requis dans certaines situations où un risque sérieux lié à la protection des données survient, et où un niveau élevé de contrôle sur les données à caractère personnel par la

[44] Le G29 a constamment défendu cette position depuis son avis 15/2011 sur la définition du consentement (WP 187), p. 34-36.

personne concernée est de ce fait jugé approprié. En vertu du RGPD, le consentement explicite joue un rôle dans l'article 9 relatif au traitement portant sur des catégories particulières de données, dans les dispositions relatives aux transferts de données vers des pays tiers ou des organisations internationales de l'article 49[45] ainsi que dans l'article 22 sur la décision individuelle automatisée, y compris le profilage[46].

Le RGPD stipule qu'une «déclaration ou un acte positif clair» est une condition *sine qua non* d'un consentement «standard». Dès lors que les exigences pour un consentement «standard» dans le RGPD sont déjà portées à un niveau supérieur à celles de la directive 95/46/CE, il convient de préciser quels efforts complémentaires un responsable du traitement devrait entreprendre afin d'obtenir le consentement *explicite* d'une personne concernée conformément au RGPD.

Le terme *explicite* se rapporte à la façon dont le consentement est exprimé par la personne concernée. Il implique que la personne concernée doit formuler une déclaration de consentement exprès. Une manière évidente de s'assurer que le consentement est explicite serait de confirmer expressément le consentement dans une déclaration écrite. Le cas échéant, le responsable du traitement pourrait s'assurer que la déclaration écrite est signée par la personne concernée afin de prévenir tout doute potentiel et toute absence potentielle de preuve à l'avenir[47].

Une telle déclaration signée n'est toutefois pas la seule façon d'obtenir le consentement explicite, et on ne peut affirmer que le RGPD préconise des déclarations écrites et signées dans toutes les situations où un consentement explicite valable est nécessaire. Par exemple, dans un contexte numérique ou en ligne, une personne concernée peut être en mesure de fournir la déclaration nécessaire en remplissant un formulaire électronique, en envoyant un courrier électronique, en téléchargeant un document scanné porteur de la signature de la personne concernée ou en utilisant une signature électronique. En théorie, le recours à des déclarations orales peut également être suffisamment explicite pour que le consentement soit valable, bien qu'il puisse être difficile pour le responsable du traitement de prouver que toutes les conditions d'un consentement explicite valable étaient remplies lorsque la déclaration a été enregistrée.
Une organisation peut également obtenir un consentement explicite moyennant une conversation téléphonique, à condition que les informations relatives au choix soient loyales, compréhensibles et

[45] Selon l'article 49, paragraphe 1, point a), du RGPD, un consentement explicite peut lever l'interdiction portant sur les transferts de données vers des pays ne disposant pas d'un niveau adéquat de droit relatif à la protection des données. Voir également le document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive
95/46/CE du 24 octobre 1995 (WP 114), p. 13, où le G29 a indiqué que le recours au consentement pour les transferts de données périodiques ou permanents n'est pas approprié.
[46] Dans son article 22, le RGPD introduit des dispositions visant à protéger les personnes concernées contre les prises de décision uniquement fondées sur un traitement automatisé, y compris le profilage. Les décisions prises sur cette base sont autorisées sous certaines conditions légales. Le consentement joue un rôle clé dans ce mécanisme de protection, dès lors que l'article 22, paragraphe 2, point c) du RGPD stipule clairement qu'un responsable du traitement peut procéder à des prises de décision automatisées, y compris à un profilage, qui pourraient affecter la personne concernée de manière significative s'il dispose du consentement explicite de celle-ci. Le G29 a publié d'autres lignes directrices à cet égard: lignes directrices du G29 sur les décisions individuelles automatisées et le profilage au titre du règlement 2016/679 du G29, 3 octobre 2017 (WP 251).
[47] Voir également l'avis 15/2011 du G29 sur la définition du consentement (WP 187), p. 28.

claires et qu'elle demande une confirmation spécifique de la part de la personne concernée (par ex. appuyer sur un bouton ou donner une conformation orale).

> [Exemple 17] Un responsable du traitement peut également obtenir le consentement explicite d'un visiteur de son site Internet en affichant un écran de consentement explicite qui contient des cases à cocher avec les mentions «Oui» et «Non», à condition que le texte indique clairement qu'il s'agit d'un consentement, par exemple moyennant une formulation telle que «Je consens par la présente au traitement de mes données» et non «Je suis conscient(e) que mes données seront traitées». Il va sans dire que les conditions d'obtention d'un consentement éclairé ainsi que les autres conditions d'obtention d'un consentement valable doivent être satisfaites.

> [Exemple 18] Une clinique de chirurgie esthétique demande le consentement explicite d'un patient afin de transférer son dossier médical à un expert consulté dans le but d'obtenir une deuxième opinion sur l'état du patient. Le dossier médical se présente sous la forme d'un fichier numérique. Au vu de la nature spécifique des informations concernées, la clinique demande la signature électronique de la personne concernée afin d'obtenir un consentement explicite valable et d'être en mesure de démontrer qu'un consentement valable a été obtenu[48].

Une vérification en deux étapes du consentement peut également être une façon de s'assurer que le consentement explicite est valable. Par exemple, une personne concernée reçoit un courrier électronique l'informant de l'intention du responsable du traitement de traiter un dossier contenant des informations médicales. Le responsable du traitement explique dans le courrier électronique qu'il lui demande son consentement pour utiliser un ensemble spécifique d'informations à une fin spécifique. Si la personne concernée consent à l'utilisation de ces données, le responsable du traitement lui demande une réponse par courrier électronique contenant la formule «Je consens». Une fois la réponse envoyée, la personne concernée reçoit un lien de vérification qu'elle doit ouvrir ou un SMS avec un code de vérification afin de confirmer le consentement.

L'article 9, paragraphe 2, ne reconnaît pas le caractère «nécessaire à l'exécution d'un contrat» comme une exception à l'interdiction générale de traiter des catégories particulières de données. Les responsables du traitement et les États membres se trouvant dans cette situation devraient se pencher sur les exceptions spécifiques des points b) à j) de l'article 9, paragraphe 2. Si aucune des exceptions listées aux points b) à j) ne s'applique, l'obtention d'un consentement explicite conforme aux conditions d'un consentement valable définies par le RGPD reste la seule exception licite permettant de traiter de telles données.

> [Exemple 19]
> Une compagnie aérienne, Holiday Airways, propose un service de voyage assisté pour les passagers qui ne peuvent voyager sans assistance, par exemple en raison d'un handicap. Une cliente réserve un vol d'Amsterdam à Budapest et demande une assistance voyage afin de pouvoir monter dans l'avion. Holiday Airways lui demande de fournir des informations sur son état de santé afin de mettre en place les services appropriés (il existe donc de nombreuses possibilités, par ex. un fauteuil roulant à la porte d'arrivée, ou un assistant voyageant avec elle de A à B). Holiday Airways lui demande son consentement explicite pour traiter ses données de santé dans l'objectif d'organiser l'assistance voyage requise. Les données traitées sur la base du consentement sont nécessaires au service requis. En outre, les vols vers Budapest sont toujours disponibles

[48] Cet exemple est sans préjudice du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

sans assistance voyage. Il convient de noter que dès lors que les données sont nécessaires à la fourniture du service requis, l'article 7, paragraphe 4, ne s'applique pas.

[Exemple 20]
Une entreprise prospère est spécialisée dans la fourniture de lunettes de snowboard et de ski personnalisées et d'autres types de lunettes personnalisées pour les sports en extérieur. L'idée est que les clients puissent les porter sans devoir porter leurs propres lunettes. L'entreprise reçoit les commandes à un point central et livre ses produits à travers l'UE à partir d'un lieu unique. Afin de pouvoir fournir ses produits personnalisés aux clients souffrant de myopie, ce responsable du traitement demande leur consentement pour utiliser des informations sur leurs problèmes oculaires. Les clients fournissent les informations de santé nécessaires, telles que des données concernant leurs ordonnances, lorsqu'ils passent commande en ligne. Sans ces données, il est impossible pour l'entreprise de fournir les lunettes personnalisées demandées. L'entreprise propose également une gamme de lunettes avec des corrections standards. Les clients qui ne souhaitent pas partager leurs données de santé pourraient opter pour ces modèles standards. Aussi un consentement explicite est-il nécessaire en vertu de l'article 9 et le consentement peut-il être considéré comme étant donné librement.

5. Conditions supplémentaires d'obtention d'un consentement valable

Le RGPD introduit des conditions exigeant des responsables du traitement qu'ils prennent des dispositions complémentaires afin de s'assurer d'obtenir, de conserver et d'être en mesure de démontrer un consentement valable. L'article 7 du RGPD établit ces conditions supplémentaires d'obtention d'un consentement valable, avec des dispositions spécifiques concernant l'archivage du consentement et le droit de retirer facilement son consentement. L'article 7 s'applique également au consentement auquel il est fait référence dans d'autres articles du RGPD, par ex. dans les articles 8 et 9. Des orientations sur les exigences complémentaires de démonstration d'un consentement valable et de retrait du consentement sont disponibles ci-après.

5.1. Démonstration du consentement

Dans son article 7, paragraphe 1, le RGPD souligne l'obligation explicite du responsable du traitement de démontrer que la personne concernée a donné son consentement. En vertu de l'article 7, paragraphe 1, la charge de la preuve reposera sur le responsable du traitement.

Le considérant 42 prévoit que: *«Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement devrait être en mesure de prouver que ladite personne a consenti à l'opération de traitement».*

Les responsables du traitement sont libres de développer des méthodes adaptées à leurs opérations quotidiennes pour se conformer à cette disposition. Parallèlement, l'obligation qu'a le responsable du traitement de démontrer qu'un consentement valable a été obtenu ne devrait pas en elle-même entraîner des volumes de traitement supplémentaire excessifs. Cela signifie que les responsables du traitement devraient disposer de suffisamment de données pour établir un lien avec le traitement (afin de démontrer que le consentement a été obtenu), mais qu'ils ne devraient pas collecter plus d'informations que nécessaire.

Il incombe au responsable du traitement de prouver qu'un consentement valable a été obtenu de la part de la personne concernée. Le RGPD ne stipule pas précisément comment cela doit être fait. Le responsable du traitement doit toutefois être en mesure de prouver qu'une personne concernée a

donné son consentement dans un cas spécifique. L'obligation de démontrer le consentement s'applique tant que l'activité de traitement en question perdure. Une fois l'activité de traitement terminée, la preuve de consentement ne devrait pas être conservée plus longtemps que strictement nécessaire pour respecter une obligation légale ou à la constatation, à l'exercice ou à la défense de droits en justice, conformément à l'article 17, paragraphe 3, points b) et e).

Le responsable du traitement peut par exemple conserver une trace des déclarations de consentement reçues afin de pouvoir attester de la façon dont le consentement a été obtenu, du moment où il a été obtenu et des informations fournies à la personne concernée à l'époque. Le responsable du traitement doit être en mesure de démontrer que la personne concernée a été informée et que le flux de travail respectait tous les critères pertinents pour un consentement valable. La raison de cette obligation établie par le RGPD est que les responsables du traitement doivent répondre de l'obtention d'un consentement valable de la part des personnes concernées et des mécanismes de consentement qu'ils ont établis. Par exemple, dans l'environnement en ligne, un responsable du traitement pourrait conserver des informations sur la session lors de laquelle le consentement a été donné, parallèlement à la documentation sur le flux de travail relatif au consentement à l'époque de la session et à une copie des informations fournies à l'époque à la personne concernée. Il ne serait pas suffisant de simplement se référer à une configuration adéquate du site Internet en question.

> [Exemple 21] Un hôpital met en place un programme de recherche scientifique, appelé projet X, pour lequel des dossiers dentaires de patients réels sont nécessaires. Les participants sont recrutés par le biais d'appels téléphoniques à des patients ayant volontairement accepté de figurer sur une liste de candidats pouvant être contactés à cette fin. Le responsable du traitement sollicite le consentement explicite des personnes concernées pour utiliser leur dossier dentaire. Le consentement est obtenu lors d'un appel téléphonique par l'enregistrement d'une déclaration orale de la personne concernée dans laquelle celle-ci confirme consentir à l'utilisation de ses données aux fins du projet X.

Le RGPD ne fixe pas de durée spécifique pendant laquelle le consentement restera valable. La durée de validité du consentement dépendra du contexte, de la portée du consentement initial et des attentes de la personne concernée. Si les opérations de traitement changent ou évoluent considérablement, le consentement initial n'est plus valable. Dans ce cas, un nouveau consentement devra être obtenu.

Le G29 recommande, à titre de meilleure pratique, que le consentement soit renouvelé à des intervalles appropriés, toujours à condition que toutes les informations permettent de garantir que la personne concernée reste bien informée de la façon dont ses données sont utilisées et dont elle peut exercer ses droits[49].

5.2. Retrait du consentement

[49] Voir les lignes directrices du G29 sur la transparence. [Citation à finaliser une fois disponible]

Le RGPD accorde une place importante au retrait du consentement. Les dispositions et considérants du RGPD sur le retrait du consentement peuvent être considérés comme la codification de l'interprétation existante de cette thématique dans les avis du G29[50].

L'article 7, paragraphe 3, du RGPD stipule que le responsable du traitement doit s'assurer qu'il soit aussi simple pour la personne concernée de retirer que de donner son consentement, et que cela puisse être fait à tout moment. Le RGPD ne précise pas que la personne concernée doit toujours pouvoir donner et retirer son consentement moyennant la même action.

Toutefois, lorsque le consentement est obtenu par voie électronique uniquement par un clic, une frappe ou en balayant l'écran, les personnes concernées doivent, en pratique, pouvoir retirer ce consentement par le même biais. Lorsque le consentement est obtenu au moyen d'une interface utilisateur spécifique au service (par exemple moyennant un site Internet, une application, un compte avec identifiant, l'interface d'un dispositif IdO ou par courrier électronique), il est évident qu'une personne concernée doit pouvoir retirer son consentement moyennant la même interface électronique, dès lors que changer d'interface à la seule fin de retirer son consentement nécessiterait des efforts inutiles. La personne concernée devrait également être en mesure de retirer son consentement sans subir de préjudice. Cela signifie, entre autres, qu'un responsable du traitement doit proposer la possibilité de retirer son consentement gratuitement ou sans entraîner la diminution du niveau de service[51].

> [Exemple 22] Un festival de musique vend des tickets par le biais d'une plateforme de vente de tickets en ligne. Pour chaque ticket vendu, il demande le consentement de l'acheteur pour utiliser ses coordonnées à des fins commerciales. Afin d'indiquer leur consentement à cette finalité, les clients peuvent sélectionner soit «Non», soit «Oui». Le responsable du traitement informe les clients qu'ils auront la possibilité de retirer leur consentement. Pour ce faire, ils peuvent contacter gratuitement un centre d'appel les jours ouvrables entre 8h et 17h. Dans cet exemple, le responsable du traitement ne respecte pas l'article 7, paragraphe 3, du RGPD. En effet, le retrait du consentement nécessite ici un appel téléphonique pendant les heures ouvrables, ce qui est plus fastidieux que le clic de souris nécessaire pour donner son consentement sur la plateforme de vente de tickets en ligne, accessible 24/7.

Le RGPD considère l'existence d'un retrait facile comme un aspect nécessaire à un consentement valable. Si le droit de retrait ne remplit pas les exigences du RGPD, le mécanisme de consentement du responsable du traitement n'est pas conforme au RGPD. Comme mentionné à la rubrique 3.1 sur la condition d'un consentement *éclairé*, le responsable du traitement doit informer la personne concernée du droit de retrait du consentement avant qu'elle ne donne son consentement, conformément à l'article 7, paragraphe 3 du RGPD. Dans le cadre de l'obligation de transparence,

[50] Le G29 a discuté de cette thématique dans son avis sur le consentement (voir l'avis 15/2011 sur la définition du consentement (WP 187), p. 10, 14-15, 22, 31 et 37-38) et, entre autres, dans son avis sur l'utilisation de données de localisation (voir l'avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée (WP 115), p. 7).

[51] Voir également l'avis 4/2010 du G29 sur le code de conduite de la FEDMA relatif à l'exploitation de données à caractère personnel dans le cadre d'opérations de marketing direct (WP 174) et l'avis sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée (WP 115).

le responsable du traitement doit en outre informer les personnes concernées de la façon dont elles peuvent exercer leurs droits[52].

En règle générale, si le consentement est retiré, toutes les opérations de traitement des données basées sur le consentement ayant eu lieu avant le retrait du consentement – et conformes au RGPD – restent licites, mais le responsable du traitement doit cesser les activités de traitement en question. Si aucune autre base juridique ne justifie le traitement des données (par ex. période de conservation), celles-ci devraient être supprimées par le responsable du traitement[53].

Comme mentionné précédemment dans les présentes lignes directrices, il est essentiel que les responsables des données évaluent les finalités pour lesquelles les données sont effectivement traitées ainsi que les bases juridiques sur lesquelles ce traitement se fonde avant que les données ne soient collectées. Les entreprises ont souvent besoin de données à caractère personnel pour différentes finalités, et le traitement se fonde sur plus d'une base juridique, par ex. les données client peuvent se fonder sur un contrat ainsi que sur le consentement. Le retrait du consentement ne signifie ainsi pas qu'un responsable du traitement doit effacer les données traitées à une fin fondée sur l'exécution d'un contrat avec la personne concernée. Aussi les responsables du traitement devraient-ils d'emblée préciser clairement quelles finalités s'appliquent à quel élément de données et quelle base juridique sert de fondement au traitement.

Les responsables du traitement ont l'obligation de supprimer les données ayant été traitées sur la base du consentement une fois le consentement retiré, à condition qu'aucune autre finalité ne justifie leur conservation[54].
Outre cette situation, couverte par l'article 17, paragraphe 1, point b), une personne concernée peut demander la suppression d'autres données la concernant traitées sur la base d'un autre fondement juridique, par ex. sur la base de l'article 6, paragraphe 1, point b)[55]. Les responsables du traitement sont contraints d'évaluer si la poursuite du traitement des données en question est appropriée, même en l'absence d'une demande d'effacement par la personne concernée[56].

Dans les cas où la personne concernée retire son consentement et où le responsable du traitement souhaite continuer à traiter les données à caractère personnel sur la base d'un autre fondement juridique, il ne peut silencieusement passer du consentement (qui est retiré) à cet autre fondement juridique. Toute modification de la base juridique du traitement doit être notifiée à la personne concernée conformément aux exigences en matière d'information définies aux articles 13 et 14 et en vertu du principe général de transparence.

[52] Le considérant 39 du RGPD, qui se réfère aux articles 13 et 14 du règlement, stipule que *«les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement.»*
[53] Voir article 17, paragraphe 1, point b) et paragraphe 3 du RGPD.
[54] Dans un tel cas, l'autre finalité justifiant le traitement doit disposer de sa propre base juridique. Cela ne signifie pas que le responsable du traitement peut remplacer le consentement par une autre base juridique, voir rubrique 6 ci-après.
[55] Voir article 17, y compris les exceptions qui peuvent s'y appliquer, et le considérant 65 du RGPD.
[56] Voir l'article 5, paragraphe 1, point e), du RGPD.

6. Interactions entre le consentement et les autres bases juridiques définies par l'article 6 du RGPD

L'article 6 établit les conditions d'un traitement des données à caractère personnel licite et décrit six bases juridiques sur lesquelles un responsable du traitement peut se fonder. L'application de l'une de ces six bases juridiques doit être établie avant l'activité de traitement et en lien avec une finalité spécifique[57].

Il est important de noter que si un responsable du traitement choisit de se fonder sur le consentement pour une partie du traitement, il doit être prêt à respecter ce choix et à interrompre le traitement si un individu retire son consentement. Indiquer que les données seront traitées sur la base du consentement, alors que le traitement se fonde sur une autre base juridique, serait fondamentalement déloyal envers les personnes concernées.

Autrement dit, le responsable du traitement ne peut passer du consentement à une autre base juridique. Par exemple, il n'est pas autorisé d'utiliser rétrospectivement la base juridique des intérêts légitimes afin de justifier le traitement lorsque des problèmes ont été rencontrés concernant la validité du consentement. Dès lors que les responsables du traitement ont l'obligation de communiquer la base juridique sur laquelle ils se fondent au moment de la collecte des données, ils doivent avoir défini leur base juridique préalablement à ladite collecte.

7. Domaines critiques spécifiques dans le RGPD

7.1. Les enfants (article 8)

Par rapport à la directive actuelle, le RGPD établit un niveau de protection supplémentaire lorsque les données à caractère personnel de personnes vulnérables, notamment d'enfants, sont traitées. L'article 8 introduit des obligations complémentaires pour garantir un niveau de protection des données à caractère personnel amélioré pour les enfants en ce qui concerne les services de la société de l'information. Les raisons de cette protection améliorée sont précisées au considérant 38: *«[...] ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel [...]».* Le considérant 38 indique également que «*Cette protection spécifique devrait, notamment, s'appliquer à l'utilisation de données à caractère personnel relatives aux enfants à des fins de marketing ou de création de profils de personnalité ou d'utilisateur et à la collecte de données à caractère personnel relatives aux enfants lors de l'utilisation de services proposés directement à un enfant.*» Le mot «notamment» indique que cette protection spécifique ne se limite pas uniquement au marketing ou au profilage, mais inclut «la collecte de données à caractère personnel relatives aux enfants» au sens large.

L'article 8, paragraphe 1, dispose que lorsque le consentement s'applique, en ce qui concerne l'offre directe de services de la société de l'information aux enfants, le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans.

[57] Conformément aux articles 13, paragraphe 1, point c) et 14, paragraphe 1, point c), le responsable du traitement doit en informer la personne concernée.

Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant[58]. Le RGPD est flexible en ce qui concerne l'âge minimum d'un consentement valable: les États membres peuvent prévoir par la loi un âge inférieur, mais il ne peut être inférieur à 13 ans.

Comme mentionné à la rubrique 3.1 sur le consentement éclairé, les informations devront être compréhensibles pour l'audience à laquelle s'adresse le responsable du traitement, avec une attention particulière pour la situation des enfants. Afin d'obtenir un «consentement éclairé» de la part d'un enfant, le responsable du traitement doit expliquer en termes clairs et simples pour les enfants comment il a l'intention d'utiliser les données qu'il collecte[59]. S'il appartient au parent de donner son consentement, un certain nombre d'informations pourrait être nécessaire afin que l'adulte en question puisse prendre une décision éclairée.

Il ressort clairement de ce qui précède que l'article 8 s'appliquera uniquement lorsque les conditions suivantes sont remplies:

- Le traitement est lié à l'offre directe de services de la société de l'information à un enfant[60, 61].
- Le traitement est fondé sur le consentement.

7.1.1. Service de la société de l'information

Afin de déterminer la portée du terme «service de la société de l'information» dans le RGPD, l'article 4, paragraphe 25, du RGPD fait référence à la directive 2015/1535.

Pour évaluer la portée de cette définition, le G29 se réfère également à la jurisprudence de la CJUE[62]. La CJUE a estimé que les *services de la société de l'information* couvrent les contrats et autres services conclus ou transmis en ligne. Lorsqu'un service a deux éléments économiquement

[58] Sans préjudice de la possibilité qu'ont les États membres de déroger par voie législative à la limite d'âge; voir l'article 8, paragraphe 1.

[59] Le considérant 58 du RGPD réaffirme cette obligation, en indiquant que, le cas échéant, un responsable du traitement devrait s'assurer que les informations fournies soient compréhensibles pour des enfants.

[60] Selon l'article 4, paragraphe 25 du RGPD, un service de la société de l'information est un service au sens de l'article 1er, paragraphe 1, point b), de la directive (UE) 2015/1535: *«b) "service", tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. Aux fins de la présente définition, on entend par: i) "à distance", un service fourni sans que les parties soient simultanément présentes; ii) "par voie électronique", un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques; iii) "à la demande individuelle d'un destinataire de services", un service fourni par transmission de données sur demande individuelle.»* Une liste indicative des services non visés par cette définition figure à l'annexe I de ladite directive. Voir aussi le considérant 18 de la directive 2000/31.

[61] Selon l'article 1er de la Convention des Nations unies relative aux droits de l'enfant, «[…] un enfant s'entend de tout être humain âgé de moins de dix-huit ans, sauf si la majorité est atteinte plus tôt en vertu de la législation qui lui est applicable»; cf. Nations unies, résolution 44/25 du 20 novembre 1989 (Convention relative aux droits de l'enfant).

[62] Cf. Cour de justice de l'Union européenne, 2 décembre 2010, affaire C-108/09 (*Ker-Optika*), paragraphes 22 et 28. Par rapport aux «services composites», le G29 se réfère également à l'affaire C-434/15 (*Asociación Profesional Elite Taxi contre Uber Systems Spain SL*), paragraphe 40, qui stipule qu'un service de la société de l'information faisant partie intégrante d'un service global dont l'élément principal n'est pas un service de la société de l'information (dans le cas d'espèce, un service de transport) ne répond pas à la qualification de «service de la société de l'information».

indépendants, l'un d'entre eux étant un élément en ligne, par exemple l'offre ou l'acceptation d'une offre dans le cadre de la conclusion d'un contrat, ou les informations liées aux produits ou services, y compris les activités de marketing, cet élément est considéré comme un service de la société de l'information, tandis que l'autre élément, qui serait la livraison ou la distribution physique de marchandises, n'est pas couvert par la notion de service de la société de l'information. La fourniture d'un service en ligne relèverait également du champ d'application du terme *service de la société de l'information* au sens de l'article 8 du RGPD.

7.1.2. Proposés directement à un enfant

L'inclusion de la formule «proposés directement à un enfant» indique que l'article 8 ne s'applique qu'à certains des services de la société de l'information, et non à tous. À cet égard, si un prestataire de services de la société de l'information indique clairement aux utilisateurs potentiels qu'il ne propose ses services qu'à des personnes âgées de 18 ans ou plus, et que cette affirmation n'est pas contredite par d'autres preuves (tels que le contenu du site Internet ou les plans de commercialisation), ces services ne seront pas considérés comme étant «proposés directement à un enfant» et l'article 8 ne s'appliquera pas.

7.1.3. Âge

Le RGPD stipule que «*Les États membres peuvent prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans.*» Lorsqu'il évalue le public ciblé par ses services, le responsable du traitement doit être conscient des différentes lois nationales. Il convient de noter en particulier qu'un responsable du traitement fournissant un service transfrontalier ne peut pas toujours se contenter de respecter uniquement la législation de l'État membre dans lequel il est principalement établi, mais peut se voir dans l'obligation de respecter les législations nationales respectives de tous les États membres dans lesquels il propose son ou ses services de la société de l'information. Cela sera fonction de si l'État membre décide d'utiliser le lieu d'établissement principal du responsable du traitement comme point de référence dans sa législation nationale, ou bien la résidence de la personne concernée. Avant toute chose, les États membres doivent tenir compte de l'intérêt supérieur de l'enfant lorsqu'ils prennent leur décision. Le groupe de travail encourage les États membres à chercher une solution harmonisée à cet égard.

Lorsqu'ils fournissent des services de la société de l'information à des enfants en se fondant sur le consentement, les responsables du traitement devront s'efforcer raisonnablement de vérifier que l'utilisateur a dépassé l'âge minimum de consentement numérique; ces efforts devraient être proportionnels à la nature des activités de traitement et aux risques qui y sont liés.

Si les utilisateurs indiquent qu'ils ont bien l'âge minimum de consentement numérique, le responsable du traitement peut effectuer des vérifications appropriées pour s'assurer que cette affirmation est vraie. Bien que la nécessité de déployer des efforts raisonnables pour vérifier l'âge n'est pas explicite dans le RGPD, elle est sous-entendue de façon implicite, dès lors que si un enfant donne son consentement alors qu'il n'a pas atteint l'âge requis pour donner un consentement valable en son nom propre, le traitement des données sera illicite.

Si l'utilisateur déclare ne pas avoir atteint l'âge minimum de consentement numérique, le responsable du traitement peut accepter cette déclaration sans vérification complémentaire, mais devra s'assurer d'obtenir une autorisation parentale et de vérifier que la personne fournissant ce consentement est titulaire de la responsabilité parentale.

La vérification de l'âge de la personne concernée ne doit pas entraîner un traitement de données supplémentaire excessif. Le mécanisme choisi pour vérifier l'âge d'une personne concernée devrait comprendre une évaluation des risques liés au traitement envisagé. Dans certaines situations à faible risque, il pourrait être approprié de demander à un nouvel abonné à un service de révéler son année de naissance ou de remplir un formulaire stipulant qu'il est ou n'est pas mineur[63]. En cas de doute, le responsable du traitement devrait réviser ses mécanismes de vérification de l'âge dans un cas donné et évaluer si des méthodes de vérification alternatives sont nécessaires[64].

7.1.4. Consentement des enfants et responsabilité parentale

Concernant l'autorisation d'un titulaire de la responsabilité parentale, le RGPD ne définit pas de méthode pratique d'obtention du consentement parental ou de vérification que la personne en question est habilitée à effectuer cette action[65]. Aussi le G29 recommande-t-il l'adoption d'une approche proportionnée, conformément à l'article 8, paragraphe 2, du RGPD et à l'article 5, paragraphe 1, point c), du RGPD (minimisation des données). Une approche proportionnée pourrait être de se concentrer sur l'obtention d'une quantité limitée d'informations, telles que les coordonnées d'un parent ou d'un tuteur.

Le caractère raisonnable d'une mesure, à la fois pour ce qui est de vérifier qu'un utilisateur est suffisamment âgé pour donner son propre consentement et que la personne donnant son consentement au nom d'un enfant est titulaire de la responsabilité parentale, peut dépendre des risques liés au traitement ainsi que des technologies disponibles. Dans les cas présentant de faibles risques, la vérification de la responsabilité parentale par courrier électronique peut être suffisante. Inversement, dans les situations à risque élevé, il peut être approprié de demander davantage de preuves afin que le responsable du traitement soit en mesure de vérifier et de conserver les informations conformément à l'article 7, paragraphe 1, du RGPD[66]. Des services de vérification tiers de confiance peuvent constituer une solution pour minimiser la quantité de données à caractère personnel traitées par le responsable du traitement.

[63] Bien qu'il ne s'agisse pas d'une solution infaillible dans tous les cas, il s'agit d'un exemple de méthode pour satisfaire à cette disposition.
[64] Voir l'avis 5/2009 du G29 sur les réseaux sociaux en ligne (WP 163).
[65] Le G29 remarque que le titulaire de la responsabilité parentale n'est pas toujours le parent biologique de l'enfant et que la responsabilité parentale peut être détenue par de multiples parties pouvant comprendre des personnes morales comme des personnes physiques.
[66] Par exemple, le responsable du traitement pourrait demander au parent ou tuteur d'effectuer un paiement de 0,01 € moyennant un virement bancaire, comprenant une brève confirmation, dans la communication associée à la transaction, que le titulaire du compte bancaire est le titulaire de la responsabilité parentale de l'utilisateur. Le cas échéant, une méthode alternative de vérification devrait être fournie afin d'éviter tout traitement discriminatoire indu de personnes ne disposant pas d'un compte bancaire.

[Exemple 23] Une plateforme de jeu en ligne souhaite s'assurer que les clients mineurs ne souscrivent ses services qu'avec le consentement de leurs parents ou tuteurs. Le responsable du traitement suit les étapes suivantes:
Étape n° 1: demander à l'utilisateur de préciser s'il a moins ou plus de 16 ans (ou tout autre âge de consentement numérique).
Si l'utilisateur indique ne pas avoir l'âge minimum de consentement numérique:
Étape n° 2: le service informe l'enfant qu'un parent ou tuteur doit donner son consentement ou autoriser le traitement avant que le service ne lui soit fourni. Il est demandé à l'utilisateur de communiquer l'adresse électronique d'un parent ou tuteur.
Étape n° 3: le service contacte le parent ou tuteur, obtient son consentement au traitement par courrier électronique et prend des mesures raisonnables pour confirmer que l'adulte en question est titulaire de la responsabilité parentale.
Étape n° 4: en cas de plainte, la plateforme prend des mesures complémentaires pour vérifier l'âge de l'abonné.
Si la plateforme respecte les autres exigences en matière de consentement, elle peut se conformer aux critères complémentaires de l'article 8 du RGPD en suivant les étapes susmentionnées.

L'exemple montre que le responsable du traitement peut démontrer que des efforts raisonnables ont été entrepris afin de vérifier que le consentement valable a été obtenu pour les services fournis à un enfant. L'article 8, paragraphe 2, ajoute notamment que «*Le responsable du traitement s'efforce raisonnablement de vérifier que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.*»

Il incombe au responsable du traitement de déterminer quelles mesures sont appropriées dans un cas spécifique. En règle générale, les responsables du traitement doivent éviter les solutions de vérification qui impliquent en elles-mêmes une collecte excessive de données à caractère personnel.

Le G29 reconnaît qu'il peut exister des cas où une telle vérification est ardue (par exemple lorsque les enfants fournissant leur propre consentement n'ont pas encore établi une «empreinte identitaire», ou lorsque la responsabilité parentale n'est pas facilement vérifiable). Ces difficultés peuvent être prises en compte au moment de décider des efforts raisonnables, mais l'on s'attend également à ce que les responsables du traitement procèdent à une évaluation constante de leurs procédures et de la technologie disponible.

Pour ce qui est de l'autonomie d'une personne concernée à donner son consentement au traitement de ses données à caractère personnel et à avoir un contrôle total sur le traitement, le consentement donné ou autorisé par un titulaire de la responsabilité parentale quant au traitement des données à caractère personnel d'un enfant peut être confirmé, modifié ou retiré une fois que la personne concernée atteint l'âge minimum de consentement numérique.

En pratique, cela signifie que si l'enfant n'entreprend aucune action, le consentement donné ou autorisé par un titulaire de la responsabilité parentale quant au traitement de données à caractère personnel avant l'âge minimum de consentement numérique restera une base juridique valable pour ledit traitement.

Une fois l'âge minimum de consentement numérique atteint, l'enfant aura la possibilité de retirer son consentement par lui-même, conformément à l'article 7, paragraphe 3. Conformément aux

principes de loyauté et de responsabilité, le responsable du traitement doit informer l'enfant de cette possibilité[67].

Il est important de noter que conformément au considérant 38, le consentement par un parent ou un tuteur n'est pas nécessaire dans le cadre de services de prévention ou de conseil proposés directement à un enfant. Par exemple, la fourniture de services de protection de l'enfant proposés en ligne à un enfant au moyen d'un service de messagerie instantanée en ligne ne devrait pas nécessiter une autorisation parentale préalable.

Enfin, le RGPD stipule que les règles relatives aux exigences d'autorisation parentale par rapport aux mineurs ne devraient pas porter atteinte «au droit général des contrats des États membres, notamment aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.» Aussi les exigences d'un consentement valable pour l'utilisation de données concernant des enfants font-elles partie d'un cadre juridique devant être considéré comme distinct du droit des contrats national. Ce document d'orientation ne traite par conséquent pas de la question de savoir s'il est licite pour un mineur de conclure des contrats en ligne. Ces deux régimes juridiques peuvent s'appliquer simultanément, mais le champ d'application du RGPD ne demande pas l'harmonisation des dispositions nationales du droit des contrats.

7.2. La recherche scientifique

La définition de ce que sont les fins de recherche scientifique a d'importantes répercussions sur le type d'activités de traitement des données qu'un responsable du traitement peut entreprendre. Le terme de «*recherche scientifique*» n'est pas défini par le RGPD. Le considérant 159 stipule que «(...) *Aux fins du présent règlement, le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large* (...).» Toutefois, le G29 considère que cette notion peut être élargie au-delà de sa signification habituelle et estime que la «*recherche scientifique*» signifie dans ce contexte un projet de recherche établi conformément aux normes méthodologiques et éthiques du secteur en question, conformément aux bonnes pratiques.

Lorsque le consentement est la base juridique de la conduite de recherches conformément au RGPD, celui-ci devrait se distinguer des autres exigences de consentement qui servent de norme éthique ou d'obligation procédurale. Un exemple d'une telle obligation procédurale où le traitement n'est pas fondé sur le consentement, mais sur une autre base juridique peut être trouvé dans le règlement relatif aux essais cliniques. Dans le contexte de la législation relative à la protection des données, cette dernière forme de consentement pourrait être considérée comme une garantie complémentaire[68]. Parallèlement, le RGPD ne restreint pas l'application de l'article 6 au seul consentement pour ce qui est du traitement de données à des fins de recherche. Du moment que des garanties appropriées existent, telles que celles énumérées à l'article 89, paragraphe 1, et que le traitement respecte les principes de loyauté, de licéité, de transparence et de minimisation des données ainsi que les droits individuels, d'autres bases juridiques, telles que l'article 6,

[67] Les personnes concernées devraient également être conscientes du droit à l'oubli prévu à l'article 17, particulièrement pertinent pour le consentement donné lorsque la personne concernée était encore un enfant, cf. considérant 63.
[68] Voir également le considérant 161 du RGPD.

paragraphe 1, point e) ou f), peuvent être envisageables[69]. Ceci s'applique également aux catégories particulières de données en vertu de la dérogation définie par l'article 9, paragraphe 2, point j)[70].

Le considérant 33 semble apporter plus de flexibilité au niveau de précision et de détail du consentement dans le cadre de la recherche scientifique. Le considérant 33 prévoit que: «*Souvent, il n'est pas possible de cerner entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient pouvoir donner leur consentement en ce qui concerne certains domaines de la recherche scientifique, dans le respect des normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet*.»

Premièrement, il convient de noter que le considérant 33 n'annule pas les obligations liées à l'exigence d'obtention d'un consentement spécifique. Cela signifie qu'en principe, les projets de recherche scientifique ne peuvent inclure des données à caractère personnel sur la base du consentement de la personne concernée que si leur finalité est décrite avec précision. Dans les cas où les finalités du traitement de données dans le cadre d'un projet scientifique ne peuvent être précisées d'entrée de jeu, le considérant 33 admet, à titre d'exception, que la finalité soit décrite de façon plus générale.

Au vu des conditions strictes établies par l'article 9 du RGPD concernant le traitement portant sur des catégories particulières de données, le G29 observe que lorsque des catégories particulières de données sont traitées sur la base d'un consentement explicite, l'application de l'approche flexible décrite au considérant 33 devra être soumise à une interprétation plus stricte et nécessitera un contrôle minutieux.

Lorsque considéré dans son ensemble, le RGPD ne peut être interprété comme permettant à un responsable du traitement d'éluder le principe clé qu'est la spécification de la finalité pour laquelle le consentement de la personne concernée est sollicité.
Lorsque les finalités de recherche ne peuvent pas être spécifiées dans leur intégralité, le responsable du traitement doit trouver d'autres méthodes pour s'assurer que l'essence des exigences en matière de consentement soit respectée autant que possible, par exemple en faisant en sorte que les personnes concernées puissent donner leur consentement pour une finalité de recherche exprimée en termes plus généraux, ainsi que pour les éventuelles étapes spécifiques du projet de recherche connues à l'avance. Au fur et à mesure que le projet de recherche progresse, le consentement pour les étapes suivantes du projet peut être obtenu avant que lesdites étapes ne débutent. Un tel consentement devrait néanmoins toujours respecter les normes éthiques applicables à la recherche scientifique.

[69] L'article 6, paragraphe 1, point c), peut également s'appliquer aux opérations de traitement spécifiquement exigées par la loi, telles que la collecte de données fiables et solides en vertu du protocole approuvé par les États membres au titre du règlement relatif aux essais cliniques.
[70] En vertu de l'article 9, paragraphe 2, point i), l'essai spécifique de médicaments peut se fonder sur une réglementation européenne ou nationale.

Dans de tels cas, le responsable du traitement peut en outre appliquer des garanties complémentaires. L'article 89, paragraphe 1, souligne par exemple la nécessité d'établir des garanties dans le cadre des activités de traitement de données à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le traitement à ces fins «*est soumis, conformément au présent règlement, à des garanties appropriées pour les droits et libertés de la personne concernée*». La minimisation, l'anonymisation et la sécurité des données sont citées comme garanties possibles[71]. L'anonymisation est la solution privilégiée dans tous les cas où la finalité de la recherche ne nécessite pas le traitement de données à caractère personnel.

La transparence constitue une garantie complémentaire lorsque les circonstances de la recherche ne permettent pas un consentement spécifique. Un manque de précision concernant la finalité peut être compensé par la communication régulière, par les responsables du traitement, d'informations sur l'évolution de la finalité à mesure que le projet progresse afin qu'avec le temps, le consentement soit aussi spécifique que possible. La personne concernée aura ainsi au moins une compréhension générale de l'état de la situation, ce qui lui permettra d'évaluer si elle souhaite ou non recourir à son droit de retrait du consentement conformément à l'article 7, paragraphe 3[72].

L'établissement d'un plan de recherche exhaustif que les personnes concernées pourraient consulter avant de donner leur consentement pourrait également contribuer à compenser le manque de précision de la finalité[73]. Ce plan de recherche devrait décrire les questions de recherche et les méthodes de travail envisagées aussi clairement que possible. Il pourrait également contribuer au respect de l'article 7, paragraphe 1, dès lors que les responsables du traitement doivent être en mesure de prouver que les informations étaient accessibles aux personnes concernées au moment du consentement afin de démontrer la validité du consentement.

Il est important de rappeler que lorsque le consentement est utilisé comme base juridique du traitement, la personne concernée doit avoir la possibilité de retirer ce consentement. Le G29 observe que le retrait du consentement pourrait compromettre les types de recherche scientifique nécessitant des données pouvant être reliées à des individus; le RGPD indique cependant clairement

[71] Voir, par exemple, le considérant 156. Le traitement de données à caractère personnel à des fins scientifiques devrait également respecter d'autres dispositions législatives pertinentes, telles que celles relatives aux essais cliniques; cf. considérant 156, mentionnant le règlement (UE) n° 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain. Voir également l'avis 15/2011 du G29 sur la définition du consentement (WP 187), p. 8: *«En outre, l'obtention d'un consentement n'annule pas les obligations imposées au responsable du traitement par l'article 6 en termes d'équité, de nécessité, de proportionnalité ainsi que de qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de l'utilisateur, cela ne justifie pas la collecte de données excessives au regard d'une fin particulière. […] En principe, le consentement ne doit pas être considéré comme une dérogation à d'autres principes applicables à la protection des données, mais bien comme une garantie. Il s'agit en premier lieu d'une condition de licéité et non d'une renonciation à l'application d'autres principes.»*

[72] D'autres mesures de transparence peuvent également être pertinentes. Lorsque des responsables du traitement procèdent au traitement de données à des fins scientifiques sans être en mesure de communiquer toutes les informations en début du projet, ils pourraient désigner une personne de contact spécifique à laquelle les personnes concernées peuvent adresser leurs questions.

[73] Une telle possibilité peut être trouvée dans l'article 14, paragraphe 1, de l'actuelle loi finlandaise relative à la protection des données (*Henkilötietolaki*, 523/1999).

que le consentement peut être retiré et que les responsables du traitement doivent s'y conformer – la recherche scientifique ne bénéficie d'aucune dérogation à cet égard. Si un responsable du traitement reçoit une demande de retrait du consentement, il doit en principe supprimer immédiatement les données à caractère personnel de la personne concernée s'il souhaite continuer à utiliser les données aux fins de sa recherche[74].

7.3. Les droits des personnes concernées

Si l'activité de traitement des données est fondée sur le consentement d'une personne concernée, cela aura une incidence sur les droits de cette personne. Lorsque le traitement est fondé sur le consentement, les personnes concernées bénéficient du droit à la portabilité des données (article 20). Le droit d'opposition (article 21) ne s'applique en revanche pas lorsque le traitement est fondé sur le consentement, bien que le droit de retrait du consentement puisse entraîner un résultat similaire.

Les articles 16 à 20 du RGPD indiquent que (lorsque le traitement est fondé sur le consentement) les personnes concernées disposent du droit à l'effacement lorsque le consentement a été retiré ainsi que du droit à la limitation, du droit de rectification et du droit d'accès[75].

8. Consentement obtenu en vertu de la directive 95/46/CE

Les responsables du traitement qui traitent actuellement des données sur la base du consentement conformément à la législation nationale relative à la protection des données ne sont pas automatiquement contraints de revoir entièrement leurs relations de consentement avec les personnes concernées en prévision du RGPD. Les consentements obtenus jusqu'ici restent valables dans la mesure où ils sont conformes aux conditions énoncées par le RGPD.

Il est essentiel que les responsables du traitement révisent en profondeur leurs processus de travail et leurs registres avant le 25 mai 2018 afin de s'assurer que les consentements existants sont conformes aux normes du RGPD (voir le considérant 171 du RGPD[76]). En pratique, le RGPD relève la barre pour ce qui est de la mise en œuvre de mécanismes de consentement et introduit une série de nouvelles exigences qui astreignent les responsables du traitement à modifier leurs mécanismes de consentement plutôt que de simplement remanier leur politique de confidentialité[77].

---

[74] Voir également l'avis 05/2014 du G29 sur les techniques d'anonymisation (WP 216).

[75] Lorsque certaines activités de traitement des données sont restreintes conformément à l'article 18 du RGPD, le consentement de la personne concernée peut être nécessaire pour lever ces restrictions.

[76] Le considérant 171 du RGPD prévoit que: «*La directive 95/46/CE devrait être abrogée par le présent règlement. Les traitements déjà en cours à la date d'application du présent règlement devraient être mis en conformité avec celui-ci dans un délai de deux ans après son entrée en vigueur. Lorsque le traitement est fondé sur un consentement en vertu de la directive 95/46/CE, il n'est pas nécessaire que la personne concernée donne à nouveau son consentement si la manière dont le consentement a été donné est conforme aux conditions énoncées dans le présent règlement, de manière à ce que le responsable du traitement puisse poursuivre le traitement après la date d'application du présent règlement. Les décisions de la Commission qui ont été adoptées et les autorisations qui ont été accordées par les autorités de contrôle sur le fondement de la directive 95/46/CE demeurent en vigueur jusqu'à ce qu'elles soient modifiées, remplacées ou abrogées.*»

[77] Comme indiqué dans l'introduction, le RGPD apporte des clarifications et des précisions complémentaires sur les conditions d'obtention et de démonstration d'un consentement valable. Nombre de ces nouvelles dispositions s'inspirent de l'avis 15/2011 sur le consentement.

Par exemple, dès lors que le RGPD stipule qu'un responsable du traitement doit être en mesure de démontrer qu'un consentement valable a été obtenu, tous les consentements présumés dont aucune trace n'est conservée seront automatiquement en deçà des normes de consentement établies par le RGPD et devront être renouvelés. De même, dès lors que le RGPD requiert une «déclaration ou un acte positif clair», tous les consentements présumés fondés sur une forme d'action plus implicite de la part de la personne concernée (par ex. une case cochée par défaut) ne seront pas conformes aux normes de consentement du RGPD.

En outre, afin d'être en mesure de démontrer qu'un consentement valable a été obtenu ou de permettre une indication plus détaillée des souhaits de la personne concernée, les opérations et les systèmes informatiques pourraient nécessiter une révision. Des mécanismes permettant aux personnes concernées de retirer facilement leur consentement doivent également être rendus disponibles, tout comme des informations sur la procédure de retrait du consentement. Si les procédures existantes d'obtention et de gestion du consentement ne sont pas conformes aux normes du RGPD, les responsables du traitement devront obtenir un nouveau consentement conforme au RGPD.

D'un autre côté, dès lors que tous les éléments énumérés aux articles 13 et 14 ne doivent pas nécessairement être présents pour que le consentement soit éclairé, les obligations d'information complémentaires fixées par le RGPD ne s'opposent pas nécessairement à la continuité de la validité du consentement obtenu avant l'entrée en vigueur du RGPD (voir page 17 ci-dessus). Il convient de signaler que la directive 95/46/CE n'établissait aucune nécessité d'informer les personnes concernées de la base sur laquelle se fondait le traitement de leurs données.

Si un responsable du traitement estime que le consentement obtenu en vertu de l'ancienne législation ne satisfera pas aux normes de consentement du RGPD, il doit prendre des mesures afin de se conformer auxdites normes, par exemple en renouvelant le consentement au moyen d'un mécanisme conforme au RGPD. En vertu du RGPD, il n'est pas possible de passer d'une base juridique à une autre. Si un responsable du traitement n'est pas en mesure de renouveler le consentement au moyen d'un mécanisme conforme au RGPD et n'est pas non plus en mesure de se conformer au nouveau règlement en fondant – à titre exceptionnel – son traitement des données sur une autre base juridique tout en s'assurant que le traitement ainsi poursuivi respecte les principes de loyauté et de responsabilité, les activités de traitement devront être interrompues. En tout état de cause, le responsable du traitement doit respecter les principes de licéité, de loyauté et de transparence du traitement.

-*-*-*-*-*-*-*-*-*-*-*-*-* **FIN DU DOCUMENT** *-*

Lignes directrices sur la transparence (WP260)

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

17/FR

WP260 rev.01

Groupe de travail «Article 29»

Lignes directrices sur la transparence au sens du règlement (UE) 2016/679

Adoptées le 29 novembre 2017

Version révisée et adoptée le 11 avril 2018

LE GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU

TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la direction C (Droits fondamentaux et État de droit) de la direction générale de la justice et des consommateurs de la Commission européenne, B-1049 Bruxelles, Belgique, bureau MO-59 02/013

Site web: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

Table des matières

GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

Introduction

1. Les présentes lignes directrices du groupe de travail «Article 29» (G29) fournissent une orientation pratique ainsi qu'une aide à l'interprétation concernant la nouvelle obligation de transparence applicable au traitement des données à caractère personnel au titre du règlement général sur la protection des données[1] (ci-après le «**RGPD**»). La transparence est une obligation globale au sens du RGPD qui s'applique à trois domaines centraux: 1) la communication aux personnes concernées d'informations relatives au traitement équitable de leurs données; 2) la façon dont les responsables du traitement communiquent avec les personnes concernées sur leurs droits au titre du RGPD; et 3) la façon dont les responsables du traitement facilitent l'exercice par les personnes concernées de leurs droits[2]. Dans la mesure où le respect de la transparence à l'égard du traitement des données est requis par la directive (UE) 2016/680[3], ces lignes directrices s'appliquent également à l'interprétation de ce principe[4]. À l'instar de toutes les lignes directrices du G29, les présentes lignes directrices ont vocation à être généralement applicables et pertinentes pour les responsables du traitement, quelles que soient les caractéristiques sectorielles, d'entreprise ou réglementaires spécifiques à un responsable du traitement en particulier. À ce titre, ces lignes directrices ne peuvent pas prendre en compte les nuances et nombreuses variables pouvant apparaître dans le contexte des obligations de transparence d'un secteur, d'une entreprise ou d'un domaine réglementé spécifique. Néanmoins, elles visent, d'une part, à permettre aux responsables du traitement de comprendre, à un degré élevé, l'interprétation par le G29 de ce que les obligations de transparence impliquent dans la pratique et, d'autre part, à indiquer l'approche que les responsables du traitement devraient, selon le G29, adopter en matière de transparence tout en intégrant les notions d'équité et de responsabilité dans leurs mesures de transparence.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

[2] Ces lignes directrices fixent les principes généraux relatifs à l'exercice des droits des personnes concernées plutôt qu'elles traitent des modalités spécifiques à chacun des droits de ces personnes au titre du RPGD.

[3] Directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

[4] Bien que la transparence ne constitue pas l'un des principes relatifs au traitement des données à caractère personnel énoncés à l'article 4 de la directive (UE) 2016/680, le considérant 26 de ladite directive dispose que «tout traitement de données à caractère personnel doit être licite, loyal et transparent à l'égard des personnes physiques concernées».

2. La transparence est une caractéristique bien ancrée dans le droit de l'Union européenne[5]. Son objectif premier est de susciter la confiance dans les processus applicables aux citoyens en leur permettant de comprendre et, au besoin, de contester lesdits processus. C'est également une expression du principe d'équité à l'égard du traitement des données à caractère personnel énoncé à l'article 8 de la charte des droits fondamentaux de l'Union européenne. Conformément au RGPD [article 5, paragraphe 1, point a)[6]], outre l'obligation de traiter les données de manière licite et loyale, la transparence constitue désormais un aspect fondamental des principes relatifs au traitement[7]. La transparence est intrinsèquement liée à l'équité et au nouveau principe de responsabilité au titre du RGPD. Il ressort également de l'article 5, paragraphe 2, que le responsable du traitement doit toujours être en mesure de démontrer que les données à caractère personnel sont traitées de manière transparente au regard de la personne concernée[8]. Parallèlement, le principe de responsabilité exige la transparence des opérations de traitement afin que les responsables du traitement puissent démontrer qu'ils satisfont aux obligations leur incombant en vertu du RGPD[9].

3. Conformément au considérant 171 du RGPD, lorsqu'un traitement a commencé avant le 25 mai 2018, le responsable du traitement doit s'assurer que le traitement en question satisfait aux obligations de transparence applicables à compter du 25 mai 2018 (conjointement à toutes les autres obligations au titre du RGPD). Cela signifie que les responsables du traitement devraient réexaminer avant le 25 mai 2018 toutes les informations fournies aux personnes concernées sur le traitement de leurs données à caractère personnel (par exemple, dans des déclarations ou des avis sur la protection de la vie privée, etc.) afin de garantir qu'ils respectent les obligations de transparence énoncées dans les présentes lignes directrices. Lorsque des modifications ou des ajouts sont apportés à ces informations, les responsables du traitement doivent clairement indiquer aux personnes concernées que ces modifications ont été effectuées aux fins de la conformité au RGPD. Le G29 recommande que ces modifications ou ajouts soient activement portés à l'attention des personnes concernées et exige, au minimum, que les responsables du traitement rendent ces informations publiques (par exemple sur leur site web). Néanmoins, si les modifications ou ajouts sont substantiels, ils devraient, conformément aux points 29 à 32 ci-après, être portés activement à l'attention des personnes concernées.

[5] L'article premier du TUE décrit les décisions comme étant prises «*dans le plus grand respect possible du principe d'ouverture et le plus près possible des citoyens*»; l'article 11, paragraphe 2, dispose que «*[l]es institutions entretiennent un dialogue ouvert, transparent et régulier avec les associations représentatives et la société civile*»; et l'article 15 du TFUE prévoit, entre autres, que les citoyens de l'Union ont un droit d'accès aux documents des institutions, organes et organismes de l'Union et que les institutions, organes et organismes de l'Union ont pour obligation d'assurer la transparence de leurs travaux.

[6] «Les données à caractère personnel doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée».

[7] Dans la directive 95/46/CE, le principe de transparence n'était évoqué qu'au considérant 38 au titre d'une obligation de traiter les données de manière loyale, sans être expressément mentionné à l'article 6, paragraphe 1, point a), de ladite directive.

[8] Conformément à l'article 5, paragraphe 2, du RGPD, il incombe au responsable du traitement de démontrer la transparence (parallèlement aux cinq autres principes liés au traitement des données tels qu'énoncés à l'article 5, paragraphe 1) en vertu du principe de responsabilité.

[9] L'obligation imposée aux responsables du traitement de mettre en œuvre des mesures techniques et organisationnelles pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au RGPD est établie à l'article 24, paragraphe 1.

4. Le principe de transparence, lorsqu'il est respecté par les responsables du traitement, permet aux personnes concernées de contrôler leurs données à caractère personnel et d'exiger des responsables du traitement et des sous-traitants qu'ils rendent des comptes à cet égard, par exemple en accordant ou en retirant leur consentement éclairé et en faisant appliquer leurs droits en tant que personnes concernées[10]. Le concept de transparence du RGPD est centré sur l'utilisateur plutôt que sur l'aspect légal et se concrétise dans plusieurs articles par des exigences pratiques spécifiques applicables aux responsables du traitement et aux sous-traitants. Les exigences pratiques (informations) sont exposées aux articles 12 à 14 du RGPD. Cependant, la qualité, l'accessibilité et l'intelligibilité des informations sont aussi importantes que le contenu réel des informations en matière de transparence devant être fournies aux personnes concernées.

5. Les exigences de transparence du RGPD s'appliquent quelle que soit la base juridique du traitement et tout au long du cycle de vie de ce dernier. Cela ressort clairement de l'article 12, qui prévoit que la transparence s'applique aux étapes suivantes du cycle de traitement des données:

- avant ou au commencement du cycle de traitement des données, c'est-à-dire quand les données à caractère personnel sont collectées auprès de la personne concernée ou obtenues d'une autre manière;
- tout au long de la période de traitement, c'est-à-dire lors des communications avec les personnes concernées sur leurs droits; et
- à des moments spécifiques du cycle de traitement, par exemple en cas de violation des données ou de modification substantielle du traitement.

Signification de la transparence

6. La transparence n'est pas définie dans le RGPD. Le considérant 39 du RGPD fournit des informations sur le sens et l'effet du principe de transparence dans le cadre du traitement des données:

> *«Le fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées. Le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples. Ce principe vaut, notamment, pour les informations communiquées aux personnes*

[10] Voir, par exemple, les conclusions de l'avocat général Cruz Villalón (9 juillet 2015) dans l'affaire Bara (affaire C-201/14), point 74: *«cette exigence d'information des personnes concernées par le traitement de leurs données personnelles, qui garantit la transparence de tout traitement, est d'autant plus importante qu'elle conditionne l'exercice par les intéressés de leur droit d'accès aux données traitées, visé à l'article 12 de la directive 95/46, et de leur droit d'opposition au traitement desdites données, défini à l'article 14 de la même directive».*

concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement.»

Éléments de transparence au titre du RGPD

7. Les articles clés du RGPD en matière de transparence, en ce qu'ils s'appliquent aux droits de la personne concernée, se trouvent au chapitre III (Droits de la personne concernée). L'article 12 établit les règles générales applicables: à la communication d'informations aux personnes concernées (visée aux articles 13 et 14); aux communications adressées aux personnes concernées au sujet de l'exercice de leurs droits (visées aux articles 15 à 22); et aux communications concernant les violations de données (article 34). Plus particulièrement, l'article 12 impose que les informations ou communications en question respectent les règles suivantes:

- elles doivent être concises, transparentes, compréhensibles et aisément accessibles (article 12, paragraphe 1);
- des termes clairs et simples doivent être employés (article 12, paragraphe 1);
- l'exigence concernant l'utilisation de termes clairs et simples est particulièrement importante pour les informations destinées à des enfants (article 12, paragraphe 1);
- les informations sont fournies «*par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique*» (article 12, paragraphe 1);
- lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement (article 12, paragraphe 1); et
- elles sont généralement fournies gratuitement (article 12, paragraphe 5).

«*concises, transparentes, compréhensibles et aisément accessibles*»

8. L'exigence que la fourniture d'informations aux personnes concernées et que les communications qui leur sont adressées soient réalisées d'une manière «concise et transparente» signifie que les responsables du traitement devraient présenter les informations/communications de façon efficace et succincte afin d'éviter de noyer d'informations les personnes concernées. Ces informations devraient être clairement différenciées des autres informations non liées à la vie privée telles que des clauses contractuelles ou des modalités d'utilisation générale. Dans un contexte en ligne, la présentation d'une déclaration de confidentialité ou de dispositions en matière de protection de la vie privée sur différents niveaux permet à la personne concernée de naviguer jusqu'à la section spécifique de la déclaration ou de l'avis sur la protection de la vie privée à laquelle elle souhaite accéder immédiatement plutôt que de devoir faire défiler de grandes quantités de texte à la recherche d'informations spécifiques.

9. L'exigence que ces informations soient «compréhensibles» signifie qu'elles devraient pouvoir être comprises par la majorité du public visé. La compréhensibilité est étroitement liée à l'exigence d'utiliser des termes clairs et simples. Un responsable du traitement connaît les personnes au sujet desquelles il collecte des informations et peut

mettre à profit ces connaissances pour déterminer ce que ce public serait susceptible de comprendre. Par exemple, un responsable du traitement collectant les données à caractère personnel de professionnels exerçant une activité peut partir du principe que son public a un niveau de compréhension plus élevé que si ce même responsable du traitement collectait des données à caractère personnel concernant des enfants. Si les responsables du traitement ont des incertitudes sur le niveau de compréhensibilité et de transparence des informations et l'efficacité des interfaces utilisateur, avis, politiques, etc., ils ont la possibilité de tester ces derniers au moyen, par exemple, de différents mécanismes tels que des panels d'utilisateurs, des tests de lisibilité, des interactions formelles et informelles ou en dialoguant, entre autres, avec des groupes d'entreprises, des organisations représentatives des intérêts des consommateurs ou des organes réglementaires, le cas échéant.

10. Un aspect primordial du principe de transparence mis en lumière dans ces dispositions est que la personne concernée devrait être en mesure de déterminer à l'avance ce que la portée et les conséquences du traitement englobent afin de ne pas être prise au dépourvu à un stade ultérieur quant à la façon dont ses données à caractère personnel ont été utilisées. C'est également un aspect important du principe d'équité au titre de l'article 5, paragraphe 1, du RGPD, qui est d'ailleurs lié au considérant 39 qui dispose que «*[l]es personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel*». Plus particulièrement, en ce qui concerne les traitements de données complexes, techniques ou non prévus, la position du G29 est que les responsables du traitement devraient, en plus de fournir les informations énoncées aux articles 13 et 14 (traitées ultérieurement dans les présentes lignes directrices), définir séparément et de façon claire les principales *conséquences* du traitement: autrement dit, quel sera réellement l'effet du traitement spécifique décrit dans une déclaration ou un avis sur la protection de la vie privée pour la personne concernée. En accord avec le principe de responsabilité et conformément au considérant 39, les responsables du traitement devraient évaluer s'il existe pour les personnes physiques concernées par ce type de traitement des risques particuliers qu'il conviendrait de porter à l'attention des intéressés. Une telle évaluation pourrait permettre de fournir un aperçu des types de traitement susceptibles d'avoir le plus d'impact sur les libertés et droits fondamentaux des personnes concernées quant à la protection de leurs données à caractère personnel.

11. Le critère «aisément accessible» signifie que la personne concernée ne devrait pas avoir à rechercher les informations mais devrait pouvoir tout de suite y accéder: par exemple, ces informations pourraient être communiquées aux personnes concernées directement ou au moyen d'un lien qui leur serait adressé; leur emplacement et accès pourraient être clairement indiqués, ou elles pourraient être fournies en réponse à une question en langage naturel (par exemple, dans une déclaration de confidentialité ou des dispositions en matière de protection de la vie privée sur différents niveaux en ligne, dans une FAQ, au moyen de fenêtres contextuelles qui s'activent quand une personne concernée remplit un formulaire en ligne, ou dans un contexte numérique interactif avec un agent conversationnel. Ces mécanismes sont présentés plus en détail ci-après, notamment aux points 33 à 40).

Exemple

Chaque entreprise disposant d'un site internet devrait publier une déclaration ou un avis sur la protection de la vie privée sur son site. Un lien direct vers cette déclaration ou cet avis sur la protection de la vie privée devrait être clairement visible sur chaque page de ce site internet sous un terme communément utilisé (comme «Confidentialité», «Politique de confidentialité» ou «Avis de protection de la vie privée»). Les textes ou liens dont la mise en page ou le choix de couleur les rend moins visibles ou difficiles à trouver sur une page web ne sont pas considérés comme aisément accessibles.

Pour les applications, les informations nécessaires devraient également être accessibles dans la boutique en ligne avant leur téléchargement. Une fois l'application installée, les informations doivent rester aisément accessibles dans l'application. L'un des moyens de satisfaire à cette exigence est de garantir que les informations ne se trouvent jamais à plus de deux actions/clics sur l'écran (par exemple, en intégrant une option «Confidentialité»/«Protection des données» dans le menu de l'application). De plus, les informations personnelles en question devraient être propres à l'application et ne devraient pas simplement être la politique de confidentialité générique de l'entreprise qui est propriétaire de l'application ou qui la met à la disposition du public.

Le G29 recommande à titre de bonne pratique que, dans un contexte en ligne, un lien vers la déclaration ou l'avis sur la protection de la vie privée soit fourni au point de collecte des données à caractère personnel, ou que ces informations soient consultables sur la même page que celle où les données à caractère personnel sont collectées.

«Des termes clairs et simples»

12. S'agissant d'informations *écrites* (et lorsque des informations écrites sont prononcées oralement ou, au moyen de méthodes audio/audiovisuelles, notamment pour les personnes concernées souffrant de problèmes de vue), les bonnes pratiques applicables au principe d'écriture claire doivent être suivies[11]. Une exigence linguistique semblable (pour des «termes clairs et compréhensibles») a été précédemment appliquée dans la législation de l'Union[12] et est explicitement énoncée dans le contexte du consentement au considérant 42 du RGPD[13]. L'exigence de termes clairs et simples signifie que les informations devraient être fournies de la façon la plus simple possible, en évitant des phrases et des structures linguistiques complexes. Les informations devraient être concrètes et fiables; elles ne devraient pas être formulées dans des termes abstraits ou ambigus ni laisser de place à différentes interprétations. Plus particulièrement, les finalités et fondements juridiques du traitement des données à caractère personnel devraient être clairs.

[11] Voir «Rédiger clairement» par la Commission européenne (2011), consultable à l'adresse suivante: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5/language-fr.

[12] Article 5 de la directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs.

[13] Le considérant 42 dispose qu'une déclaration de consentement rédigée préalablement par le responsable du traitement devrait être fournie sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples, et qu'elle ne devrait contenir aucune clause abusive.

Exemples de mauvaises pratiques

Les phrases suivantes ne sont pas suffisamment claires pour que l'on comprenne la finalité du traitement:

- «*Il se peut que nous utilisions vos données à caractère personnel en vue de la mise au point de nouveaux services*» (car le sens de «services» et la façon dont ces données permettront de mettre au point les services ne sont pas clairs);
- «*Il se peut que nous utilisions vos données à caractère personnel à des fins de recherche*» (car le type de «recherche» visé n'est pas clair); et
- «*Il se peut que nous utilisions vos données à caractère personnel afin de vous proposer des services personnalisés*» (car ce qu'englobe la «personnalisation» n'est pas clair).

Exemples de bonnes pratiques[14]

- «*Nous conserverons votre historique d'achats et utiliserons les informations sur les produits que vous avez précédemment achetés afin de vous suggérer d'autres produits qui, selon nous, devraient vous intéresser*» (cette phrase indique clairement quels types de données seront traités, que la personne concernée recevra des annonces ciblées pour des produits et que ses données seront utilisées à cette fin);
- «*Nous conserverons et analyserons les informations relatives à vos dernières visites sur notre site internet et la façon dont vous naviguez parmi les différentes rubriques de notre site à des fins d'analyse en vue de comprendre comment les internautes consultent notre site pour, à terme, le rendre plus intuitif*» (cette phrase indique clairement le type de données qui seront traitées et le type d'analyses que le responsable du traitement effectuera); et
- «*Nous conserverons une trace des articles de notre site internet sur lesquels vous avez cliqué et utiliserons ces informations pour adapter la publicité sur ce site à vos centres d'intérêt, que nous avons déterminés au vu des articles que vous avez lus*» (cette phrase indique clairement en quoi consiste la personnalisation et la façon dont les centres d'intérêt de la personne concernée ont été identifiés).

13. Les qualificatifs tels que «peut», «pourrait», «certains», «souvent» et «possible» sont à éviter. Lorsque les responsables du traitement choisissent d'utiliser des termes vagues, ils devraient pouvoir, conformément au principe de responsabilité, démontrer que ce type

[14] L'exigence de transparence est entièrement valable, indépendamment de l'exigence imposée aux responsables du traitement de garantir l'existence d'une base juridique pour le traitement en vertu de l'article 6.

de langage ne pouvait pas être évité et prouver qu'il ne nuit pas à l'équité du traitement. Les paragraphes et phrases doivent être bien structurés, en utilisant des puces et des alinéas pour indiquer les relations hiérarchiques. Il convient de privilégier la forme active plutôt que la voix passive et d'éviter les mots superflus. Les informations fournies à une personne concernée ne devraient pas contenir de termes trop juridiques, techniques ou spécialisés. Lorsque les informations sont traduites dans une ou plusieurs langues, le responsable du traitement doit s'assurer que toutes les traductions sont exactes et que la phraséologie et la syntaxe ont du sens dans la langue cible de sorte que le texte traduit n'ait pas à être déchiffré ou réinterprété. (Une traduction dans une ou plusieurs langues devrait être fournie lorsque le responsable du traitement cible[15] des personnes concernées parlant ces langues.)

Communication d'informations à des enfants et d'autres personnes vulnérables

14. Quand un responsable du traitement cible des enfants[16] ou est, ou devrait être, conscient que ses biens et/ou services sont particulièrement utilisés par des enfants (y compris lorsque le responsable du traitement est tributaire du consentement de l'enfant)[17], il doit s'assurer que le vocabulaire, le ton et le style de langage utilisés sont adaptés aux enfants et peuvent être compris par ces derniers de sorte que les enfants destinataires des informations reconnaissent que le message/les informations leur sont adressés[18]. Un exemple utile de langage axé sur l'enfant, utilisé en remplacement du langage juridique d'origine, est accessible dans la «Convention des droits de l'enfant des Nations unies expliquée aux enfants»[19].

15. La position du G29 est que la transparence est un droit indépendant qui s'applique autant aux enfants qu'aux adultes. Le G29 insiste en particulier sur le fait que les enfants ne perdent pas leur droit à la transparence en tant que personnes concernées simplement parce que leur consentement a été donné ou autorisé par le titulaire de la responsabilité parentale dans une situation où l'article 8 du RGPD s'applique. Bien qu'un tel consentement soit, dans de nombreux cas, donné ou autorisé sur une base ponctuelle par le titulaire de la responsabilité parentale, un enfant (comme toute autre personne concernée) dispose d'un droit permanent à la transparence pendant toute la durée de son interaction avec le responsable du traitement. Ceci est conforme à

[15] Par exemple, si le responsable du traitement exploite un site internet dans la langue en question et/ou offre des options spécifiques à un pays et/ou facilite le paiement de biens ou services dans la monnaie d'un État membre en particulier, cela peut être le signe que ce responsable du traitement cible les personnes concernées d'un État membre spécifique.

[16] Le terme «enfant» n'est pas défini dans le RGPD; néanmoins le G29 reconnaît, en accord avec la convention internationale relative aux droits de l'enfant des Nations unies – que tous les États membres de l'Union européenne ont ratifiée –, qu'un enfant est une personne âgée de moins de 18 ans.

[17] C'est-à-dire les enfants âgés de 16 ans et plus [ou, lorsque (conformément à l'article 8, paragraphe 1, du RGPD) le droit national de l'État membre a fixé l'âge du consentement à un âge spécifique situé entre 13 et 16 ans, permettant aux enfants de consentir à une offre de prestation de services d'une société de l'information, les enfants ayant atteint ledit âge de consentement national].

[18] Le considérant 38 indique que «[l]es enfants méritent une protection spécifique en ce qui concerne leurs données à caractère personnel parce qu'ils peuvent être moins conscients des risques, des conséquences et des garanties concernées et de leurs droits liés au traitement des données à caractère personnel». Le considérant 58 prévoit que «[l]es enfants méritant une protection spécifique, toute information et communication, lorsque le traitement les concerne, devraient être rédigées en des termes clairs et simples que l'enfant peut aisément comprendre».

[19] https://www.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf

l'article 13 de la convention internationale relative aux droits de l'enfant des Nations unies qui prévoit qu'un enfant a droit à la liberté d'expression, ce qui comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce[20]. Il est important de signaler que, bien qu'il prévoie la fourniture du consentement au nom d'un enfant en dessous d'un âge spécifique[21], l'article 8 *ne prévoit pas* de mesures de transparence destinées au titulaire de la responsabilité parentale qui donne un tel consentement. Par conséquent, les responsables du traitement ont pour obligation, en vertu des dispositions spécifiques aux mesures de transparence destinées aux enfants prévues à l'article 12, paragraphe 1 (et appuyées par les considérants 38 et 58), de garantir que, lorsqu'ils ciblent des enfants ou ont conscience que leurs biens ou services sont particulièrement utilisés par des enfants en âge de savoir lire et écrire, ces informations et communications soient transmises en des termes clairs et simples ou fournies par un moyen facilement compréhensible par des enfants. Pour éviter toute ambiguïté, le G29 reconnaît néanmoins que dans le cas d'enfants très jeunes ou seulement pré-alphabétisés, les mesures de transparence peuvent également être adressées aux titulaires de la responsabilité parentale, étant donné que ces enfants, dans la plupart des cas, ne parviendront pas à comprendre les messages écrits ou non écrits les plus élémentaires au sujet de la transparence.

16. De même, si un responsable du traitement est informé que ses biens et/ou services sont utilisés par (ou ciblent) d'autres membres vulnérables de la société, notamment des personnes souffrant de handicaps ou des personnes éprouvant des difficultés à accéder à l'information, il devrait prendre en compte les vulnérabilités de ces personnes dans son analyse de la façon de garantir le respect de ses obligations de transparence à l'égard de ces personnes concernées[22]. Cette exigence est liée à la nécessité pour le responsable du traitement d'évaluer le niveau probable de compréhension de son public, comme expliqué au point 9 du présent document.

«Par écrit ou par d'autres moyens»

17. Conformément à l'article 12, paragraphe 1, les informations et les communications doivent, en principe, être adressées aux personnes concernées par écrit[23]. (L'article 12, paragraphe 7, prévoit également que les informations peuvent être accompagnées d'icônes normalisées. Cette question est abordée dans la rubrique sur les éléments visuels aux points 49 à 53 du présent document). Cependant, le RGPD autorise également l'utilisation d'autres «voies» non déterminées notamment des voies électroniques. La position du G29 à l'égard des moyens électroniques écrits est que, lorsqu'un responsable du traitement alimente (ou exploite en partie ou en totalité) un site

[20] L'article 13 de la convention internationale relative aux droits de l'enfant des Nations unies dispose comme suit: «L'enfant a droit à la liberté d'expression. Ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen du choix de l'enfant.»
[21] Voir la note de bas de page 17 ci-dessus.
[22] Par exemple, la convention relative aux droits des personnes handicapées des Nations unies exige que des formes appropriées d'aide et d'accompagnement soient fournies aux personnes handicapées afin de leur assurer l'accès à l'information.
[23] L'article 12, paragraphe 1, porte sur les termes utilisés et dispose que les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique.

internet, il lui est recommandé d'avoir recours à une déclaration ou à un avis sur la protection de la vie privée à différents niveaux permettant aux visiteurs du site de naviguer parmi les aspects spécifiques de la déclaration ou de l'avis sur la protection de la vie privée qui les intéressent le plus (voir les points 35 à 37 pour en savoir plus sur les déclarations et avis sur la protection de la vie privée à différents niveaux)[24]. Néanmoins, l'intégralité des informations adressées à une personne concernée devrait également être accessible à un endroit unique ou dans un même document (au format papier ou électronique) pouvant être aisément consulté par cette personne si elle souhaite consulter l'intégralité des informations qui lui sont adressées. Il est également important de noter que le recours à une approche à plusieurs niveaux ne se limite pas à la communication des informations aux personnes concernées par des moyens électroniques écrits. Comme expliqué aux points 35 à 36 et 38 ci-après, une approche à plusieurs niveaux pour la communication d'informations aux personnes concernées peut également être utilisée en employant un ensemble de *méthodes* visant à garantir la transparence à l'égard du traitement.

18. Bien entendu, les déclarations et avis sur la protection de la vie privée à différents niveaux ne sont pas les seuls moyens électroniques écrits dont disposent les responsables du traitement. Ces derniers peuvent également utiliser des avis apparaissant dans des fenêtres contextuelles à des moments spécifiques, des avis apparaissant par pression sur l'écran ou par déplacement au-dessus de l'écran, et des tableaux de bord sur la protection de la vie privée. Les moyens électroniques non écrits pouvant être utilisés *en sus* d'une déclaration ou d'un avis sur la protection de la vie privée à différents niveaux peuvent inclure des vidéos ainsi que des alertes vocales pour smartphone ou objet connecté[25]. Les «autres moyens», qui ne sont pas nécessairement électroniques, peuvent inclure, par exemple, des bandes dessinées, des infographies ou des organigrammes. Lorsque les informations sur la transparence sont destinées spécifiquement à des enfants, les responsables du traitement devraient prendre en compte le type de mesures pouvant être particulièrement accessibles aux enfants (par exemple, des dessins animés, des bandes dessinées, des pictogrammes, des animations, etc.).

19. La méthode choisie pour communiquer les informations, c'est-à-dire la façon dont le responsable du traitement et la personne concernée interagissent ou la façon dont les informations de la personne concernée sont collectées, doit impérativement être adaptée aux circonstances particulières de la situation. Ainsi, fournir simplement les informations par voie électronique et par écrit, par exemple dans une déclaration ou un avis sur la protection de la vie privée en ligne, peut ne pas être adapté ou ne pas fonctionner sur un dispositif collectant les données à caractère personnel qui ne dispose pas d'un écran (dispositifs connectés/intelligents) pour afficher le site internet ou ces informations écrites. Dans un tel cas, des moyens alternatifs *supplémentaires* et adaptés devraient être envisagés, par exemple la fourniture de la déclaration ou de l'avis sur la protection de la vie privée dans un guide d'instruction au format papier ou la fourniture

[24] La reconnaissance par le G29 des avantages des avis à différents niveaux a déjà été notée dans l'avis 10/2004 relatif aux dispositions davantage harmonisées en matière d'information et l'avis 2/2013 sur les applications destinées aux dispositifs intelligents.
[25] Ces exemples de moyens électroniques ne sont fournis qu'à titre indicatif et les responsables du traitement peuvent élaborer de nouvelles méthodes innovantes en vue de satisfaire à l'article 12.

au format papier, dans les instructions ou sur l'emballage, de l'adresse URL du site internet (plus précisément, la page spécifique du site internet) où se trouve l'avis ou la déclaration sur la protection de la vie privée. La communication audio (orale) des informations est également possible si le dispositif sans écran dispose de fonctions audio. Le G29 a précédemment formulé des recommandations touchant à la transparence et à la communication d'informations aux personnes concernées dans son avis sur les récentes évolutions relatives à l'internet des objets[26] (comme l'utilisation de codes QR imprimés sur des objets connectés qui, lorsqu'ils sont scannés, affichent les informations requises sur la transparence). Ces recommandations demeurent applicables au titre du RGPD.

«…les informations peuvent être fournies oralement»

20. L'article 12, paragraphe 1, envisage en particulier que les informations puissent être fournies oralement à une personne concernée, si elle en fait la demande, à condition que son identité soit démontrée par d'autres moyens. En d'autres termes, les moyens employés ne peuvent pas se fonder uniquement sur la simple affirmation par l'intéressé qu'il est bien la personne concernée et les moyens devraient permettre au responsable du traitement de vérifier l'identité de la personne concernée avec suffisamment de certitude. L'exigence de vérification de l'identité de la personne concernée avant la communication orale des informations ne s'applique qu'aux informations liées à l'exercice par une personne concernée de ses droits en vertu des articles 15 à 22 et 34. Cette condition préalable à la communication d'informations orales ne peut s'appliquer à la communication d'informations confidentielles générales telles qu'énoncées aux articles 13 et 14, puisque les informations requises au titre de ces articles doivent également être rendues accessibles aux *futurs* utilisateurs et clients (dont l'identité ne pourrait pas être vérifiée par un responsable du traitement). Aussi les informations à fournir en vertu des articles 13 et 14 peuvent-elles être fournies oralement sans que le responsable du traitement n'ait besoin que la personne concernée justifie son identité.

21. La fourniture orale des informations requises au titre des articles 13 et 14 ne doit pas nécessairement se faire d'une personne à une autre (c'est-à-dire en personne ou par téléphone). Des informations orales enregistrées peuvent être fournies en plus d'informations écrites. Par exemple, cela peut s'appliquer dans le contexte de personnes malvoyantes lorsqu'elles interagissent avec des prestataires de services de la société de l'information, ou dans le contexte de dispositifs intelligents sans écran, comme indiqué précédemment au point 19. Quand un responsable du traitement choisit de fournir des informations oralement à une personne concernée, ou quand une personne concernée demande la fourniture orale d'informations ou de communications, le G29 estime que le responsable du traitement doit permettre à la personne concernée de réécouter les messages préenregistrés. Cela est impératif lorsque la demande d'informations orales émane de personnes concernées malvoyantes ou d'autres personnes concernées ayant des difficultés à accéder à des informations écrites ou à les comprendre. Le responsable du traitement devrait également veiller à conserver une trace écrite, et s'assurer qu'il est en mesure de le prouver (aux fins de la conformité à l'exigence de responsabilité), de: i) la demande d'informations par voie orale, ii) la méthode par laquelle l'identité de la

[26] Avis 8/2014 du G29 adopté le 16 septembre 2014.

personne concernée a été vérifiée (le cas échéant, voir le point 20 ci-dessus), et iii) du fait que les informations ont été transmises à la personne concernée.

«Gratuitement»

22. Conformément à l'article 12, paragraphe 5[27], les responsables du traitement ne peuvent généralement pas exiger de paiement de la part des personnes concernées pour la fourniture d'informations au titre des articles 13 et 14, ou pour les communications et la prise de mesures au titre des articles 15 à 22 (sur les droits de la personne concernée) et de l'article 34 (communication à la personne concernée d'une violation de données à caractère personnel)[28]. Cet aspect de la transparence signifie également que les informations fournies en vertu des exigences de transparence ne peuvent pas être subordonnées à des opérations financières, par exemple le paiement ou l'achat de biens ou services[29].

Informations à fournir à la personne concernée - Articles 13 et 14

Contenu

23. Le RGPD répertorie les catégories d'informations à fournir à une personne concernée en ce qui concerne le traitement de ses données à caractère personnel lorsque celles-ci sont collectées auprès de la personne concernée (article 13) ou obtenues d'une autre source (article 14). Le **tableau en annexe** des présentes lignes directrices résume les catégories d'informations à fournir au titre des articles 13 et 14. Il prend également en compte la nature, la portée et le contenu de ces exigences. Par souci de clarté, la position du G29 est qu'il n'y a pas de différence entre le statut des informations à fournir au titre du paragraphe 1 et du paragraphe 2 des articles 13 et 14, respectivement. Toutes les informations contenues dans ces paragraphes sont d'égale importance et doivent être fournies à la personne concernée.

«Mesures appropriées»

24. À l'instar du contenu, la forme et la manière dont les informations requises au titre des articles 13 et 14 devraient être fournies à la personne concernée sont importantes. L'avis contenant ces informations est fréquemment désigné comme un avis sur la

[27] Cet article prévoit qu'«[a]ucun paiement n'est exigé pour fournir les informations au titre des articles 13 et 14 et pour procéder à toute communication et prendre toute mesure au titre des articles 15 à 22 et de l'article 34».
[28] Toutefois, au titre de l'article 12, paragraphe 5, le responsable du traitement peut exiger le paiement de frais raisonnables lorsque, par exemple, la demande d'une personne concernée en lien avec les informations au titre des articles 13 ou 14 ou les droits prévus aux articles 15 à 22 ou à l'article 34 est excessive ou manifestement infondée. (D'un autre côté, en ce qui concerne le droit d'accès au titre de l'article 15, paragraphe 3, un responsable du traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire des données à caractère personnel demandée par la personne concernée.)
[29] À titre d'exemple, si les données à caractère personnel d'une personne concernée sont collectées dans le cadre d'un achat, les informations requises au titre de l'article 13 devraient être fournies avant le paiement et au moment de la collecte des informations, plutôt qu'après la conclusion de l'opération. Néanmoins, lorsque des services gratuits sont fournis à une personne concernée, les informations au titre de l'article 13 doivent être transmises avant, plutôt qu'après, l'inscription, puisque l'article 13, paragraphe 1, exige la fourniture des informations «au moment où les données à caractère personnel sont obtenues».

protection de la vie privée, un avis de confidentialité, une politique de confidentialité, une déclaration de confidentialité ou un avis de traitement loyal. Le RGPD ne prescrit pas la forme ou les modalités selon lesquelles les informations devraient être fournies à la personne concernée; cependant, il établit clairement que le responsable du traitement est tenu de prendre des «mesures appropriées» pour fournir les informations requises à des fins de transparence. Cela signifie que le responsable du traitement devrait prendre en compte toutes les circonstances de la collecte et du traitement des données lorsqu'il décide des modalités et de la forme appropriées pour la fourniture des informations. Plus particulièrement, les mesures appropriées devront être analysées à la lumière de l'expérience de l'utilisateur du service ou du produit. À cet égard, il conviendra de prendre en compte le type de dispositif utilisé (le cas échéant), la nature des interfaces utilisateur et des interactions avec le responsable du traitement (le «parcours» de l'utilisateur) et les limitations que ces facteurs entraînent. Comme indiqué ci-dessus au point 17, le G29 recommande que, lorsqu'un responsable du traitement est présent sur internet, il y a lieu de fournir en ligne une déclaration de confidentialité ou des dispositions en matière de protection de la vie privée sur différents niveaux.

25. Pour déterminer les modalités les mieux adaptées à la communication d'informations, les responsables du traitement devraient, avant de se décider, essayer différentes modalités au moyen de tests utilisateurs (par exemple, des tests en salle ou d'autres tests normalisés sur la lisibilité ou l'accessibilité) afin de connaître la réaction des utilisateurs sur l'accessibilité, la compréhensibilité et la facilité d'utilisation des mesures proposées. (Voir également les commentaires complémentaires du point 9 sur les autres mécanismes d'exécution de tests pour les utilisateurs). La documentation de cette approche devrait également aider les responsables du traitement à satisfaire à leurs obligations de responsabilité, en démontrant que les outils et l'approche choisis pour communiquer les informations sont les mieux adaptés aux circonstances.

Délai de soumission des informations

26. Les articles 13 et 14 indiquent les informations à fournir aux personnes concernées dès la phase de commencement du cycle de traitement[30]. L'article 13 s'applique au cas de figure dans lequel les données sont collectées auprès de la personne concernée. Cela comprend les données à caractère personnel:

- qu'une personne concernée fournit sciemment à un responsable du traitement (par exemple lorsqu'elle remplit un formulaire en ligne); ou
- qu'un responsable du traitement collecte auprès d'une personne concernée par observation (par exemple en utilisant des appareils de saisie automatique de données ou des logiciels de saisie de données tels que des caméras, un équipement de réseau, un système de repérage Wi-Fi, la radio-identification ou d'autres types de capteurs).

[30] Conformément aux principes d'équité et de limitation de la finalité, l'entité qui collecte les données à caractère personnel auprès de la personne concernée devrait toujours préciser les finalités du traitement au moment de la collecte. Si la finalité comprend la création de données à caractère personnel déduites, la finalité prévue de créer puis de traiter ces données à caractère personnel induites, ainsi que les catégories des données induites traitées, doit toujours être communiquée à la personne concernée au moment de la collecte ou avant le traitement ultérieur à d'autres fins, conformément à l'article 13, paragraphe 3, ou à l'article 14, paragraphe 4.

L'article 14 s'applique au cas de figure dans lequel les données n'ont pas été collectées auprès de la personne concernée. Il s'agit des données à caractère personnel qu'un responsable du traitement a obtenues de sources telles que:

- des responsables du traitement tiers;
- des sources en libre accès;
- des courtiers en données; ou
- d'autres personnes concernées.

27. S'agissant des délais de fourniture de ces informations, leur communication rapide est un élément essentiel de l'obligation de transparence et de l'obligation de traiter les données avec équité. Lorsque l'article 13 s'applique, les informations doivent, en vertu de son paragraphe 1, être fournies «*au moment où les données en question sont obtenues*». Lorsque les données à caractère personnel ont été obtenues de façon indirecte au titre de l'article 14, les délais dans lesquels les informations requises doivent être fournies à la personne concernée sont définis à l'article 14, paragraphe 3, points a) à c), comme suit:

- l'exigence générale est que les informations doivent être communiquées «dans un délai raisonnable» après avoir obtenu les données à caractère personnel, mais ne dépassant pas un mois, «*eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées*» [article 14, paragraphe 3, point a)];

- le délai général d'un mois fixé à l'article 14, paragraphe 3, point a), peut être encore réduit en vertu de l'article 14, paragraphe 3, point b)[31], qui prévoit le cas où les données sont utilisées aux fins de la communication avec la personne concernée. Dans un tel cas, les informations doivent être fournies au plus tard lors de la première communication avec ladite personne. Si la première communication a lieu avant le délai d'un mois après l'obtention des données à caractère personnel, les informations doivent être fournies *au plus tard* lors de la première communication avec la personne concernée, nonobstant le fait que le délai d'un mois à compter de l'obtention des données n'a pas expiré. Si la première communication avec une personne concernée a lieu plus d'un mois après l'obtention des données à caractère personnel, l'article 14, paragraphe 3, point a), continue de s'appliquer, de sorte que les informations énoncées à cet article doivent être fournies à la personne concernée au plus tard un mois après l'obtention des données;

[31] La formule à l'article 14, paragraphe 3, point b) «*si les données à caractère personnel doivent être utilisées aux fins de…*» , indique l'ajout d'une précision à la situation générale concernant le délai maximal établi à l'article 14, paragraphe 3, point a), mais elle ne la remplace pas.

- le délai général d'un mois énoncé à l'article 14, paragraphe 3, point a), peut également être réduit en vertu de l'article 14, paragraphe 3, point c)[32], qui prévoit le cas où les données sont communiquées à un autre destinataire (qu'il s'agisse ou non d'un tiers)[33]. Dans un tel cas, les informations doivent être fournies au plus tard au moment de la première communication. Dans cette hypothèse, si la communication a lieu avant l'expiration du délai d'un mois, les informations doivent être fournies *au plus tard* au moment de la première communication, nonobstant le fait que le délai d'un mois à compter de l'obtention des données n'a pas expiré. De façon similaire à la situation visée à l'article 14, paragraphe 3, point b), si la communication de données à caractère personnel se produit plus d'un mois après l'obtention des données en question, l'article 14, paragraphe 3, point a), continue de s'appliquer, de sorte que les informations énoncées à cet article doivent être fournies à la personne concernée au plus tard un mois après l'obtention des données.

28. Par conséquent, dans tous les cas, le délai maximal pendant lequel les informations prévues à l'article 14 doivent être fournies à une personne concernée est d'un mois. Toutefois, les principes d'équité et de responsabilité prévus par le RGPD exigent des responsables du traitement qu'ils prennent toujours en compte les attentes raisonnables des personnes concernées ainsi que les effets que ce traitement peut avoir sur elles et sur leur capacité à exercer leurs droits en lien avec ledit traitement, lorsqu'ils choisissent le moment auquel fournir les informations prévues par l'article 14. Le principe de responsabilité exige des responsables du traitement qu'ils expliquent les motifs de leur décision et justifient le choix du moment où ils ont fourni les informations. En pratique, il peut être difficile de satisfaire à ces exigences lorsque des informations sont fournies au «dernier moment». À cet égard, le considérant 39 indique, entre autres, que les personnes concernées devraient «*être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement*». Le considérant 60 fait également référence au fait que la personne concernée doit être informée de l'existence de l'opération de traitement et de ses finalités dans le cadre du principe de traitement loyal et transparent. Pour toutes ces raisons, la position du G29 est que, dans la mesure du possible, les responsables du traitement devraient, conformément au principe d'équité, fournir les informations aux personnes concernées bien avant les délais indiqués. D'autres commentaires sur l'adéquation du délai entre la notification des opérations de traitement aux personnes concernées et le moment où lesdites opérations de traitement prennent effet sont formulés aux points 30 à 31 et 48.

Modifications des informations à fournir au titre des articles 13 et 14

[32] La formule à l'article 14, paragraphe 3, point c) «*s'il est envisagé de communiquer les informations à un autre destinataire…*» , indique de la même manière l'ajout d'une précision à la situation générale concernant le délai maximal établi à l'article 14, paragraphe 3, point a), mais elle ne la remplace pas.

[33] L'article 4, paragraphe 9, donne la définition de «destinataire» et précise qu'un destinataire auquel des données à caractère personnel sont communiquées ne doit pas nécessairement être un tiers. Par conséquent, un destinataire peut être un responsable du traitement, un responsable conjoint du traitement ou un sous-traitant.

29. La responsabilité en matière de transparence s'applique non seulement au moment de la collecte des données à caractère personnel, mais aussi tout au long du cycle de vie de leur traitement, quelles que soient les informations ou les communications fournies. C'est par exemple le cas lors de la modification du contenu des avis et déclarations existants sur la protection de la vie privée. Le responsable du traitement devrait respecter les mêmes principes lorsqu'il communique l'avis ou la déclaration initial(e) sur la protection de la vie privée et toute modification substantielle apportée ultérieurement à cet avis ou à cette déclaration. Les facteurs que les responsables du traitement devraient prendre en compte lors de l'évaluation de ce que constitue une modification substantielle comprennent l'incidence sur la personne concernée (notamment sa capacité à exercer ses droits) et le caractère inattendu ou surprenant de la modification pour cette personne. Les modifications d'un avis ou d'une déclaration sur la protection de la vie privée doivent toujours être communiquées à la personne concernée, notamment: une modification de la finalité du traitement; une modification de l'identité du responsable du traitement; ou une modification de la façon dont les personnes concernées peuvent exercer leurs droits concernant le traitement. Inversement, à titre d'exemple, les corrections de fautes d'orthographe ou de problèmes de syntaxe ou de grammaire ne sont pas considérées par le G29 comme une modification substantielle. Dès lors que la plupart des clients ou utilisateurs actuels ne font que jeter un coup d'œil aux communications portant sur la modification d'un avis ou d'une déclaration sur la protection de la vie privée, le responsable du traitement devrait prendre toutes les mesures nécessaires pour garantir que ces modifications soient communiquées de manière à être lues par la plupart des destinataires. Cela signifie, par exemple, qu'une notification de modification devrait toujours être communiquée par un moyen adapté (par exemple, e-mail, courrier postal, fenêtre contextuelle sur une page web ou autre moyen captant efficacement l'attention de la personne concernée) spécifiquement consacré à la modification (par exemple, séparée d'un contenu de marketing direct), et cette communication doit respecter les prescriptions de l'article 12, c'est-à-dire être adressée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Les mentions contenues dans l'avis ou la déclaration sur la protection de la vie privée indiquant que la personne concernée devrait régulièrement vérifier l'avis ou la déclaration sur la vie privée afin d'en connaître les éventuelles modifications ou mises à jour sont jugées non seulement insuffisantes, mais également déloyales au sens de l'article 5, paragraphe 1, point a). D'autres orientations relatives aux délais de notification des modifications aux personnes concernées sont présentées ci-après, aux points 30 et 31.

Délai de notification des modifications des informations à fournir au titre des articles 13 et 14

30. Le RGPD ne traite pas des délais (et donc des méthodes y afférentes) qui s'appliquent aux notifications des modifications des informations préalablement fournies à une personne concernée au titre de l'article 13 ou de l'article 14 (sauf en cas d'intention d'effectuer un traitement ultérieur pour une finalité autre, auquel cas les informations sur cette finalité ultérieure doivent être notifiées avant le commencement dudit traitement, conformément à l'article 13, paragraphe 3, et à l'article 14, paragraphe 4. À ce sujet, voir le point 45 ci-après). Cependant, comme indiqué plus haut, dans le cadre des délais applicables à la communication des informations au titre de l'article 14, le

responsable du traitement doit à nouveau prêter attention aux principes d'équité et de responsabilité à l'égard des attentes raisonnables de la personne concernée ou de l'incidence potentielle de ces modifications sur la personne concernée. Si la modification des informations change fondamentalement la nature du traitement (par exemple, l'élargissement des catégories de destinataires ou l'introduction de transferts vers un pays tiers) ou s'il s'agit d'une modification qui peut ne pas être fondamentale pour l'opération de traitement, mais qui peut l'être pour la personne concernée et avoir une incidence sur cette dernière, les informations devraient être fournies à la personne concernée bien avant que la modification ait lieu et la méthode utilisée pour informer la personne concernée des modifications devrait être explicite et efficace. L'objectif étant de garantir à la personne concernée qu'elle ne «rate» pas la modification et de lui accorder une période de temps raisonnable pour qu'elle puisse a) évaluer la nature et l'incidence de la modification, et b) exercer ses droits au titre du RGPD en lien avec la modification (par exemple, retirer son consentement ou s'opposer au traitement).

31. Les responsables du traitement devraient évaluer attentivement les circonstances et le contexte de chaque situation où une mise à jour des informations sur la transparence est requise, notamment l'incidence potentielle des modifications pour la personne concernée et les modalités utilisées pour communiquer la modification, et être capables de démontrer que l'intervalle de temps entre la notification des modifications et la date de prise d'effet des modifications respecte le principe d'équité pour la personne concernée. Par ailleurs, la position du G29 est que, conformément au principe d'équité, le responsable du traitement devrait également, lors de la notification de modifications aux personnes concernées, leur expliquer l'incidence que ces modifications pourraient avoir sur elles. Toutefois, le respect des exigences de transparence ne «blanchit» pas les situations où les modifications apportées au traitement sont telles que le traitement devient complètement différent par nature de ce en quoi il consistait auparavant. Le G29 met l'accent sur le fait que toutes les autres règles du RGPD, y compris celles concernant un traitement ultérieur incompatible, continuent de s'appliquer, que les obligations de transparence aient été satisfaites ou non.

32. De plus, même lorsque les informations relatives à la transparence (par exemple, celles contenues dans un avis ou une déclaration sur la protection de la vie privée) ne sont pas modifiées de façon substantielle, il est probable que les personnes concernées qui font appel à un service depuis un certain temps ne se souviendront pas des informations qui leur ont été fournies au départ au titre des articles 13 et/ou 14. Le G29 recommande que les responsables du traitement permettent aux personnes concernées de disposer en continu d'un accès facilité aux informations afin qu'elles puissent se refamiliariser avec la portée du traitement des données. Conformément au principe de responsabilité, les responsables du contrôle devraient également évaluer s'il y a lieu d'adresser, et à quels intervalles, des rappels exprès aux personnes concernées sur l'existence d'un avis ou d'une déclaration sur la protection de la vie privée et sur l'endroit où elles peuvent le/la trouver.

Modalités: format de la communication des informations

33. Les articles 13 et 14 font référence à l'obligation imposée au responsable du traitement de «*[fournir] toutes les informations suivantes…*». Le mot «fournir» est crucial en

l'occurrence. Il signifie que le responsable du traitement doit prendre des mesures concrètes pour fournir les informations en question à la personne concernée ou pour diriger activement la personne concernée vers l'emplacement desdites informations (par exemple au moyen d'un lien direct, d'un code QR, etc.). La personne concernée ne doit pas avoir à chercher activement les informations couvertes par ces articles parmi d'autres informations telles que les conditions d'utilisation d'un site internet ou d'une application. L'exemple donné au paragraphe 11 est explicite à cet égard. Comme indiqué au point 17, le G29 recommande que l'intégralité des informations adressées aux personnes concernées soit également consultable à un endroit unique ou dans un même document (sous forme numérique sur un site internet ou au format papier) qui serait aisément accessible dans le cas où elles souhaiteraient consulter l'intégralité des informations.

34. Il existe dans le RGPD un conflit inhérent entre, d'une part, l'exigence de communiquer aux personnes concernées les informations complètes qui sont requises au titre du RGPD et, d'autre part, l'exigence de le faire d'une manière concise, transparente, compréhensible et aisément accessible. À cet effet, et en gardant à l'esprit les principes fondamentaux de responsabilité et d'équité, les responsables du traitement doivent entreprendre leur propre analyse de la nature, des circonstances, de la portée et du contexte du traitement des données à caractère personnel qu'ils exécutent, et décider, en vertu des exigences légales du RGPD et compte tenu des recommandations des présentes lignes directrices et notamment du point 36 ci-après, comment hiérarchiser les informations à fournir aux personnes concernées et quels sont les niveaux de détail et les méthodes adaptés à la communication des informations.

Approche à plusieurs niveaux dans un environnement numérique et avis/déclarations sur la protection de la vie privée à différents niveaux

35. Dans le contexte numérique, à la lumière du volume d'informations à fournir à la personne concernée, le responsable du traitement peut adopter une approche à plusieurs niveaux, par laquelle il choisit d'utiliser plusieurs méthodes pour garantir la transparence. Le G29 recommande en particulier que les avis/déclarations sur la protection de la vie privée à différents niveaux soient utilisés pour relier les différentes catégories d'informations à fournir à la personne concernée, au lieu d'afficher toutes ces informations sur une seule et même page, afin d'éviter de noyer d'informations la personne concernée. Les avis/déclarations sur la protection de la vie privée à différents niveaux peuvent contribuer à résoudre le conflit entre l'exhaustivité et la compréhension des informations, notamment en permettant aux utilisateurs de naviguer directement vers la partie de la déclaration/de l'avis qu'ils souhaitent lire. Il convient de noter que les avis/déclarations sur la protection de la vie privée à différents niveaux ne sont pas simplement des pages imbriquées nécessitant que l'utilisateur effectue plusieurs clics avant d'accéder aux informations pertinentes. La mise en page et l'organisation du premier niveau de l'avis ou de la déclaration sur la protection de la vie privée devraient être telles que la personne concernée bénéficie d'un aperçu clair des informations qui lui sont accessibles sur le traitement de ses données à caractère personnel et du lieu ainsi que de la façon de trouver ces informations détaillées parmi les niveaux de l'avis ou de la déclaration sur la protection de la vie privée. Il est également important que les

informations contenues aux différents niveaux d'un tel avis soient cohérentes et que les niveaux ne fournissent pas d'informations contradictoires.

36. En ce qui concerne le contenu de la première modalité utilisée par un responsable du traitement pour informer la personne concernée dans le cadre d'une approche à plusieurs niveaux (en d'autres termes, la principale façon de communiquer pour la première fois avec une personne concernée) ou le contenu du premier niveau d'une déclaration/d'un avis sur la protection de la vie privée, le G29 recommande que le premier niveau/la première modalité inclue les détails de la finalité du traitement, l'identité du responsable du traitement et une description des droits des personnes concernées. (En outre, ces informations devraient être directement portées à l'attention de la personne concernée au moment de la collecte des données à caractère personnel, par exemple en les affichant pendant que ladite personne remplit un formulaire en ligne.) L'importance de fournir ces informations en amont découle en particulier du considérant 39[34]. Alors que les responsables du traitement doivent être en mesure de démontrer qu'ils ont fait preuve de responsabilité à l'égard des informations qu'ils décident de fournir en priorité, la position du G29 est que, conformément au principe d'équité, en plus des informations détaillées ci-dessus dans ce paragraphe, le premier niveau ou la première modalité devrait également contenir des informations sur le traitement qui aura la plus forte incidence sur la personne concernée et sur tout traitement qui pourrait la surprendre. Aussi la personne concernée devrait-elle être en mesure de comprendre à partir des informations fournies au premier niveau/à la première modalité quelles seront pour elle les conséquences du traitement en question (voir également le point 10 ci-dessus).

37. Dans un contexte numérique, en plus de fournir en ligne un avis/une déclaration sur la protection de la vie privée à différents niveaux, les responsables du traitement peuvent choisir d'utiliser des outils de transparence *supplémentaires* (voir les autres exemples proposés ci-après) offrant des informations sur mesure, spécifiques à la personne concernée et spécifiques aux biens et services que celle-ci utilise. Il convient toutefois de noter que, même si le G29 recommande le recours à des avis/déclarations sur la protection de la vie privée à différents niveaux en ligne, cette recommandation n'exclut pas l'élaboration et l'utilisation d'autres méthodes innovantes pour satisfaire aux exigences de transparence.

Approche à plusieurs niveaux dans un environnement non numérique

38. Une approche à plusieurs niveaux pour communiquer des informations sur la transparence aux personnes concernées peut également être utilisée dans un contexte hors ligne ou non numérique (c'est-à-dire dans un environnement réel tel qu'un engagement entre deux personnes ou des communications par téléphone) où plusieurs modalités peuvent être déployées par les responsables du traitement afin de faciliter la fourniture d'informations. (Voir également les points 33 à 37 et 39 à 40 en ce qui

[34] Le considérant 39 indique, en ce qui concerne le principe de transparence, que «[c]e principe vaut, notamment, pour les informations communiquées aux personnes concernées sur l'identité du responsable du traitement et sur les finalités du traitement ainsi que pour les autres informations visant à assurer un traitement loyal et transparent à l'égard des personnes physiques concernées et leur droit d'obtenir la confirmation et la communication des données à caractère personnel les concernant qui font l'objet d'un traitement».

concerne les différentes modalités applicables à la communication des informations.) Cette approche ne doit pas être confondue avec l'émission distincte d'un avis ou d'une déclaration sur la protection des données à différents niveaux. Quels que soient les formats utilisés dans cette approche à plusieurs niveaux, le G29 recommande que le premier «niveau» (autrement dit, la principale façon de communiquer pour la première fois avec une personne concernée) communique de manière générale les informations les plus importantes (comme énoncé au point 36 ci-dessus), à savoir les détails de la finalité du traitement, l'identité du responsable du traitement et l'existence des droits des personnes concernées, ainsi que les informations ayant la plus forte incidence sur le traitement ou tout traitement susceptible de surprendre les personnes concernées. Par exemple, quand le premier contact avec une personne concernée se fait par téléphone, ces informations pourraient être fournies lors de l'appel téléphonique tandis que les autres informations requises au titre des articles 13 et 14 pourraient être fournies ultérieurement et par d'autres moyens, notamment en envoyant un exemplaire de la politique de confidentialité par e-mail et/ou en envoyant à la personne concernée un lien vers l'avis/la déclaration en ligne du responsable du traitement sur la protection de la vie privée à différents niveaux .

Notifications de type «push» et «pull»

39. Pour fournir des informations sur la transparence, il est également possible d'avoir recours à des notifications de type «push» et «pull». Les notifications de type «push» consistent à envoyer des notifications d'informations sur la transparence «juste à temps» tandis que les notifications de type «pull» facilitent l'accès aux informations par différentes méthodes, comme la gestion des autorisations, les tableaux de bord sur la protection de la vie privée et les tutoriels «en savoir plus». Ces notifications assurent à la personne concernée une transparence davantage axée sur l'utilisateur.

- Un tableau de bord sur la protection de la vie privée est un lieu unique depuis lequel les personnes concernées peuvent visualiser les informations relatives à la confidentialité et gérer leurs préférences en permettant ou en empêchant que leurs données soient utilisées de certaines façons par le service en question. Un tel outil est particulièrement utile lorsqu'un même service est utilisé par les personnes concernées sur une pluralité d'appareils différents, car cela leur donne accès à leurs données à caractère personnel et leur permet de les gérer sans égard à la façon dont elles utilisent le service. Permettre aux personnes concernées de régler manuellement leurs paramètres de confidentialité au moyen d'un tableau de bord sur la protection de la vie privée peut également faciliter la personnalisation d'un avis ou d'une déclaration sur la protection de la vie privée, en reflétant uniquement les types de traitement ayant lieu précisément pour cette personne concernée. L'intégration d'un tableau de bord sur la protection de la vie privée dans l'architecture existante d'un service (par exemple en utilisant la même mise en page et le même marquage que le reste du service) est préférable, puisqu'elle rendra l'accès et l'utilisation du tableau intuitifs, ce qui peut contribuer à inciter les utilisateurs à s'intéresser à ces informations, de la même façon qu'ils s'intéresseraient à d'autres aspects du service. Une telle intégration peut être un moyen efficace de montrer que les «informations sur la confidentialité» constituent une partie nécessaire et

intégrale d'un service, à la place d'une liste interminable de dispositions juridiques.

- Une notification à «flux tendus» sert à fournir de façon *ad hoc* des informations spécifiques sur la confidentialité, au moment où leur lecture est la plus pertinente pour la personne concernée. Cette méthode est utile pour fournir des informations à différents moments du processus de collecte de données; elle aide à scinder la fourniture d'informations en blocs facilement assimilables et réduit le recours à un avis ou une déclaration sur la protection de la vie privée unique contenant des informations difficiles à comprendre une fois sorties de leur contexte. Par exemple, si une personne concernée achète un produit en ligne, une brève explication peut être fournie sous forme de fenêtres contextuelles accompagnant les champs de texte pertinents. Des informations placées à côté d'un champ exigeant le numéro de téléphone de la personne concernée pourraient expliquer, par exemple, que ces données ne sont collectées qu'en vue de contacter la personne au sujet de son achat et ne seront communiquées qu'au service de livraison.

Autres types de «mesures appropriées»

40. Étant donné le niveau très élevé d'accès à internet dans l'Union et le fait que les personnes concernées ont la possibilité de se connecter à tout moment, depuis divers endroits et sur différents appareils, comme indiqué plus haut, la position du G29 est qu'une «mesure appropriée» pour fournir des informations sur la transparence, dans le cas des responsables du traitement maintenant une présence numérique/en ligne, est de le faire au moyen d'un avis ou d'une déclaration électronique sur la protection de la vie privée. Néanmoins, selon les circonstances de la collecte et du traitement des données, un responsable du traitement peut avoir besoin d'utiliser en plus (ou à titre subsidiaire si le responsable du traitement ne bénéficie pas d'une présence numérique ou en ligne) d'autres modalités et formats pour fournir les informations. Les autres moyens possibles de communiquer des informations à une personne concernée dans les différents environnements de données à caractère personnel suivants peuvent inclure les modes répertoriés ci-dessous, applicables à chaque environnement correspondant. Comme indiqué précédemment, une approche à plusieurs niveaux peut être suivie par les responsables du traitement s'ils choisissent d'utiliser plusieurs de ces méthodes tout en s'assurant que les informations les plus importantes (voir les points 36 et 38) sont toujours transmises dans la première modalité utilisée pour communiquer avec la personne concernée.

a. Environnement papier, par exemple lors de la conclusion d'un contrat par voie postale: explications écrites, brochures, informations figurant dans un document contractuel, bandes dessinées, infographies ou organigrammes.
b. Environnement téléphonique: explications orales fournies par une personne physique permettant une interaction, questions appelant une réponse, ou informations automatisées ou pré-enregistrées proposant l'option d'entendre d'autres informations plus détaillées.
c. Environnement de technologie intelligente sans écran/connectée tel que les analyses de repérage Wi-Fi: icônes, codes QR, alertes vocales, informations

écrites intégrées dans des instructions d'installation papier, vidéos intégrées dans des instructions d'installation numériques, informations écrites sur un dispositif intelligent, messages envoyés par SMS ou par e-mail, tableaux visibles contenant les informations, signalisation publique ou campagnes d'information publiques.

d. Environnement réunissant deux personnes, comme lors de la réponse à une enquête d'opinion ou l'inscription d'une personne à un service: explications orales ou écrites fournies au format papier ou électronique.

e. Environnement «réel» au moyen d'un système CCTV ou d'un enregistrement par drone: tableaux visibles contenant les informations, signalisation publique, campagnes d'information publiques ou avis dans la presse et les médias.

Informations sur le profilage et la prise de décision automatisée

41. Les informations sur l'existence d'une prise de décision automatisée, y compris un profilage, visées à l'article 22, paragraphes 1 et 4, et les informations utiles concernant la logique sous-jacente, ainsi que l'importance des conséquences prévues de ce traitement pour la personne concernée font partie des informations obligatoires devant être fournies à une personne concernée au titre de l'article 13, paragraphe 2, point f), et de l'article 14, paragraphe 2, point g). Le G29 a élaboré des lignes directrices sur les décisions individuelles automatisées et le profilage[35] auxquelles il y a lieu de se reporter pour obtenir davantage d'orientations quant à la façon dont la transparence devrait être mise en œuvre dans les circonstances particulières du profilage. Il convient de noter que, parallèlement aux exigences de transparence spécifiques applicables à la prise de décision automatisée au titre de l'article 13, paragraphe 2, point f), et de l'article 14, paragraphe 2, point g), les commentaires contenus dans les présentes lignes directrices quant à l'importance d'informer les personnes concernées sur les conséquences du traitement de leurs données à caractère personnel, ainsi que le principe général selon lequel les personnes concernées ne devraient pas être surprises par le traitement de leurs données à caractère personnel, s'appliquent de la même façon au profilage en général (et non pas uniquement au profilage visé à l'article 22[36]), en tant que type de traitement[37].

Autres questions: risques, règles et garanties

42. Le considérant 39 du RGPD porte également sur la fourniture de certaines informations qui ne sont pas explicitement couvertes par l'article 13 et l'article 14 (voir la citation du considérant au point 28 ci-dessus). Le renvoi à ce considérant qui indique que les personnes concernées devraient être informées des risques, règles et garanties liés au traitement des données à caractère personnel se rattache à plusieurs autres questions. Celles-ci comprennent notamment les analyses d'impact relatives à la protection des

[35] Lignes directrices sur les décisions individuelles automatisées et le profilage au titre du règlement 2016/679, WP 251.

[36] Cela s'applique aux prises de décision fondées uniquement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques pour la personne concernée ou, de façon similaire, l'affecte de manière significative.

[37] Le considérant 60, pertinent en l'occurrence, indique qu'«[e]n outre, la personne concernée devrait être informée de l'existence d'un profilage et des conséquences de celui-ci».

données (AIPD). Conformément aux lignes directrices du G29 concernant les AIPD[38], les responsables du traitement peuvent envisager la publication de l'AIPD (ou de toute partie de celle-ci) comme un moyen de favoriser la confiance dans les opérations de traitement et de démontrer le respect des principes de transparence et de responsabilité, bien qu'une telle publication ne soit pas obligatoire. Par ailleurs, l'application d'un code de conduite (comme le prévoit l'article 40) peut servir d'élément pour démontrer le respect des obligations de transparence, puisque les codes de conduite peuvent être rédigés en vue de préciser l'application du RGPD concernant: le traitement loyal et transparent; les informations communiquées au public et aux personnes concernées; et les informations communiquées aux enfants et relatives à leur protection, parmi d'autres enjeux.

43. Un autre élément pertinent concernant la transparence est la protection des données dès la conception et la protection des données par défaut (comme requis à l'article 25). Ces principes exigent des responsables du traitement qu'ils intègrent des considérations sur la protection des données dans leurs systèmes et opérations de traitement dès le début, plutôt que de prendre en compte la protection des données à la dernière minute, en réponse à un problème de conformité. Le considérant 78 fait référence à l'application par les responsables du traitement de mesures satisfaisant aux exigences en matière de protection des données dès la conception et de protection des données par défaut, notamment des mesures portant sur la transparence à l'égard des fonctions et du traitement des données à caractère personnel.

44. D'un autre côté, la question des responsables conjoints du traitement est aussi liée au devoir d'informer les personnes concernées des risques, règles et garanties possibles. L'article 26, paragraphe 1, impose aux responsables conjoints du traitement de déterminer leurs responsabilités respectives aux fins d'assurer le respect des exigences du RGPD de manière transparente, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 13 et 14. L'article 26, paragraphe 2, exige que les grandes lignes de l'accord entre les responsables du traitement soient mises à la disposition de la personne concernée. En d'autres termes, une personne concernée doit avoir parfaitement compris à quel responsable du traitement elle doit s'adresser si elle souhaite exercer un ou plusieurs de ses droits au titre du RGPD[39].

Informations concernant un traitement ultérieur

45. Les articles 13 et 14 contiennent une disposition[40] exigeant du responsable du traitement qu'il informe la personne concernée lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle

[38] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, WP 248, rev.1.

[39] En vertu de l'article 26, paragraphe 3, indépendamment des termes de l'accord entre les responsables conjoints du traitement visé à l'article 26, paragraphe 1, une personne concernée peut exercer les droits que lui confère le RGPD à l'égard de et contre chacun des responsables conjoints du traitement.

[40] Aux articles 13, paragraphe 3, et 14, paragraphe 4, qui sont formulés en termes identiques, à l'exception du mot «collectées», qui est utilisé à l'article 13 et est remplacé par le mot «obtenues» à l'article 14.

pour laquelle les données à caractère personnel ont été collectées/obtenues. Dans un tel cas, «*le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée au paragraphe 2*». Ces dispositions donnent spécifiquement effet au principe énoncé à l'article 5, paragraphe 1, point b), selon lequel les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités[41]. La seconde partie de l'article 5, paragraphe 1, point b), indique que le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales. Lorsque des données à caractère personnel sont traitées ultérieurement à des fins *compatibles* avec les finalités initiales (l'article 6, paragraphe 4, porte sur cette question[42]), les articles 13, paragraphe 3, et 14, paragraphe 4, s'appliquent. Les exigences contenues dans ces articles, qui imposent d'informer une personne concernée en cas de traitement ultérieur de ses données, appuient la position du RGPD quant au fait qu'une personne concernée devrait raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée[43]. Autrement dit, une personne concernée ne devrait pas être surprise par la finalité du traitement de ses données à caractère personnel.

46. Les articles 13, paragraphe 3, et 14, paragraphe 4, dans la mesure où ils visent la fourniture de «*toute autre information pertinente visée au paragraphe 2*», peuvent être interprétés de prime abord comme laissant certains éléments à l'appréciation du responsable du traitement concernant la mesure et les catégories particulières d'informations tirées du paragraphe 2 correspondant (c'est-à-dire l'article 13, paragraphe 2, ou l'article 14, paragraphe 2, le cas échéant) qui devraient être fournies à la personne concernée. (Le considérant 61 y fait référence sous l'expression «*toute autre information nécessaire*».) Néanmoins, la position par défaut est que toutes les informations énoncées dans ce paragraphe devraient être fournies à la personne concernée à moins qu'une ou plusieurs catégories d'informations n'existe(nt) pas ou ne soi(en)t pas applicable(s).

47. Le G29 recommande que les responsables du traitement, pour être transparents, loyaux et responsables, envisagent d'intégrer dans leur avis ou leur déclaration sur la protection de la vie privée les informations concernant l'analyse de compatibilité menée au titre de l'article 6, paragraphe 4[44], lorsqu'une base juridique autre que le consentement, le droit national ou le droit de l'Union est suivie au titre de la nouvelle finalité de traitement, afin

[41] Sur ce principe, voir par exemple les considérants 47, 50, 61, 156 et 158 et les articles 6, paragraphe 4, et 89.

[42] L'article 6, paragraphe 4, énonce d'une manière non exhaustive les facteurs à prendre en compte lors de la vérification de la compatibilité du traitement à d'autres finalités avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, à savoir: le lien entre lesdites finalités; le contexte dans lequel les données à caractère personnel ont été collectées; la nature des données à caractère personnel (en particulier si le traitement porte sur des catégories particulières de données à caractère personnel ou si des données à caractère personnel relatives à des infractions pénales et à des infractions sont incluses); les conséquences possibles du traitement ultérieur envisagé pour les personnes concernées; et l'existence de garanties appropriées.

[43] Considérants 47 et 50.

[44] Également au titre du considérant 50.

que ces informations soient accessibles aux personnes concernées. (En d'autres termes, une explication justifiant que le traitement en vue d'autres finalités est compatible avec la finalité initiale.) L'objectif est de donner aux personnes concernées la possibilité d'évaluer la compatibilité du traitement ultérieur et les garanties fournies et de décider d'exercer ou non leurs droits, par exemple le droit de limiter le traitement ou le droit de le refuser, entre autres[45]. Lorsque les responsables du traitement choisissent de ne pas inclure ces informations dans un avis ou une déclaration sur la protection de la vie privée, le G29 recommande qu'ils signalent clairement aux personnes concernées qu'elles ont la possibilité d'obtenir ces informations sur demande.

48. La question des délais se rattache à l'exercice des droits des personnes concernées. Comme souligné précédemment, la communication d'informations en temps utile est un élément essentiel des obligations de transparence au titre des articles 13 et 14 et elle est, par nature, associée au concept de traitement loyal. Les informations concernant un *traitement ultérieur* doivent être fournies «avant de procéder à ce traitement ultérieur». La position du G29 est qu'une période de temps raisonnable devrait s'écouler entre la notification et le commencement du traitement, au lieu que le traitement démarre immédiatement dès réception de la notification par la personne concernée. Cela offrirait aux personnes concernées les avantages pratiques du principe de transparence, en les faisant bénéficier de la possibilité utile d'analyser (et éventuellement d'exercer leur droit à cet égard) le traitement ultérieur. La définition d'une période raisonnable dépendra des circonstances particulières. Selon le principe d'équité, plus le traitement ultérieur est intrusif (ou moins attendu), plus la période devrait être longue. De même, le principe de responsabilité exige des responsables du traitement qu'ils soient en mesure de démontrer que les délais raisonnables déterminés pour la communication de ces informations sont justifiés eu égard aux circonstances et que les délais dans l'ensemble sont équitables pour les personnes concernées. (Voir également les commentaires précédents en lien avec la vérification des délais raisonnables, aux points 30 à 32 ci-dessus.)

<u>Outils de visualisation</u>

49. Il est important de noter que le principe de transparence prévu par le RGPD ne doit pas nécessairement être mis en œuvre par des modes de communication linguistiques (écrits ou oraux). Le RGPD prévoit des outils de visualisation (en faisant notamment référence aux icônes, aux mécanismes de certification et aux labels et marques en matière de protection des données), le cas échéant. Le considérant 58[46] indique que l'accessibilité des informations adressées au public ou aux personnes concernées est particulièrement importante dans l'environnement numérique[47].

[45] Conformément au considérant 63, cette recommandation permettra à la personne concernée d'exercer son droit d'accès afin de prendre connaissance du traitement et d'en vérifier la licéité.

[46] «Ces informations pourraient être fournies sous forme électronique, par exemple via un site internet lorsqu'elles s'adressent au public. Ceci vaut tout particulièrement dans des situations où la multiplication des acteurs et la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité en ligne.»

[47] Dans ce contexte, les responsables du traitement devraient prendre en compte les personnes concernées qui sont malvoyantes (par exemple, les daltoniens rouge-vert).

Icônes

50. Le considérant 60 prévoit que les informations à communiquer à une personne concernée peuvent être «accompagnées» d'icônes normalisées, permettant ainsi une approche à plusieurs niveaux. Cependant, les icônes ne devraient pas simplement remplacer les informations nécessaires aux personnes concernées pour l'exercice de leurs droits ni ne devraient servir de solution de substitution pour satisfaire aux obligations du responsable du traitement au titre des articles 13 et 14. L'article 12, paragraphe 7, prévoit explicitement l'utilisation de telles icônes:

> *«Les informations à communiquer aux personnes concernées en application des articles 13 et 14 peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles sont lisibles par machine.»*

51. L'article 12, paragraphe 7, dispose que «*[l]orsque les icônes sont présentées par voie électronique, elles sont lisibles par machine*», ce qui laisse à penser qu'il peut exister des situations où les icônes ne sont pas présentées par voie électronique[48], par exemple les icônes présentées physiquement sur des documents, des appareils connectés ou l'emballage d'un appareil connecté, les notifications envoyées dans des lieux publics concernant le repérage Wi-Fi, les codes QR et les notifications de CCTV.

52. La finalité de l'utilisation d'icônes est claire: améliorer la transparence pour les personnes concernées en réduisant éventuellement la nécessité de devoir présenter de grandes quantités d'informations écrites à ces dernières. Néanmoins, l'utilité des icônes pour communiquer efficacement les informations requises au titre des articles 13 et 14 aux personnes concernées dépend de la normalisation des symboles et images, qui doivent être utilisés de façon universelle et reconnus dans l'Union européenne comme des raccourcis indiquant ces informations. À cet égard, le RGPD attribue à la Commission la responsabilité de l'élaboration d'un code d'icônes, mais le comité européen de la protection des données peut, à la demande de la Commission ou de son propre chef, fournir à la Commission un avis sur ces icônes[49]. Le G29 reconnaît, conformément au

[48] Il n'existe pas de définition de l'expression «lisible par machine» dans le RGPD, mais le considérant 21 de la directive 2013/37/UE définit un format «lisible par machine» comme étant:

> *«un format de fichier structuré de telle manière que des applications logicielles puissent facilement identifier, reconnaître et extraire des données spécifiques, notamment chaque énoncé d'un fait et sa structure interne. Les données encodées présentes dans des fichiers qui sont structurés dans un format lisible par machine sont des données lisibles par machine. Les formats lisibles par machine peuvent être ouverts ou propriétaires; il peut s'agir de normes formelles ou non. Les documents encodés dans un format de fichier qui limite le traitement automatique, en raison du fait que les données ne peuvent pas, ou ne peuvent pas facilement, être extraites de ces documents, ne devraient pas être considérés comme des documents dans des formats lisibles par machine. Les États membres devraient, le cas échéant, encourager l'utilisation de formats ouverts, lisibles par machine».*

[49] L'article 12, paragraphe 8, dispose que la Commission est habilitée à adopter des actes délégués en conformité avec l'article 92, aux fins de déterminer les informations à présenter sous la forme d'icônes ainsi que les procédures régissant la fourniture d'icônes normalisées. Le considérant 166 (qui traite des actes délégués de la Commission en général) est instructif et prévoit que la Commission procède aux consultations appropriées durant son travail

considérant 166, que l'élaboration d'un code d'icônes devrait être centrée sur une approche factuelle et qu'il sera nécessaire, en amont d'une telle normalisation, de mener des recherches approfondies conjointement avec les entreprises et le grand public à l'égard de l'efficacité des icônes dans ce contexte.

Mécanismes de certification, labels et marques

53. Outre l'utilisation d'icônes normalisées, le RGPD prévoit (à l'article 42) l'utilisation de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le RGPD et d'améliorer la transparence pour les personnes concernées[50]. Le G29 publiera des lignes directrices sur les mécanismes de certification en temps utile.

Exercice des droits des personnes concernées

54. La transparence impose une triple obligation aux responsables du traitement en ce qui concerne les droits des personnes concernées au titre du RGPD; en effet, ils doivent[51]:

- fournir aux personnes concernées des informations sur leurs droits[52] [conformément à l'article 13, paragraphe 2, point b), et à l'article 14, paragraphe 2, point c)];
- respecter le principe de transparence (par exemple, en ce qui concerne la qualité des communications énoncées à l'article 12, paragraphe 1) lorsqu'ils communiquent avec les personnes concernées au sujet de leurs droits au titre des articles 15 à 22 et 34; et
- faciliter l'exercice des droits des personnes concernées au titre des articles 15 à 22.

55. Les exigences du RGPD concernant l'exercice de ces droits et la nature des informations requises sont conçues de manière à *doter* les personnes concernées des informations *utiles* pour qu'elles puissent revendiquer leurs droits et demander des comptes aux responsables du traitement quant au traitement de leurs données à caractère personnel. Le considérant 59 souligne que «*des modalités devraient être prévues pour faciliter l'exercice par la personne concernée des droits qui lui sont conférés*» et que le responsable du traitement devrait «*également fournir les moyens de présenter des demandes par voie électronique, en particulier lorsque les données à caractère personnel font l'objet d'un traitement électronique*». La modalité fournie par un

préparatoire, y compris au niveau des experts. Toutefois, le comité européen de la protection des données joue également un rôle consultatif important en ce qui concerne la normalisation des icônes, puisque l'article 70, paragraphe 1, point r), dispose que le comité, de sa propre initiative ou, le cas échéant, à la demande de la Commission, a pour mission de rendre à la Commission un avis sur les icônes.

[50] Voir la référence au considérant 100.

[51] Conformément à la rubrique Transparence et modalités du RGPD sur les droits des personnes concernées (section 1, chapitre III, article 12).

[52] Accès, rectification, effacement, limitation du traitement, opposition au traitement, portabilité.

responsable du traitement pour que la personne concernée puisse exercer ses droits devrait être adaptée au contexte et à la nature de la relation et des interactions entre le responsable du traitement et la personne concernée. À cette fin, un responsable du traitement peut souhaiter fournir à une personne concernée une ou plusieurs modalités différentes pour l'exercice des droits de celle-ci, reflétant les différentes façons selon lesquelles la personne concernée interagit avec le responsable du traitement.

Exemple

Un prestataire de services de santé propose un formulaire électronique sur son site internet et des formulaires papier à la réception de ses cliniques afin de faciliter le dépôt des demandes d'accès aux données à caractère personnel, que ce soit en ligne ou en personne. En plus de proposer ces deux modalités, le service de santé accepte les demandes d'accès soumises par un autre moyen (par lettre ou e-mail, par exemple) et met à la disposition des personnes concernées un point de contact dédié (joignable par e-mail et par téléphone) pour les aider à exercer leurs droits.

Dérogations à l'obligation de fournir des informations

Dérogations à l'article 13

56. La seule dérogation possible aux obligations visées à l'article 13 d'un responsable du traitement qui a directement collecté des données à caractère personnel auprès d'une personne concernée est «*lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations*»[53]. Le principe de responsabilité exige des responsables du traitement qu'ils démontrent (en le documentant) quelles informations étaient déjà en la possession de la personne concernée, comment et quand elle les a reçues et qu'aucune modification n'a été apportée à ces informations susceptibles de les rendre obsolètes. De plus, l'utilisation de l'expression «dans la mesure où» à l'article 13, paragraphe 4, montre bien que même si la personne concernée a déjà reçu certaines informations relevant des catégories énoncées à l'article 13, le responsable du traitement a toujours pour obligation de compléter ces informations afin de garantir que la personne concernée dispose de toutes les informations répertoriées à l'article 13, paragraphes 1 et 2. L'exemple suivant est un exemple de bonne pratique concernant les limitations d'interprétation de la dérogation visée à l'article 13, paragraphe 4.

Exemple

Une personne s'inscrit à un service de messagerie en ligne et reçoit toutes les informations requises au titre de l'article 13, paragraphes 1 et 2, lors de son inscription. Six mois plus tard, la personne concernée active une fonctionnalité de messagerie instantanée connectée proposée par le prestataire de service de

[53] Article 13, paragraphe 4.

messagerie et indique son numéro de téléphone portable à cette fin. Le prestataire de service communique à la personne concernée certaines informations au titre de l'article 13, paragraphes 1 et 2, à l'égard du traitement du numéro de téléphone (par exemple, les finalités et la base juridique du traitement, les destinataires et la période de conservation), mais il ne fournit pas les informations que la personne a déjà reçues six mois auparavant et qui n'ont pas changé depuis (par exemple, l'identité et les coordonnées du responsable du traitement et du délégué à la protection des données, les informations sur les droits de la personne concernée et son droit de porter plainte auprès de l'autorité de contrôle pertinente). Par souci de bonne pratique, la série complète d'informations devrait néanmoins être à nouveau fournie à la personne concernée, mais cette dernière devrait pouvoir distinguer facilement quelles informations sont nouvelles. Le nouveau traitement exécuté au titre du service de messagerie instantanée peut affecter la personne concernée d'une façon qui pourrait l'inciter à vouloir exercer un droit dont elle ne se souvient peut-être pas, ayant été informée de celui-ci six mois auparavant. Fournir à nouveau toutes les informations permet de garantir que la personne concernée demeure bien informée de ses droits et de la façon dont ses données sont utilisées.

Dérogations à l'article 14

57. L'article 14 définit une série bien plus longue de dérogations à l'obligation d'information du responsable du traitement lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. Ces dérogations devraient, en règle générale, être interprétées et appliquées *stricto sensu*. Outre les circonstances où la personne concernée dispose déjà des informations en question [article 14, paragraphe 5, point a)], l'article 14, paragraphe 5, prévoit les dérogations suivantes:

- la communication de ces informations est impossible ou exigerait des efforts disproportionnés, en particulier pour le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ou elle rendrait impossible ou compromettrait gravement la réalisation des objectifs dudit traitement;
- l'obtention ou la communication des informations sont prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit des mesures appropriées visant à protéger les intérêts légitimes de la personne concernée; ou
- une obligation de secret professionnel (y compris une obligation légale de secret professionnel) qui est réglementée par le droit de l'Union ou le droit des États membres prévoit que les données à caractère personnel doivent rester confidentielles.

Se révèle impossible, exigerait des efforts disproportionnés et compromettrait gravement la réalisation des objectifs

58. L'article 14, paragraphe 5, point b), prévoit trois situations distinctes où l'obligation de fournir les informations visées à l'article 14, paragraphes 1, 2 et 4, est levée:

(i) lorsqu'elle se révèle impossible (en particulier à des fins archivistiques, de recherche scientifique ou historique ou à des fins statistiques);
(ii) lorsqu'elle exigerait des efforts disproportionnés (en particulier à des fins archivistiques, de recherche scientifique ou historique ou à des fins statistiques); ou
(iii) lorsque la fourniture des informations requises au titre de l'article 14, paragraphe 1, rendrait impossible ou compromettrait gravement la réalisation des objectifs dudit traitement.

«Se révèle impossible»

59. La situation dans laquelle la fourniture d'informations «se révèle impossible» en vertu de l'article 14, paragraphe 5, point b), est absolue et ne permet pas de demi-mesure, car la fourniture est simplement possible ou impossible; il n'existe pas de degrés d'impossibilité. Par conséquent, si un responsable du traitement souhaite faire jouer cette dérogation, il doit démontrer quels facteurs l'empêchent effectivement de communiquer les informations en question à la personne concernée. Si, après une certaine période, les facteurs ayant généré l'«impossibilité» cessent d'exister et qu'il devient donc possible de communiquer les informations à la personne concernée, le responsable du traitement devrait les communiquer immédiatement. Dans la pratique, rares sont les situations où un responsable du traitement peut démontrer qu'il est effectivement impossible de communiquer les informations à la personne concernée. L'exemple suivant en est l'illustration.

Exemple

Une personne s'inscrit à un service d'abonnement en ligne post-payé. Après l'inscription, le responsable du traitement collecte les données de crédit de la personne auprès d'une agence d'évaluation du crédit afin de décider de fournir ou non le service en question. Le protocole du responsable du traitement impose à ce dernier d'informer la personne concernée de la collecte de ses données de crédit dans les trois jours suivant la collecte, conformément à l'article 14, paragraphe 3, point a). Toutefois, l'adresse et le numéro de téléphone de la personne concernée ne figurent pas dans les registres publics (et la personne concernée vit à l'étranger). De plus, la personne concernée n'a pas donné d'adresse e-mail lors de son inscription au service, ou son adresse e-mail n'est pas valide. Le responsable du traitement réalise qu'il ne dispose d'aucun moyen pour contacter directement la personne concernée. Dans ce cas, toutefois, le responsable du traitement a la possibilité de fournir les informations relatives à la collecte des données par l'agence d'évaluation du crédit sur son site internet, avant la validation de l'inscription. Dans une telle situation, il ne serait donc pas impossible de fournir les informations au titre de l'article 14.

Impossibilité de fournir la source des données

60. Le considérant 61 indique que «*lorsque l'origine des données à caractère personnel n'a pas pu être communiquée à la personne concernée parce que plusieurs sources ont été utilisées, des informations générales devraient être fournies*». La levée de l'obligation de

fournir à la personne concernée des informations sur la source de ses données à caractère personnel s'applique uniquement lorsqu'une telle fourniture n'est pas possible en raison de l'impossibilité d'attribuer différents éléments des données à caractère personnel concernant une même personne à une source en particulier. En revanche, le simple fait qu'une base de données comprenant les données à caractère personnel de plusieurs personnes concernées ait été compilée par un responsable du traitement utilisant plus d'une source ne suffit pas à lever cette obligation s'il est possible (bien que chronophage ou fastidieux) de déterminer la source dont proviennent les données à caractère personnel des personnes concernées. Étant donné les obligations propres à la protection des données dès la conception et par défaut[54], les mécanismes de transparence devraient être intégrés à des systèmes de traitement dès le départ afin que toutes les sources des données à caractère personnel reçues par une entreprise puissent être suivies et retracées jusqu'à leur source à tout moment pendant le cycle de vie du traitement des données (voir le point 43 ci-dessus).

«*Efforts disproportionnés*»

61. Conformément à l'article 14, paragraphe 5, point b), à l'instar d'une situation où la fourniture d'informations «se révèle impossible», une situation exigeant des «efforts disproportionnés» peut s'appliquer, en particulier, au traitement «*à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques sous réserve des [...] garanties visées à l'article 89, paragraphe 1*». Le considérant 62 fait également référence à ces objectifs comme des cas où la fourniture d'informations à la personne concernée exigerait des efforts disproportionnés et dispose à cet égard que le nombre de personnes concernées, l'ancienneté des données, ainsi que les garanties appropriées éventuelles adoptées devraient être pris en considération. Compte tenu de l'importance accordée au considérant 62 et à l'article 14, paragraphe 5, point b), aux fins archivistiques, de recherche et statistiques à l'égard de l'application de cette dérogation, la position du G29 est que la dérogation ne devrait pas être *systématiquement* revendiquée par les responsables du traitement qui ne traitent pas des données à caractère personnel à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le G29 souligne le fait que, lorsque ces finalités sont effectivement poursuivies, les conditions énoncées à l'article 89, paragraphe 1, doivent être respectées et la communication des informations doit représenter un effort disproportionné.

62. Pour déterminer ce qui peut constituer une impossibilité ou des efforts disproportionnés au titre de l'article 14, paragraphe 5, point b), il apparaît pertinent qu'aucune dérogation comparable n'existe au titre de l'article 13 (lorsque les données à caractère personnel sont collectées auprès d'une personne concernée). La seule différence entre une situation au titre de l'article 13 et une situation au titre de l'article 14 est que, s'agissant de cette dernière, les données à caractère personnel ne sont pas collectées auprès de la personne concernée. Dès lors, il s'ensuit que l'impossibilité ou les efforts disproportionnés découlent généralement de circonstances qui ne s'appliquent pas si les données à caractère personnel sont collectées auprès de la personne concernée. En d'autres termes, l'impossibilité ou les efforts disproportionnés doivent être directement

[54] Article 25.

liés au fait que les données à caractère personnel ont été collectées autrement qu'auprès de la personne concernée.

Exemple

Un grand hôpital métropolitain exige de tous les patients admis pour un traitement de jour, un séjour de longue durée ou des consultations qu'ils remplissent un formulaire de renseignements demandant les coordonnées de deux parents proches (personnes concernées). Étant donné le très grand nombre de patients transitant par l'hôpital chaque jour, communiquer les informations requises au titre de l'article 14 à toutes les personnes désignées comme parent proche dans les formulaires remplis chaque jour par les patients exigerait des efforts disproportionnés de la part de l'hôpital.

63. Les facteurs susmentionnés correspondant au considérant 62 (le nombre de personnes concernées, l'ancienneté des données, ainsi que les garanties appropriées éventuelles adoptées) peuvent être à l'origine de situations obligeant un responsable du traitement à mettre en œuvre des efforts disproportionnés pour informer une personne concernée des informations pertinentes au titre de l'article 14.

Exemple

Des spécialistes de la recherche historique entreprennent de retracer une ascendance d'après des noms de famille et obtiennent indirectement un large ensemble de données correspondant à 20 000 personnes concernées. Cependant, l'ensemble de données a été collecté il y a 50 ans, n'a pas été mis à jour depuis et ne contient aucune coordonnée. Vu la taille de la base de données et, plus particulièrement, l'ancienneté des données, essayer de retrouver chaque personne concernée pour lui communiquer les informations prévues à l'article 14 exigerait des efforts disproportionnés de la part des chercheurs.

64. Quand un responsable du traitement souhaite s'appuyer sur la dérogation prévue à l'article 14, paragraphe 5, point b), au motif que la fourniture des informations exigerait des efforts disproportionnés, il devrait mettre en balance les efforts qui lui sont demandés pour communiquer les informations à la personne concernée et l'incidence et les effets sur la personne concernée dans le cas où celle-ci ne recevrait pas ces informations. Cette mise en balance devrait être documentée par le responsable du traitement conformément à ses obligations de responsabilité. Dans un tel cas, l'article 14, paragraphe 5, point b), précise que le responsable du traitement doit prendre des mesures appropriées pour protéger les droits, les libertés et les intérêts légitimes de la personne concernée. Cette disposition s'applique également lorsqu'un responsable du traitement constate que la fourniture des informations se révèle impossible ou est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. Une mesure appropriée, au sens de l'article 14, paragraphe 5, point b), devant être systématiquement prise par les responsables du traitement est de rendre les informations accessibles au public. Un responsable du traitement peut remplir cette obligation de différentes façons, par exemple en mettant les informations sur son site internet ou en les présentant de façon proactive dans un journal ou sur des affiches dans ses locaux. Les autres mesures appropriées, en plus de rendre les informations

accessibles au public, dépendront des circonstances du traitement, mais peuvent inclure: la réalisation d'une analyse d'impact relative à la protection des données; l'application de techniques de pseudonymisation des données; la réduction du nombre de données collectées et de la période de conservation; et la mise en œuvre de mesures techniques et organisationnelles pour garantir un niveau élevé de sécurité. Par ailleurs, des situations peuvent se présenter où un responsable du traitement traite des données à caractère personnel qui ne requièrent pas d'identifier une personne concernée (par exemple, des données pseudonymisées). Dans de tels cas, l'article 11, paragraphe 1, peut également être pertinent puisqu'il dispose qu'un responsable du traitement n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter le RGPD.

Compromettrait gravement la réalisation des objectifs

65. La situation finale couverte par l'article 14, paragraphe 5, point b), est celle où la fourniture d'informations par un responsable du traitement à une personne concernée au titre de l'article 14, paragraphe 1, est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. Pour appliquer cette dérogation, les responsables du traitement doivent démontrer que le simple fait de communiquer les informations prévues à l'article 14, paragraphe 1, anéantirait les objectifs du traitement. Le recours à cet aspect de l'article 14, paragraphe 5, point b), notamment, présuppose que le traitement des données satisfasse à tous les principes établis à l'article 5 et, plus important encore, que le traitement des données à caractère personnel soit loyal et fondé sur une base juridique en toutes circonstances.

Exemple

La banque A est tenue, en vertu de la législation en matière de lutte contre le blanchiment des capitaux, de signaler toute activité suspecte associée aux comptes qu'elle détient à l'autorité chargée de faire appliquer le droit financier. La banque B (située dans un autre État membre) informe la banque A que le titulaire d'un compte dans son établissement lui a demandé d'effectuer un virement, apparemment suspect, sur un compte détenu à la banque A. La banque A transmet les données concernant le titulaire du compte dans son établissement et signale les activités suspectes à l'autorité chargée de faire appliquer le droit financier. D'après la législation en matière de lutte contre le blanchiment des capitaux, une banque qui signale une suspicion de fraude et prévient le titulaire du compte en question qu'il peut faire l'objet d'une enquête des autorités de réglementation commet une infraction pénale. Dans ce cas, l'article 14, paragraphe 5, point b), s'applique, car communiquer à la personne concernée (le titulaire du compte de la banque A) les informations prévues à l'article 14 sur le traitement des données à caractère personnel du titulaire du compte reçues de la banque B compromettrait gravement les objectifs de la législation, qui comprennent la prévention des dénonciations. Toutefois, des informations générales devraient être communiquées à toutes les personnes décidant d'ouvrir un compte à la banque A, leur indiquant que leurs données à caractère personnel peuvent être traitées à des fins de lutte contre le blanchiment d'argent.

L'obtention ou la communication des informations sont expressément prévues par la loi

66. L'article 14, paragraphe 5, point c), autorise une levée des obligations d'information prévues à l'article 14, paragraphes 1, 2 et 4, dans la mesure où l'obligation ou la communication des données à caractère personnel «*sont expressément prévues par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis*». Cette dérogation dépend de la prévision par le droit en question de «*mesures appropriées visant à protéger les intérêts légitimes de la personne concernée*». Un tel droit doit concerner directement le responsable du traitement et l'obtention ou la communication en question devraient être obligatoires pour ce dernier. De même, le responsable du traitement doit être en mesure de démontrer que le droit en question lui est applicable et lui impose d'obtenir ou de communiquer lesdites données à caractère personnel. Bien qu'il revienne au droit de l'Union ou au droit de l'État membre d'élaborer la loi de sorte qu'elle prévoie des «*mesures appropriées visant à protéger les intérêts légitimes de la personne concernée*», le responsable du traitement devrait garantir (et être en mesure de démontrer) que l'obtention ou la communication de données à caractère personnel par ses soins respectent ces mesures. En outre, le responsable du traitement devrait signaler clairement aux personnes concernées qu'il obtient ou communique les données à caractère personnel en accord avec le droit en question, sauf en cas d'interdiction légale l'empêchant de le faire. Cette disposition est conforme au considérant 41 du RGPD, qui dispose qu'une base juridique ou une mesure législative devrait être claire et précise et que son application devrait être prévisible pour les justiciables, conformément à la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme. Toutefois, l'article 14, paragraphe 5, point c), ne s'applique pas lorsque le responsable du traitement est tenu de collecter les données *directement auprès de la personne concernée*, auquel cas l'article 13 s'applique. Dans cette situation, la seule dérogation au titre du RGPD exemptant le responsable du traitement de l'obligation de fournir à la personne concernée les informations sur le traitement est celle prévue par l'article 13, paragraphe 4 (c'est-à-dire lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations). Cependant, comme indiqué au point 68 ci-dessous, les États membres peuvent également légiférer, à l'échelon national et en accord avec l'article 23, sur d'autres limitations spécifiques au droit de transparence visé à l'article 12 et aux informations prévues aux articles 13 et 14.

Exemple

En vertu du droit national, une administration fiscale est soumise à l'obligation d'obtenir de la part des employeurs le montant des rémunérations de leurs salariés. Les données à caractère personnel n'étant pas collectées auprès des personnes concernées, l'administration fiscale est soumise aux obligations visées à l'article 14. Mais dès lors que l'obtention des données à caractère personnel par l'administration fiscale auprès des employeurs est expressément prévue par la loi, l'obligation d'information de l'article 14 ne s'applique pas à l'administration fiscale dans ce cas précis.

Confidentialité du fait d'une obligation de confidentialité

67. L'article 14, paragraphe 5, point d), prévoit une dérogation à l'obligation d'information imposée aux responsables du traitement lorsque les données à caractère personnel «*doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée par le droit de l'Union ou le droit des États membres, y compris une obligation légale de secret professionnel*». Lorsqu'un responsable du traitement souhaite se prévaloir de cette dérogation, il doit être en mesure de prouver qu'il a correctement identifié la dérogation en question et de démontrer que l'obligation de secret professionnel le concerne directement, de sorte que cela l'empêche de communiquer toutes les informations visées à l'article 14, paragraphes 1, 2 et 4, à la personne concernée.

Exemple

Un médecin (responsable du traitement) est tenu au secret professionnel à l'égard des informations médicales de ses patients. Un patient (auquel le respect du secret professionnel s'applique) communique au médecin des informations sur sa santé concernant une maladie génétique dont certains de ses proches sont atteints. Le patient fournit également au médecin certaines données à caractère personnel sur ses proches (personnes concernées), qui sont atteints de cette même maladie. Le médecin n'est pas tenu de fournir aux proches les informations visées à l'article 14 puisque la dérogation prévue à l'article 14, paragraphe 5, point d), s'applique. Si le médecin communiquait les informations prévues à l'article 14 aux proches, cela constituerait une violation du secret professionnel vis-à-vis de son patient.

<u>Limitations applicables aux droits des personnes concernées</u>

68. L'article 23 dispose que les États membres (ou l'Union) peuvent légiférer de manière à limiter davantage la portée des droits des personnes concernées à l'égard de la transparence et de leurs droits fondamentaux[55] lorsque de telles mesures respectent l'essence des libertés et droits fondamentaux et sont nécessaires et proportionnées pour garantir un ou plusieurs des dix objectifs énoncés à l'article 23, paragraphe 1, points a) à j). Lorsque de telles mesures nationales réduisent soit les droits spécifiques des personnes concernées soit les obligations générales de transparence, qui, autrement, s'appliqueraient aux responsables du traitement en vertu du RGPD, les responsables du traitement concernés devraient être en mesure de démontrer de quelle manière lesdites mesures nationales s'appliquent à eux. Conformément à l'article 23, paragraphe 2, point h), la mesure législative doit contenir une disposition concernant le droit des personnes concernées d'être informées de toute limitation de leurs droits, à moins que cela risque de nuire à la finalité de la limitation. Dans le même ordre d'idée, et en vertu du principe de loyauté, le responsable du traitement devrait également informer la personne concernée qu'il invoque (ou invoquera, au cas où ladite personne déciderait d'exercer un de ses droits en particulier) une telle *limitation législative nationale* à l'exercice des droits

[55] Conformément aux articles 12 à 22 et 34, ainsi qu'à l'article 5, dans la mesure où ses dispositions correspondent aux droits et obligations prévus aux articles 12 à 22.

de celle-ci ou à l'obligation de transparence, sauf si cela risquait de nuire à la finalité de la limitation législative. À ce titre, le principe de transparence impose au responsable du traitement de fournir des informations adaptées et en amont à la personne concernée au sujet de ses droits et de toute restriction spécifique applicable à ces droits que le responsable du traitement déciderait d'invoquer, de sorte que la personne concernée ne soit pas surprise par une prétendue limitation d'un droit en particulier si elle cherche à exercer, ultérieurement, ce droit contre le responsable du traitement. En ce qui concerne la pseudonymisation et la minimisation des données, et dans la mesure où le responsable du traitement peut chercher à invoquer l'article 11 du RGPD, le G29 a précédemment confirmé dans l'avis 3/2017[56] que l'article 11 du RGPD devrait être interprété comme un moyen de faire appliquer une véritable minimisation des données sans entraver l'exercice des droits des personnes concernées, et qu'un tel exercice doit être rendu possible grâce aux informations complémentaires fournies par les personnes concernées.

69. Par ailleurs, l'article 85 exige des États membres qu'ils concilient, par la loi, le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information. Cette obligation impose, entre autres, aux États membres de prévoir des exemptions ou dérogations appropriées à certaines dispositions du RGPD (notamment aux obligations de transparence au titre des articles 12 à 14) pour les traitements menés à des fins journalistiques et à des fins d'expression universitaire, artistique ou littéraire, si cela est nécessaire pour concilier les deux droits en question.

Transparence et violation de données

70. Le G29 a établi des lignes directrices distinctes sur les violations de données[57] mais, aux fins des présentes lignes directrices, les obligations d'un responsable du traitement concernant la communication des violations de données à une personne concernée doivent prendre pleinement en compte les obligations de transparence énoncées à l'article 12[58]. La communication d'une violation de données doit satisfaire aux mêmes obligations, telles que détaillées ci-dessus (notamment concernant le recours à des termes clairs et simples), que celles applicables à toute autre communication adressée à une personne concernée au sujet de ses droits ou liée à la communication d'informations au titre des articles 13 et 14.

[56] Avis 3/2017 sur le traitement des données à caractère personnel dans le contexte des systèmes de transport intelligents coopératifs (STI-C) – voir point 4.2.
[57] Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement 2016/679, WP 250.
[58] Ce point est clairement défini à l'article 12, paragraphe 1, qui fait spécifiquement référence à «…toute communication au titre des articles 15 à 22 **et de l'article 34** en ce qui concerne le traitement à la personne concernée…» [soulignement ajouté].

Annexe
Informations devant être communiquées à une personne concernée au titre de l'article 13 ou de l'article 14

Type d'information requise	Article pertinent (si les données à caractère personnel sont collectées directement auprès de la personne concernée)	Article pertinent (si les données à caractère personnel ne sont pas collectées auprès de la personne concernée)	Commentaires du G29 sur l'obligation d'information
L'identité et les coordonnées du responsable du traitement et, le cas échéant, de son représentant[59]	Article 13, paragraphe 1, point a)	Article 14, paragraphe 1, point a)	Ces informations devraient permettre d'identifier facilement le responsable du traitement et favoriser différentes formes de communication avec le responsable du traitement (par exemple, numéro de téléphone, e-mail, adresse postale, etc.)
Coordonnées du délégué à la protection des données, le cas échéant	Article 13, paragraphe 1, point b)	Article 14, paragraphe 1, point b)	Voir les lignes directrices du G29 sur le délégué à la protection des données[60].
Les finalités du traitement ainsi que sa base juridique	Article 13, paragraphe 1, point c)	Article 14, paragraphe 1, point c)	En plus d'établir la finalité du traitement visé pour les données à caractère personnel, la base juridique pertinente appliquée au titre de l'article 6 doit être précisée. Dans le cas de catégories spécifiques de données à caractère

[59] Conformément à l'article 4, paragraphe 17, du RGPD (et au sens du considérant 80), on entend par «représentant» une personne physique ou morale établie dans l'Union, désignée par le responsable du traitement ou le sous-traitant par écrit, en vertu de l'article 27, qui les représente en ce qui concerne leurs obligations respectives en vertu du RGPD. Cette obligation s'applique lorsque, conformément à l'article 3, paragraphe 2, le responsable du traitement ou le sous-traitant n'est pas établi dans l'Union européenne, mais qu'il traite les données à caractère personnel de personnes concernées qui se trouvent dans l'Union, et que ce traitement est lié à l'offre de biens ou services à ces personnes concernées dans l'Union ou au suivi de leur comportement.

[60] Lignes directrices sur le délégué à la protection des données, WP243 rev.01, version révisée et adoptée le 5 avril 2017.

			personnel, la disposition pertinente de l'article 9 (et, le cas échéant, du droit de l'Union ou de l'État membre en vertu duquel les données sont traitées) doit être précisée. Lorsque, conformément à l'article 10, des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes sont traitées au titre de l'article 6, paragraphe 1, le droit pertinent de l'Union ou d'un État membre en vertu duquel le traitement est effectué devrait, le cas échéant, être précisé.
Lorsque des intérêts légitimes [article 6, paragraphe 1, point f)] constituent la base juridique du traitement, les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers	Article 13, paragraphe 1, point d)	Article 14, paragraphe 2, point b)	L'intérêt spécifique en question doit être déterminé dans l'intérêt de la personne concernée. Par souci de bonne pratique, le responsable du traitement peut également fournir à la personne concernée les informations issues de la *mise en balance*, qui doit être réalisée pour pouvoir invoquer l'article 6, paragraphe 1, point f), en tant que base juridique au traitement, en amont de toute collecte de données à caractère personnel auprès de personnes concernées. Afin d'éviter de noyer d'informations les personnes concernées, ces éléments peuvent être inclus dans un avis ou une déclaration sur la protection de la vie privée à différents niveaux (voir le point 35). En tout état de cause, la position du G29 est que les informations

			communiquées aux personnes concernées devraient indiquer clairement que ces dernières ont la possibilité d'obtenir sur simple demande des informations relatives à la mise en balance. Cela est essentiel pour garantir une transparence efficace lorsque les personnes concernées ont des doutes quant au fait que la mise en balance ait été menée de façon équitable ou si elles souhaitent déposer plainte auprès d'une autorité de contrôle.
Catégories de données à caractère personnel concernées	Sans objet	Article 14, paragraphe 1, point d)	Ces informations sont requises dans un scénario au titre de l'article 14, car les données à caractère personnel n'ont pas été collectées auprès de la personne concernée qui n'a donc pas connaissance des catégories des données à caractère personnel obtenues par le responsable du traitement.
Les destinataires[61] (ou catégories de destinataires) des données à caractère personnel	Article 13, paragraphe 1, point e)	Article 14, paragraphe 1, point e)	Le terme «destinataire» est défini à l'article 4, paragraphe 9, comme signifiant «*la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel,* ***qu'il s'agisse ou non d'un tiers***» (mise en gras ajoutée). À cet effet, un destinataire n'est pas nécessairement un tiers. Par conséquent, les autres responsables du traitement, responsables conjoints du

[61] Selon la définition donnée à l'article 4, paragraphe 9, du RGPD et conformément au considérant 31.

			traitement et sous-traitants auxquels les données sont transférées ou communiquées sont couverts par le terme «destinataire» et des informations relatives à ces destinataires devraient être fournies en plus des informations relatives aux autres destinataires tiers. Les destinataires réels (nommément désignés) des données à caractère personnel ou les catégories de destinataires doivent être indiqués. Conformément au principe d'équité, les responsables du traitement doivent fournir aux personnes concernées les informations les plus significatives sur les destinataires. En pratique, il s'agit généralement de destinataires nommément désignés afin que les personnes concernées puissent savoir exactement qui détient leurs données à caractère personnel. Si les responsables du traitement choisissent de communiquer les catégories de destinataires, les informations devraient être les plus spécifiques possible et indiquer le type de destinataire (en fonction des activités qu'il mène), l'industrie, le secteur et le sous-secteur ainsi que l'emplacement des destinataires.
Le détail des transferts vers des pays tiers, la situation de tels transferts, et le	Article 13, paragraphe 1, point f)	Article 14, paragraphe 1, point f)	L'article pertinent du RGPD permettant le transfert et le mécanisme correspondant

détail des garanties pertinentes[62] (notamment l'existence ou l'absence d'une décision d'adéquation de la Commission[63]) ainsi que les moyens d'obtenir une copie de ces informations ou de connaître l'endroit où elles ont été mises à disposition			(par exemple, la décision d'adéquation au titre de l'article 45/ les règles d'entreprise contraignantes au titre de l'article 47/ les clauses types de protection des données au titre de l'article 46, paragraphe 2/ les dérogations et garanties au titre de l'article 49, etc.) devraient être précisés. Des informations concernant l'endroit où se trouvent les documents correspondants et la façon d'y accéder ou de les obtenir devraient également être fournies, par exemple en indiquant un lien vers le mécanisme utilisé. Conformément au principe d'équité, les informations fournies sur les transferts vers des pays tiers devraient être aussi utiles que possible aux personnes concernées; cela nécessite généralement la désignation des pays tiers.
La période de conservation (ou, si ce n'est pas possible, les critères utilisés pour déterminer cette période)	Article 13, paragraphe 2, point a)	Article 14, paragraphe 2, point a)	Ceci est lié à l'obligation de minimisation des données visée à l'article 5, paragraphe 1, point c), et à l'obligation de limitation de la conservation visée à l'article 5, paragraphe 1, point e). La période de conservation (ou les critères pour la déterminer) peut être dictée par différents facteurs comme des exigences réglementaires ou des lignes directrices industrielles, mais elle devrait être formulée de manière à ce que la personne concernée puisse évaluer, selon la situation dans

[62] Conformément à l'article 46, paragraphes 2 et 3.
[63] En vertu de l'article 45.

			laquelle elle se trouve, quelle sera la période de conservation s'agissant de données spécifiques ou en cas de finalités spécifiques. Le responsable du traitement ne peut se contenter de déclarer de façon générale que les données à caractère personnel seront conservées aussi longtemps que la finalité légitime du traitement l'exige. Le cas échéant, différentes périodes de stockage devraient être mentionnées pour les différentes catégories de données à caractère personnel et/ou les différentes finalités de traitement, notamment les périodes à des fins archivistiques.
Les droits suivants de la personne concernée: • accès; • rectification; • effacement; • limitation du traitement; • objection au traitement; • portabilité.	Article 13, paragraphe 2, point b)	Article 14, paragraphe 2, point c)	Ces informations devraient être spécifiques au scénario de traitement et inclure un résumé de ce que comprend le droit en question et des mesures pouvant être prises par la personne concernée pour l'exercer, ainsi que toute limitation audit droit (voir point 68 ci-dessus). En particulier, le droit de s'opposer au traitement doit être explicitement porté à l'attention de la personne concernée au plus tard au moment de la première communication avec la personne concernée et doit être présenté clairement et séparément de toute autre information[64]. En ce qui concerne le droit à

[64] Article 21, paragraphe 4, et considérant 70 (qui s'applique à la prospection).

			la portabilité, voir les lignes directrices du G29 sur le droit à la portabilité des données[65].
Lorsque le traitement dépend du consentement (ou du consentement explicite), le droit de retirer son consentement à tout moment	Article 13, paragraphe 2, point c)	Article 14, paragraphe 2, point d)	Ces informations devraient inclure des explications sur la façon de retirer son consentement, prenant en compte le fait qu'il devrait être aussi facile pour une personne concernée de retirer son consentement que de le donner[66].
Le droit d'introduire une réclamation auprès d'une autorité de contrôle	Article 13, paragraphe 2, point d)	Article 14, paragraphe 2, point e)	Ces informations devraient expliquer que, conformément à l'article 77, une personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, notamment dans l'État membre de sa résidence habituelle ou de son lieu de travail, ou en cas de violation alléguée du RGPD.
Si l'exigence de fournir les informations revêt un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat, ou s'il existe une obligation de fourniture des informations, ainsi que les conséquences éventuelles de leur non-fourniture.	Article 13, paragraphe 2, point e)	Sans objet	Par exemple, dans le cadre de relations de travail, fournir certaines informations à un employeur actuel ou éventuel peut être une exigence contractuelle. Les formulaires en ligne devraient déterminer clairement les champs «obligatoires», les champs facultatifs, et les conséquences si des champs obligatoires sont laissés vides.
La source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont	Sans objet	Article 14, paragraphe 2, point f)	La source spécifique aux données devrait être fournie à moins qu'il ne soit pas possible de le faire. Voir le point 60 pour plus

[65] Lignes directrices sur le droit à la portabilité des données, WP 242 rev.01, version révisée et adoptée le 5 avril 2017.
[66] Article 7, paragraphe 3.

issues ou non de sources accessibles au public			d'informations à cet égard. Si la source spécifique n'est pas nommée, les informations fournies devraient indiquer: la nature des sources (c'est-à-dire les sources publiques et privées) et les types d'organismes, d'entreprises et de secteurs.
L'existence d'une prise de décision automatisée, y compris un profilage et, le cas échéant, des informations utiles sur la logique utilisée et l'importance et les conséquences envisagées d'un tel traitement pour la personne concernée	Article 13, paragraphe 2, point f)	Article 14, paragraphe 2, point g)	Voir les lignes directrices du G29 sur les décisions individuelles automatisées et le profilage[67].

[67] Lignes directrices sur les décisions individuelles automatisées et le profilage au titre du règlement 2016/679, WP 251.

Lignes directrices relatives aux dérogations prévues à l'article 49 du RGPD (2/2018)

Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679

Adoptées le 25 mai 2018

1

Table des matières

Le comité européen de la protection des données,

Considérant l'article 70, paragraphe 1, points e) et j), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE,

A ADOPTÉ LES PRÉSENTES LIGNES DIRECTRICES:

1. GÉNÉRALITÉS

Le présent document vise à fournir des orientations concernant l'application de l'article 49 du règlement général sur la protection des données (ci-après le «RGPD»)[1], qui traite des dérogations dans le contexte des transferts de données à caractère personnel vers des pays tiers.

Le document s'appuie sur les précédents travaux[2] réalisés par le groupe de travail des autorités de protection des données de l'Union établi au titre de l'article 29 de la directive sur la protection des données (ci-après le «groupe de travail "Article 29"»), qui ont été repris par le comité européen de la protection des données (« CEPD ») en ce qui concerne les questions centrales soulevées par l'application des dérogations dans le contexte des transferts de données à caractère personnel vers des pays tiers. Le présent document sera revu et, si nécessaire, mis à jour, sur la base de l'expérience pratique acquise dans le cadre de l'application du RGPD.

Au moment d'appliquer l'article 49, il convient de garder à l'esprit que, conformément à l'article 44, l'exportateur de données qui transfère des données à caractère personnel vers des pays tiers ou à des organisations internationales doit aussi respecter les conditions définies dans les autres dispositions du RGPD. Chaque activité de traitement doit respecter les dispositions applicables en matière de protection des données, en particulier les articles 5 et 6. Un test en deux étapes doit donc être appliqué: d'abord, une base juridique doit s'appliquer au traitement des données proprement dit, avec toutes les dispositions pertinentes du RGPD; et, ensuite, les dispositions du chapitre V doivent être respectées.

Conformément à l'article 49, paragraphe 1, en l'absence de décision d'adéquation ou de garanties appropriées, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à certaines conditions. Dans le même temps, l'article 44 exige que toutes les dispositions du chapitre V soient appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le RGPD ne soit pas compromis. Cela

[1] RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
[2] Groupe de travail «Article 29», document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, 25 novembre 2005 (WP 114).

signifie aussi que le recours aux dérogations prévues à l'article 49 ne devrait jamais créer une situation dans laquelle pourrait se produire une violation des droits fondamentaux[3].

Le groupe de travail «Article 29», prédécesseur du CEPD, recommande depuis longtemps d'adopter [4] à l'égard des transferts, une approche par étapes fondée sur les meilleures pratiques et consistant à examiner d'abord si le pays tiers garantit un niveau de protection adéquat et à s'assurer que les données exportées y seront sauvegardées. Si le niveau de protection n'est pas adéquat eu égard à toutes les circonstances, l'exportateur de données devrait envisager de fournir des garanties adéquates. Les exportateurs de données devraient donc d'abord s'efforcer de trouver des possibilités de procéder au transfert à l'aide d'un des mécanismes prévus aux articles 45 et 46 du RGPD, et ne recourir aux dérogations prévues à l'article 49, paragraphe 1, qu'en l'absence de tels mécanismes.

Les dérogations visées à l'article 49 sont donc des exemptions du principe général selon lequel des données à caractère personnel ne peuvent être transférées vers des pays tiers que si un niveau de protection adéquat est offert dans le pays tiers ou si des garanties appropriées ont été apportées et si les personnes concernées bénéficient de droits opposables et effectifs afin de continuer à bénéficier de leurs droits fondamentaux et garanties[5]. De ce fait et conformément aux principes de droit inhérents à l'ordre juridique européen[6], les dérogations doivent être interprétées de manière restrictive afin que l'exception ne devienne pas la règle[7]. L'intitulé de l'article 49, qui indique que les dérogations doivent être utilisées pour les situations particulières («Dérogations pour des situations particulières»), va aussi dans ce sens.

Lorsqu'ils envisagent de transférer des données à caractère personnel vers des pays tiers ou à des organisations internationales, les exportateurs de données devraient donc privilégier les solutions qui offrent aux personnes concernées la garantie qu'elles continueront de bénéficier des droits fondamentaux et des garanties auxquels elles ont droit concernant le traitement de leurs données une fois que celles-ci ont été transférées. Comme les dérogations n'offrent pas de protection adéquate ou de garanties appropriées pour les données à caractère personnel transférées et comme les transferts basés sur une dérogation ne sont soumis à aucune autorisation préalable de la part des autorités de contrôle, le transfert de données à caractère personnel vers des pays tiers sur la base de dérogations entraîne des risques accrus pour les droits et les libertés des personnes concernées.

Les exportateurs de données doivent aussi savoir qu'en l'absence de décision d'adéquation, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer

[3]Groupe de travail «Article 29», WP 114, p. 11, et document de travail du groupe de travail «Article 29» sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale (WP 228), p. 41.

[4] Groupe de travail «Article 29», WP 114, p. 10.

[5] Considérant 114.

[6] Groupe de travail «Article 29», WP 114, p. 9.

[7] Voir groupe de travail «Article 29», WP 114, p. 9. La Cour de justice européenne a souligné à de nombreuses reprises que «la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire» (arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, point 56; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, point 77; Digital rights, point 52; du 6 octobre 2015, Schrems, C-362/14, point 92; et du 21 décembre 2016, Tele2 Sverige AB, C-203/15, point 96). Voir aussi le rapport sur le protocole additionnel à la Convention 108 concernant les autorités de contrôle et les flux transfrontières de données, article 2, paragraphe 2, point a), p. 6, accessible à l'adresse https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/181.1)

expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou à une organisation internationale (article 49, paragraphe 5).

Transferts occasionnels et non répétitifs

Le CEPD fait remarquer que le terme «occasionnel» est utilisé au considérant 111 et que l'expression «pas de caractère répétitif» est utilisée en rapport avec la dérogation aux fins d'«intérêts légitimes impérieux» visée à l'article 49, paragraphe 1, deuxième alinéa. Ces termes indiquent que ces transferts peuvent avoir lieu plus d'une fois, mais pas régulièrement, et ce en dehors du déroulement normal des opérations, par exemple dans des circonstances aléatoires ou inconnues et à des intervalles arbitraires. Par exemple, un transfert de données qui se déroule régulièrement dans le cadre d'une relation stable entre l'exportateur de données et un certain importateur de données peut au fond être considéré comme systématique et répété et ne peut donc pas être jugé occasionnel ou non répétitif. En outre, un transfert sera par exemple généralement considéré comme non occasionnel ou répétitif lorsque l'importateur de données dispose d'un accès direct à une base de données (par exemple au moyen d'une interface vers une application informatique) de manière générale.

Le considérant 111 opère une distinction entre les dérogations en indiquant expressément que les dérogations liées à un «contrat» et à une «action en justice» [article 49, paragraphe 1, premier alinéa, points b), c) et e)] sont limitées aux transferts «occasionnels», tandis que cette limitation n'existe pas pour les dérogations relatives au «consentement explicite», aux «motifs importants d'intérêt public», aux «intérêts vitaux» et au «registre» en application de l'article 49, paragraphe 1, premier alinéa, respectivement points a), d), f) et g).

Il convient néanmoins de souligner que même les dérogations qui ne sont pas expressément limitées aux transferts «occasionnels» ou «non répétitifs» doivent être interprétées de manière à ne pas contredire la nature même des dérogations, qui sont des exceptions à la règle qui veut que les données à caractère personnel ne peuvent être transférées vers un pays tiers à moins que ce pays offre un niveau adéquat de protection des données ou que des garanties appropriées soient mises en place[8].

Test de nécessité

Une condition fondamentale qui s'applique à plusieurs dérogations est que le transfert de données doit être «nécessaire» à une certaine fin. Le test de nécessité doit être appliqué pour évaluer la possibilité de recourir aux dérogations prévues à l'article 49, paragraphe 1, points b), c), d), e) et f). Ce test exige que l'exportateur de données dans l'Union évalue si un transfert de données à caractère personnel peut être considéré comme nécessaire pour la finalité spécifique de la dérogation envisagée. Pour de plus amples informations sur l'application particulière du test de nécessité à chacune des dérogations concernées, voir les sections correspondantes ci-après.

Article 48 en relation avec les dérogations

Le RGPD introduit une nouvelle disposition à l'article 48, dont il convient de tenir compte lorsque des transferts de données à caractère personnel sont envisagés. L'article 48 et le considérant 115 correspondant disposent que les décisions d'autorités ou de juridictions de pays tiers ne constituent pas en elles-mêmes des motifs légitimes de transferts de données vers les pays tiers. Un transfert en réponse à une décision d'autorités d'un pays tiers n'est donc en tout état de cause licite que s'il remplit les conditions définies au chapitre V[9].

[9]Voir considérant 115, 4e phrase.

Dans les situations où il existe un accord international, tel qu'un traité d'entraide judiciaire, les entreprises de l'Union devraient généralement refuser les demandes directes et renvoyer l'autorité du pays tiers requérante aux traités d'entraide judiciaire ou à un accord existant.

Cette interprétation est aussi tout à fait conforme à l'article 44, qui définit un principe général applicable à toutes les dispositions du chapitre V, afin de garantir que le niveau de protection des personnes physiques garanti par le RGPD n'est pas compromis.

2. INTERPRÉTATION PARTICULIÈRE DES DISPOSITIONS DE L'ARTICLE 49

2.1 La personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées – article 49, paragraphe 1, point a)

Les conditions générales pour que le consentement soit considéré comme valable sont définies à l'article 4, point 11[10], et à l'article 7 du RGPD[11]. Le groupe de travail «Article 29» donne des orientations concernant ces conditions générales applicables au consentement dans un document distinct, que le CEPD a endossé[12]. Ces conditions s'appliquent aussi au consentement dans le contexte de l'article 49, paragraphe 1, point a). Cependant, certains éléments supplémentaires sont requis pour que le consentement soit considéré comme une base juridique valable pour les transferts internationaux de données vers des pays tiers et à des organisations internationales, tel que prévu à l'article 49, paragraphe 1, point a), et c'est à ceux-ci que le présent document s'intéressera plus particulièrement.

Cette section 1 des présentes lignes directrices doit donc être lue en combinaison avec les lignes directrices sur le consentement du groupe de travail «Article 29», endossées par le CEPD,, qui fournissent une analyse plus détaillée de l'interprétation des conditions générales et des critères de consentement au titre du RGPD[13]. Il est aussi à noter que, conformément à l'article 49, paragraphe 3, les autorités publiques ne peuvent recourir à cette dérogation dans l'exercice de leurs prérogatives de puissance publique.

Selon l'article 49, paragraphe 1, point a), un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu en l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, à condition que «*la personne concernée [ait] donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées*».

2.1.1 Le consentement doit être explicite

Conformément à l'article 4, point 11, du RGPD, tout consentement doit être libre, spécifique, éclairé et univoque. Concernant cette dernière condition, l'article 49, paragraphe 1, point a), est plus strict puisqu'il exige un consentement «explicite». Il s'agit aussi d'une nouvelle exigence par rapport à l'article 26, paragraphe 1, point a), de la directive 95/46/CE, qui exigeait seulement que la personne concernée ait «indubitablement» donné son consentement. Le RGPD exige un consentement explicite dans les situations dans lesquelles il peut exister des risques particuliers pour la protection des données et, dès lors, un niveau individuel élevé de contrôle des données à caractère personnel est requis, comme c'est le cas pour le traitement de catégories particulières de données [article 9,

[10] Selon l'article 4, point 11, du RGPD, on entend par «consentement» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

[11] Les considérants 32, 33, 42 et 43 donnent également des orientations supplémentaires concernant le consentement

[12] Voir lignes directrices sur le consentement au sens du règlement 2016/679 du groupe de travail «Article 29» (WP 259).

[13] Idem.

paragraphe 2, point a)] et des décisions automatisées [article 22, paragraphe 2, point c)]. Ces risques particuliers apparaissent aussi dans le contexte des transferts internationaux de données.

Pour obtenir davantage d'orientations concernant l'exigence de consentement explicite, et pour les autres exigences applicables nécessaires pour que le consentement soit considéré comme valable, voir les lignes directrices sur le consentement du groupe de travail «Article 29», que le CEPD endossée[14].

2.1.2 Le consentement doit être spécifiquement donné pour le transfert/l'ensemble de transferts de données en question

Une des exigences pour que le consentement soit valable est qu'il soit spécifique. Pour constituer un motif valable de transfert de données en vertu de l'article 49, paragraphe 1, point a), le consentement doit donc être spécifiquement donné pour le transfert ou l'ensemble de transfert de données en question.

L'élément «spécifique» dans la définition du consentement vise à garantir un certain contrôle des utilisateurs et une certaine transparence pour la personne concernée. Cet élément est aussi étroitement lié à l'obligation que le consentement soit «éclairé».

Étant donné que le consentement doit être spécifique, il est parfois impossible d'obtenir, au moment de la collecte des données, le consentement préalable de la personne concernée pour un futur transfert ; par exemple, si la survenance et les circonstances particulières d'un transfert ne sont pas connues au moment où le consentement est demandé, l'incidence sur la personne concernée ne peut être évaluée. À titre d'exemple, une entreprise de l'Union collecte les données de ses clients à des fins bien précises (livraison de biens) sans envisager, au moment de la collecte, de transférer ces données à un tiers en dehors de l'Union. Quelques années plus tard, cependant, cette même entreprise est rachetée par une entreprise établie en dehors de l'Union qui souhaite transférer les données à caractère personnel de ses clients à une autre entreprise en dehors de l'Union. Pour que ce transfert soit valable en vertu de la dérogation relative au consentement, la personne concernée doit donner son consentement à ce transfert spécifique au moment où celui-ci est envisagé. Par conséquent, le consentement donné au moment de la collecte des données par l'entreprise de l'Union à des fins de livraison n'est pas suffisant pour justifier le recours à cette dérogation pour le transfert des données à caractère personnel en dehors de l'Union qui est envisagé ultérieurement.

L'exportateur de données doit donc veiller à obtenir le consentement spécifique avant que le transfert soit mis en place, même si cela se produit après la collecte des données. Cette exigence est aussi liée à la nécessité que le consentement soit éclairé. Il est possible d'obtenir le consentement spécifique d'une personne concernée avant le transfert et au moment de la collecte des données à caractère personnel tant que la personne concernée est informée de ce transfert particulier et que les circonstances du transfert ne changent pas après que la personne concernée a donné son consentement spécifique. L'exportateur de données doit donc veiller à ce que les exigences définies au point 1.3 ci-après soient aussi satisfaites.

2.1.3 Le consentement doit être éclairé[15], en particulier en ce qui concerne les éventuels risques du transfert

Cette condition est particulièrement importante, car elle renforce et précise d'avantage l'exigence générale de consentement «éclairé» telle qu'applicable à tout consentement et prévue à l'article 4,

[14] Idem.

[15] Les exigences générales de transparence prévues aux articles 13 et 14 du RGPD doivent aussi être satisfaites. Pour de plus amples informations, voir les lignes directrices sur la transparence en vertu du règlement (UE) 2016/679 (WP 260).

point 11[16]. En conséquence, l'exigence générale de consentement «éclairé» nécessite, dans le cas du consentement en tant que base licite en vertu de l'article 6, paragraphe 1, point a), à un transfert de données, que la personne concernée soit dûment informée à l'avance des circonstances spécifiques du transfert (à savoir, l'identité du responsable du traitement, la finalité du transfert, le type de données, l'existence du droit de retirer son consentement, et l'identité ou les catégories des destinataires)[17].

Outre cette exigence générale de consentement «éclairé», lorsque des données à caractère personnel sont transférées vers un pays tiers en vertu de l'article 49, paragraphe 1, point a), cette disposition exige que les personnes concernées soient aussi informées des risques spécifiques résultant du fait que leurs données seront transférées vers un pays qui n'offre pas une protection adéquate et qu'aucune garantie appropriée visant à protéger les données n'est mise en œuvre. Il est essentiel de fournir ces informations à la personne concernée afin de lui permettre de donner son consentement en pleine connaissance de ces faits particuliers concernant le transfert; dès lors, si elles ne sont pas fournies, la dérogation ne s'appliquera donc pas.

Les informations fournies aux personnes concernées afin d'obtenir leur consentement en vue du transfert de leurs données à caractère personnel à des tiers établis dans des pays tiers doivent aussi préciser tous les destinataires ou toutes les catégories de destinataires des données, tous les pays vers lesquels les données à caractère personnel sont transférées, le fait que le consentement est la base licite du transfert, ainsi que la circonstance que le pays tiers vers lequel les données seront transférées n'offre pas un niveau adéquat de protection des données fondé sur une décision de la Commission Européenne[18]. De plus, comme indiqué ci-dessus, des informations doivent être fournies concernant les éventuels risques pour la personne concernée découlant de l'absence de protection adéquate dans le pays tiers et de l'absence de garanties appropriées. Cet avertissement, qui pourrait être normalisé, devrait par exemple indiquer que le pays tiers est susceptible de ne pas disposer d'une autorité de contrôle ou de principes de traitement des données, ou encore de droits des personnes concernées.

Dans le cas particulier où un transfert est effectué après la collecte des données à caractère personnel auprès de la personne concernée, l'exportateur de données doit informer la personne concernée du transfert et des risques qu'il comporte avant que celui-ci n'ait lieu afin d'obtenir son consentement explicite au transfert «envisagé».

Comme le montre l'analyse ci-dessus, le RGPD fixe un seuil élevé pour le recours à la dérogation relative au consentement. Ce seuil élevé, combiné au fait que la personne concernée peut à tout moment retirer son consentement, signifie que le consentement peut s'avérer ne pas être une solution réalisable à long terme pour les transferts vers les pays tiers.

[16] Voir lignes directrices sur le consentement au sens du règlement 2016/679 du groupe de travail «Article 29» (WP 259).
[17] Idem, p. 15.
[18] Cette dernière exigence découle aussi de l'obligation d'informer les personnes concernées [article 13, paragraphe 1, point f), et article 14, paragraphe 1, point e)].

2.2 Le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée – article 49, paragraphe 1, point b)

Selon le considérant 111, les transferts de données en vertu de cette dérogation peuvent avoir lieu «*lorsque le transfert est **occasionnel** et **nécessaire** dans le cadre d'un contrat […]*»[19].

En général, bien que les dérogations relatives à l'exécution d'un contrat puissent sembler potentiellement assez larges, elles sont limitées par les critères de «*nécessité*» et de «*transferts occasionnels*».

Nécessité du transfert de données

Le «test *de nécessité*» [20] limite le nombre de cas dans lesquels l'article 49, paragraphe 1, point b), peut être invoqué[21]. Il exige un lien étroit et important entre le transfert de données et les finalités du contrat.

Cette dérogation ne peut, par exemple, pas être utilisée lorsqu'un groupe d'entreprises a, à des fins commerciales, centralisé ses fonctions de paiement et de gestion des ressources humaines pour l'ensemble de son personnel dans un pays tiers, car il n'existe pas de lien direct et objectif entre l'exécution du contrat de travail et ce transfert[22]. D'autres motifs de transfert prévus au chapitre V, tels que les clauses contractuelles types ou les règles d'entreprise contraignantes, peuvent cependant être adéquats pour le transfert en question.

En revanche, le transfert par les agents de voyage de données à caractère personnel concernant leurs différents clients à des hôtels ou à d'autres partenaires commerciaux auxquels il est fait appel dans le cadre de l'organisation du séjour de ces clients à l'étranger peut être jugé nécessaire aux fins du contrat conclu par l'agent de voyage et le client car, dans ce cas, il existe un lien suffisamment étroit et important entre le transfert de données et la finalité du contrat (l'organisation du voyage du client).

Cette dérogation ne peut être appliquée aux transferts d'informations supplémentaires non nécessaires à l'exécution du contrat ou, respectivement, à la mise en œuvre des mesures précontractuelles demandées par la personne concernée[23]; pour les données supplémentaires, d'autres outils seront donc requis.

Transferts occasionnels

Cette dérogation n'autorise le transfert de données à caractère personnel que si ce transfert est occasionnel[24]. Il convient d'établir au cas par cas si un ou des transferts de données sont jugés «*occasionnels*» ou «*non occasionnels*».

Un transfert peut ici être jugé occasionnel par exemple si les données à caractère personnel d'un directeur des ventes, qui, dans le contexte de son contrat de travail, se rend chez différents clients

[19] Le critère des transferts «occasionnels» se trouve au considérant 111 et s'applique aux dérogations prévues à l'article 49, paragraphe 1, points b), c) et e).
[20] Voir aussi avis 06/2014 du groupe de travail «Article 29» sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE (WP 217).
[21] L'exigence de «nécessité» se retrouve aussi dans les dérogations prévues à l'article 49, paragraphe 1, points c) à f).
[22] Il ne sera en outre pas considéré comme occasionnel (voir ci-après).
[23] De façon plus générale, toutes les dérogations prévues à l'article 49, paragraphe 1, points b) à f), permettent uniquement que les données qui sont nécessaires aux fins du transfert soient transférées.
[24] Concernant la définition générale du terme «occasionnel», voir page 4.

dans des pays tiers, doivent être envoyées à ces clients afin d'organiser les réunions. Un transfert pourrait aussi être considéré comme occasionnel si une banque de l'Union transfère des données à caractère personnel à une banque dans un pays tiers afin d'exécuter une demande de paiement d'un client, tant que ce transfert n'a pas lieu dans le cadre d'une relation de coopération stable entre les deux banques.

En revanche, les transferts ne sont pas considérés comme «occasionnels» lorsqu'une entreprise multinationale organise des formations dans un centre de formation dans un pays tiers et transfère systématiquement les données à caractère personnel des employés qui suivent un cours de formation (par exemple, des données telles que le nom et l'intitulé du poste, mais potentiellement aussi des exigences alimentaires ou des restrictions de mobilité). Les transferts de données qui se produisent régulièrement dans le cadre d'une relation stable sont jugés systématiques et répétés, et dépassent donc le caractère «occasionnel». En conséquence, dans ce cas, de nombreux transferts de données dans le cadre d'une relation d'affaires ne peuvent être basés sur l'article 49, paragraphe 1, point b).

En vertu de l'article 49, paragraphe 3, cette dérogation n'est pas applicable aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

2.3 Le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale – article 49, paragraphe 1, point c)

L'interprétation de cette disposition est nécessairement analogue à celle de l'article 49, paragraphe 1, point b); à savoir qu'un transfert de données vers un pays tiers ou à une organisation internationale en l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, ne peut être jugé comme relevant de la dérogation de l'article 49, paragraphe 1, point c), que s'il peut être considéré comme «*nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale*».

En plus de devoir être nécessaires, le considérant 111 indique que les transferts de données ne peuvent avoir lieu que «*lorsque le transfert est **occasionnel** et **nécessaire** dans le cadre d'un contrat [...]*». Par conséquent, outre le «test *de nécessité*», les données à caractère personnel ne peuvent ici aussi être transférées au titre de cette dérogation que si le transfert est occasionnel.

Nécessité du transfert de données et conclusion du contrat dans l'intérêt de la personne concernée

Lorsqu'une organisation a, à des fins commerciales, externalisé des activités telles que la gestion des salaires à des prestataires de services en dehors de l'Union, cette dérogation ne peut constituer la base des transferts de données à ces fins, car aucun lien étroit et important entre le transfert et un contrat conclu dans l'intérêt de la personne concernée ne peut être établi, même si l'objectif final est la gestion du salaire de l'employé[25]. D'autres outils de transfert prévus au chapitre V peuvent constituer une base plus adéquate pour ces transferts, tels que les clauses contractuelles types ou les règles d'entreprise contraignantes.

Transferts occasionnels

De plus, des données à caractère personnel ne peuvent être transférées en vertu de cette dérogation que lorsque le transfert est occasionnel, comme c'est le cas en vertu de la dérogation prévue à

[25] Il ne sera en outre pas considéré comme occasionnel (voir ci-après).

l'article 49, paragraphe 1, point b). Par conséquent, afin d'évaluer si ce transfert est occasionnel, il convient d'appliquer le même critère[26].

Enfin, en vertu de l'article 49, paragraphe 3, cette dérogation n'est pas applicable aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique[27].

2.4 Le transfert est nécessaire pour des motifs importants d'intérêt public – article 49, paragraphe 1, point d)

Cette dérogation, généralement appelée «dérogation relative à un intérêt public important», est très semblable à la disposition de l'article 26, paragraphe 1, point d), de la directive 95/46/CE[28], qui prévoit qu'un transfert ne doit avoir lieu que s'il est nécessaire ou rendu juridiquement obligatoire pour des motifs importants d'intérêt public.

En vertu de l'article 49, paragraphe 4, seuls les intérêts publics reconnus par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis peuvent entraîner l'application de cette dérogation.

Cependant, pour que cette dérogation soit applicable, il ne suffit pas que le transfert de données soit requis (par exemple par une autorité d'un pays tiers) pour une enquête dans l'intérêt public d'un pays tiers qui, au sens abstrait, existe aussi dans le droit de l'Union ou le droit de l'État membre. Lorsque, par exemple, une autorité d'un pays tiers demande un transfert de données pour une enquête dans le cadre de la lutte contre le terrorisme, la simple existence d'un acte législatif de l'Union ou de l'État membre également destiné à lutter contre le terrorisme ne constitue pas en soi une raison suffisante pour appliquer l'article 49, paragraphe 1, point d), à ce transfert. Comme le groupe de travail «Article 29», prédécesseur du CEPD, l'a souligné dans de précédentes déclarations[29], la dérogation s'applique plutôt uniquement lorsqu'il peut aussi être déduit du droit de l'Union ou du droit de l'État membre auquel le responsable du traitement est soumis que ces transferts de données sont autorisés pour des motifs importants d'intérêt public, y compris dans l'esprit de réciprocité pour la coopération internationale. L'existence d'un accord international ou d'une convention internationale qui reconnaît un certain objectif et qui prévoit une coopération internationale afin de favoriser cet objectif peut être un indicateur au moment d'évaluer l'existence d'un intérêt public en vertu de l'article 49, paragraphe 1, point d), tant que l'Union ou les État membres sont parties à cet accord ou à cette convention.

Bien qu'il soit essentiellement destiné à être utilisé par les autorités publiques, les entités privées peuvent aussi se fonder sur l'article 49, paragraphe 1, point d). Certains exemples cités au considérant 112 vont dans ce sens et mentionnent des transferts effectués tant par des autorités publiques que par des entités privées[30].

[26] Concernant la définition générale du terme «occasionnel», voir page 4.
[27] Pour de plus amples informations, voir section 1, page 5 ci-dessus.
[28] DIRECTIVE 95/46/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[29] Avis 10/2006 du groupe de travail «Article 29»sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), WP 128, p. 27.
[30] *«[É]change international de données entre autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financière, entre services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des contacts des personnes atteintes de maladies contagieuses ou en vue de réduire et/ou d'éliminer le dopage dans le sport.»*

En conséquence, l'exigence essentielle pour que cette dérogation soit applicable est l'existence d'un intérêt public important et non la nature de l'organisation (publique, privée ou internationale) qui transfère ou reçoit les données.

Les considérants 111 et 112 indiquent que cette dérogation n'est pas limitée aux transferts de données qui sont «occasionnels»[31]. Cela ne signifie cependant pas que les transferts de données en vertu de la dérogation relative à l'intérêt public important prévue à l'article 49, paragraphe 1, point d), peuvent avoir lieu à grande échelle et de façon systématique. Il convient plutôt de respecter le principe général selon lequel les dérogations définies à l'article 49 ne doivent pas devenir «la règle» en pratique, mais bien être limitées à des situations particulières, et chaque exportateur de données doit veiller à ce que le transfert remplisse le strict test de nécessité[32].

Lorsque des transferts sont effectués dans l'exercice normal des activités ou des pratiques, le CEPD encourage vivement tous les exportateurs de données (en particulier les organismes publics[33]) à encadrer ceux-ci en mettant en place des garanties appropriées conformément à l'article 46 plutôt qu'en se fondant sur la dérogation prévue à l'article 49, paragraphe 1, point d).

2.5 Le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice – article 49, paragraphe 1, point e)

Constatation, exercice ou défense de droits en justice

En vertu de l'article 49, paragraphe 1, point e), des transferts peuvent avoir lieu lorsque «*le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice*». Selon le considérant 111, un transfert peut être effectué lorsqu'il est «*occasionnel et nécessaire dans le cadre d'un contrat ou d'une action en justice, qu'il s'agisse d'une procédure judiciaire, administrative ou extrajudiciaire, y compris de procédures devant des organismes de régulation*». Cela couvre toute une série d'activités, par exemple, dans le contexte d'une enquête pénale ou administrative dans un pays tiers (par exemple, loi anti-trust, corruption, délit d'initié ou situations similaires), dans le cadre desquelles la dérogation peut s'appliquer à un transfert de données afin de permettre à la personne concernée de se défendre ou d'obtenir la levée d'une amende légalement prévue, ou une réduction de celle-ci, par exemple dans les enquêtes anti-trust. Par ailleurs, les transferts de données aux fins de procédures préliminaires formelles de production de pièces dans les litiges civils peuvent relever de cette dérogation. Elle peut aussi couvrir les actes de l'exportateur de données visant à engager des procédures dans un pays tiers, par exemple à intenter un procès ou demander l'approbation d'une fusion. La dérogation ne peut être utilisée pour justifier le transfert de données à caractère personnel sur la base de la simple possibilité que des procédures judiciaires ou des procédures formelles pourraient être engagées à l'avenir.

Cette dérogation peut s'appliquer aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique (article 49, paragraphe 3).

La combinaison des termes «droits en justice» et «procédure» signifie que la procédure en question doit avoir une base juridique, y compris un processus formel, défini juridiquement, mais qu'elle ne se limite pas nécessairement aux procédures judiciaires ou administratives («ou [d'une procédure] extrajudiciaire»). Comme un transfert doit être effectué **dans le cadre** d'une procédure, un lien étroit

[31] Concernant la définition générale du terme «occasionnel», voir page 4.
[32] Voir également page 3.
[33] Par exemple, les autorités de surveillance financière qui échangent des données dans le contexte des transferts internationaux de données à caractère personnel à des fins de coopération administrative.

est nécessaire entre le transfert de données et une procédure spécifique concernant la situation en question. L'applicabilité abstraite d'un certain type de procédure n'est pas suffisante.

Les responsables du traitement et les sous-traitants doivent savoir que le droit national peut aussi contenir ce que l'on appelle des «lois de blocage», qui interdisent ou limitent le transfert de données à caractère personnel à des juridictions étrangères, voire à d'autres organismes officiels étrangers.

Nécessité du transfert de données

Un transfert de données particulier ne peut avoir lieu que lorsqu'il est **nécessaire** à la constatation, à l'exercice ou à la défense des droits en justice en question. Ce «test *de nécessité*» exige un lien étroit et important entre les données en question et la constatation, l'exercice ou la défense spécifique de la position juridique[34]. Le simple intérêt des autorités du pays tiers ou l'éventuelle «bonne volonté» dont celles-ci pourraient faire preuve ne sont en tant que tels pas suffisants.

S'il peut être tentant pour l'exportateur de données de transférer toutes les données à caractère personnel susceptibles d'être utiles en réponse à une demande ou pour engager des procédures judiciaires, cela ne serait pas conforme à cette dérogation ni au RGPD en général, car (selon le principe de minimisation des données) cela souligne la nécessité que les données à caractère personnel soient adéquates, pertinentes et limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées.

Concernant les procédures contentieuses, le groupe de travail «Article 29», prédécesseur du CEPD , a déjà présenté une approche en plusieurs étapes pour déterminer si les données à caractère personnel doivent être transférées, comprenant l'application de ce principe. Dans un premier temps, il convient d'évaluer soigneusement si des données anonymisées seraient suffisantes dans le cas en question. Dans le cas contraire, alors le transfert de données pseudonymisées pourrait être envisagé. S'il est nécessaire d'envoyer des données à caractère personnel vers un pays tiers, leur pertinence pour la finalité en question doit être évaluée avant le transfert, de sorte que seul un ensemble de données à caractère personnel réellement nécessaires soit transféré et divulgué.

Transfert occasionnel

Ces transferts ne devraient être effectués que s'ils sont occasionnels. Pour de plus amples informations sur la définition des transferts occasionnels, voir la section pertinente consacrée aux transferts «occasionnels et non répétitifs»[35]. Les exportateurs de données devraient évaluer soigneusement chaque cas particulier.

2.6 Le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement – article 49, paragraphe 1, point f)

La dérogation prévue à l'article 49, paragraphe 1, point f), s'applique évidemment lorsque les données sont transférées en cas d'urgence médicale et lorsqu'il est considéré que ce transfert est directement nécessaire afin de prodiguer les soins médicaux requis.

Il doit donc par exemple être juridiquement possible de transférer des données (y compris certaines données à caractère personnel) si la personne concernée, alors qu'elle se trouve en dehors de l'Union, est inconsciente et nécessite des soins médicaux d'urgence, et que seul un exportateur (par exemple,

[34] Considérant 111: «nécessaire dans le cadre d'un contrat ou d'une action en justice».
[35] Page 4.

son médecin habituel), établi dans un État membre de l'Union, est en mesure de fournir ces données. Dans ce cas, le droit part du principe que le risque imminent de préjudice grave pour la personne concernée l'emporte sur les préoccupations de protection des données.

Le transfert doit être lié à l'intérêt individuel de la personne concernée ou à celui d'une autre personne et, lorsqu'il concerne des données de santé, il doit être nécessaire pour poser un diagnostic essentiel. En conséquence, cette dérogation ne peut être utilisée pour justifier un transfert de données médicales à caractère personnel en dehors de l'Union si la finalité du transfert n'est pas de traiter le cas particulier de la personne concernée ou celui d'une autre personne mais bien, par exemple, d'effectuer des recherches médicales générales qui ne produiront pas de résultats avant un certain temps dans le futur.

En effet, le RGPD ne limite pas le recours à cette dérogation à l'intégrité physique d'une personne, elle donne aussi la possibilité, par exemple, d'envisager les cas dans lesquels l'intégrité mentale d'une personne devrait être protégée. Dans ce cas, la personne concernée serait aussi incapable (physiquement ou juridiquement) de donner son consentement au transfert de ses données à caractère personnel. De plus, la personne concernée dont les données à caractère personnel font l'objet du transfert doit spécifiquement ne pas être en mesure (physiquement ou juridiquement) de donner son consentement à ce transfert.

Cependant, lorsque la personne concernée est en mesure de prendre une décision valable, et que son consentement peut être sollicité, alors cette dérogation ne peut s'appliquer.

Par exemple, lorsque les données à caractère personnel sont requises pour empêcher l'expulsion d'une propriété, elles ne relèvent pas de cette dérogation, car bien que le logement puisse être considéré comme un intérêt vital, la personne concernée peut donner son consentement au transfert de ses données.

Cette capacité de prendre une décision valable peut dépendre d'une incapacité physique, mentale, mais aussi juridique. Une incapacité juridique peut englober, sans préjudice des mécanismes nationaux de représentation, par exemple le cas d'un mineur d'âge. Cette incapacité juridique doit être prouvée, selon le cas, au moyen d'un certificat médical attestant l'incapacité mentale de la personne concernée ou d'un document des autorités publiques confirmant la situation juridique de la personne concernée.

Les transferts de données à une organisation humanitaire internationale nécessaires en vue d'accomplir une mission relevant des conventions de Genève ou de respecter le droit humanitaire international applicable dans un conflit armé peuvent aussi relever de l'article 49, paragraphe 1, point f) (voir considérant 112). De nouveau, dans ces cas, la personne concernée doit être physiquement ou juridiquement incapable de donner son consentement.

Le transfert de données à caractère personnel à la suite de catastrophes naturelles et dans le contexte du partage d'informations à caractère personnel avec des entités et des personnes aux fins d'opérations de secours (par exemple, les proches de victimes de catastrophes naturelles, ainsi qu'avec les services gouvernementaux et d'urgence) peut être justifié au titre de cette dérogation. Ce genre d'événements inattendus (inondations, séismes, ouragans, etc.) peut justifier le transfert d'urgence de certaines données à caractère personnel afin de connaître, par exemple, la position géographique et la situation des victimes. Dans ces situations, on considère que la personne concernée est incapable de donner son consentement au transfert de ses données.

2.7. Transfert effectué au départ d'un registre public – article 49, paragraphe 1, point g), et paragraphe 2

L'article 49, paragraphe 1, point g), et paragraphe 2, autorise le transfert de données à caractère personnel au départ de registres à certaines conditions. Un registre est généralement défini comme une «*archive (écrite) contenant des entrées régulières d'éléments ou de détails*» ou comme «*une liste officielle de noms ou d'éléments*» [36]; dans le contexte de l'article 49, un registre pourrait être au format écrit ou électronique.

Le registre en question doit, conformément au droit de l'Union ou au droit d'un État membre, être destiné à fournir des informations au public. Par conséquent, les registres privés (qui relèvent de la responsabilité d'organismes privés) ne rentrent pas dans le champ d'application de cette dérogation (par exemple, les registres privés qui permettent d'évaluer la solvabilité).

Le registre doit être ouvert à la consultation:

a) du public en général ou

b) de toute personne justifiant d'un intérêt légitime.

Il peut par exemple s'agir de: registres d'entreprises, registres d'associations, registres de condamnations pénales, registres de propriétés (foncières) et registres de véhicules publics.

Outre les exigences générales relatives à l'établissement des registres eux-mêmes, les transferts au départ de ces registres ne peuvent avoir lieu que si et dans la mesure où, dans chaque cas, les conditions de consultation prévues dans le droit de l'Union ou de l'État membre sont remplies [concernant ces conditions générales, voir article 49, paragraphe 1, point g)].

Les responsables du traitement et les sous-traitants qui souhaitent transférer des données à caractère personnel au titre de cette dérogation doivent savoir qu'un transfert ne peut porter sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre (article 49, paragraphe 2). Lorsqu'un transfert intervient au départ d'un registre établi par la loi et lorsqu'il est destiné à être consulté par des personnes ayant un intérêt légitime, il ne peut être effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires, compte tenu des intérêts et des droits fondamentaux de la personne concernée[37]. Au cas par cas, les exportateurs de données, au moment d'évaluer si le transfert est approprié, doivent toujours prendre en considération les intérêts et les droits de la personne concernée.

Toute utilisation ultérieure des données à caractère personnel issues de ces registres susmentionnés ne peut avoir lieu qu'en conformité avec le droit applicable en matière de protection des données.

Cette dérogation peut, elle aussi, s'appliquer aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique (article 49, paragraphe 3).

2.8. Intérêts légitimes impérieux – article 49, paragraphe 1, deuxième alinéa

L'article 49, paragraphe 1, deuxième alinéa, introduit une nouvelle dérogation qui ne figurait auparavant pas dans la directive. Dans un certain nombre de conditions spécifiques énumérées expressément, des données à caractère personnel peuvent être transférées si c'est nécessaire aux fins des intérêts légitimes impérieux poursuivis par l'exportateur de données.

[36] Merriam Webster Dictionary, https://www.merriam-webster.com/dictionary/register (22.1.2018); Oxford Dictionary https://en.oxforddictionaries.com/definition/register (22.1.2018).
[37] Considérant 111 du RGPD.

Cette dérogation est envisagée par le droit comme un dernier ressort, car elle ne s'appliquera que «*[l]orsqu'un transfert ne peut pas être fondé sur une disposition de l'article 45 ou 46, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières [...] n'est applicable*»[38].

Cette approche en plusieurs étapes en vue d'envisager le recours aux dérogations comme base des transferts nécessite d'examiner s'il est possible d'utiliser un outil de transfert prévu à l'article 45 ou 46 ou une des dérogations spécifiques définies à l'article 49, paragraphe 1, premier alinéa, avant de recourir à la dérogation de l'article 49, paragraphe 1, deuxième alinéa. Celle-ci ne peut être utilisée que dans les cas résiduels en vertu du considérant 113 et dépend d'un nombre significatif de conditions expressément définies par la législation. Conformément au principe de responsabilité ancré dans le RGPD[39], l'exportateur de données doit donc être en mesure de démontrer qu'il n'était possible ni d'encadrer le transfert de données de garanties appropriées en vertu de l'article 46 ni d'appliquer une des dérogations prévues à l'article 49, paragraphe 1, premier alinéa.

Cela suppose que l'exportateur de données puisse démontrer de sérieux efforts à cet égard, compte tenu des circonstances du transfert de données. Il peut par exemple s'agir, selon le cas, de démontrer qu'il a vérifié si le transfert de données pouvait être effectué sur la base du consentement explicite de la personne concernée en vertu de l'article 49, paragraphe 1, point a). Cependant, dans certaines circonstances, le recours à d'autres outils pourrait ne pas s'avérer possible en pratique. Par exemple, certains types de garanties appropriées en vertu de l'article 46 peuvent ne pas constituer une option réaliste pour un exportateur de données qui est une petite ou moyenne entreprise[40]. Cela peut par exemple aussi être le cas lorsque l'importateur de données a expressément refusé de conclure un contrat de transfert de données sur la base de clauses types de protection des données [article 46, paragraphe 2, point c)] et qu'aucune autre option n'est disponible (y compris, selon le cas, le choix d'un autre «importateur de données») – voir aussi le paragraphe ci-après sur l'intérêt légitime «impérieux».

Intérêt légitime impérieux du responsable du traitement

Selon le libellé de la dérogation, le transfert doit être nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée. La prise en considération des intérêts d'un exportateur de données en sa qualité de sous-traitant ou de l'importateur de données n'est pas pertinente.

De plus, seuls les intérêts qui peuvent être reconnus comme «impérieux» sont pertinents, ce qui limite considérablement le champ d'application de la dérogation, car tous les «intérêts légitimes» concevables en vertu de l'article 6, paragraphe 1, point f), ne s'appliqueront pas ici. À la place, un seuil plus strict s'appliquera, qui exigera que l'intérêt légitime impérieux soit essentiel pour le responsable du traitement. Cela peut par exemple être le cas si le responsable du traitement est tenu de transférer les données à caractère personnel afin de protéger son organisation ou ses systèmes d'un préjudice immédiat grave ou d'une sanction sévère qui affecterait gravement son entreprise.

Non répétitif

[38] Article 49, paragraphe 1, deuxième alinéa, du RGPD.
[39] Article 5, paragraphe 2, et article 24, paragraphe 1.
[40] Par exemple, les règles d'entreprise contraignantes peuvent souvent ne pas constituer une option réalisable pour les petites et moyennes entreprises en raison des investissements administratifs considérables qu'elles impliquent.

Selon sa formulation expresse, l'article 49, paragraphe 1, deuxième alinéa, ne peut s'appliquer qu'à un transfert qui ne revêt pas de caractère répétitif[41].

Nombre limité de personnes concernées

De plus, le transfert ne doit toucher qu'un nombre limité de personnes concernées. Aucun seuil absolu n'a été fixé, car cela dépendra du contexte, mais le nombre doit être suffisamment faible compte tenu du type de transfert en question.

En pratique, la notion de «nombre limité de personnes concernées» dépend du cas en question. Par exemple, si un responsable du traitement doit transférer des données à caractère personnel afin de détecter un incident de sécurité unique et grave pour protéger son organisation, la question serait de savoir de combien d'employés le responsable du traitement devrait transférer les données afin de satisfaire à cet intérêt légitime impérieux.

Par conséquent, pour que la dérogation s'applique, ce transfert ne devrait pas s'appliquer à tous les employés du responsable du traitement mais à quelques-uns d'entre eux seulement.

Mise en balance des «intérêts légitimes impérieux du responsable du traitement» et des «intérêts ou les droits et les libertés de la personne concernée» sur la base d'une évaluation de toutes les circonstances entourant le transfert de données et offrant des garanties appropriées

Une exigence supplémentaire consiste à procéder à une mise en balance de l'intérêt légitime (impérieux) poursuivi par l'exportateur de données et des intérêts ou des droits et libertés de la personne concernée. À cet égard, la législation exige expressément que l'exportateur de données évalue toutes les circonstances du transfert de données en question et, sur la base de cette évaluation, offre des «garanties appropriées» en ce qui concerne la protection des données transférées. Cette exigence met en évidence le rôle particulier que les garanties peuvent jouer en réduisant l'incidence indue du transfert de données sur les personnes concernées et en influençant ainsi peut-être l'équilibre entre les droits et les intérêts dans la mesure où les intérêts du responsable du traitement ne seront pas outrepassés[42].

Quant aux intérêts, aux droits et aux libertés de la personne concernée qui doivent être pris en considération, les effets négatifs possibles, c'est-à-dire les risques du transfert de données pour tout type d'intérêt (légitime) de la personne concernée, doivent être soigneusement prévus et évalués, en prenant en considération leur probabilité et leur gravité[43]. À cet égard, en particulier, tout préjudice possible (physique et matériel, mais aussi moral, comme par exemple une atteinte à la réputation) doit être pris en considération[44]. Au moment d'évaluer ces risques et ce qui pourrait, dans les circonstances données, éventuellement être considéré comme des «garanties appropriées» pour les droits et libertés de la personne concernée, l'exportateur de données doit en particulier tenir compte de la

[41] Pour de plus amples informations sur l'expression «pas de caractère répétitif», voir page 4.
[42] Le rôle important des garanties dans le contexte de la mise en balance des intérêts du responsable du traitement et des personnes concernées a déjà été mis en évidence par le groupe de travail «Article 29» dans le document WP 217, p. 34.
[43] Voir considérant 75: «*Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie […]*».
[44] Voir considérant 75: «*Des risques pour les droits et libertés des personnes physiques, dont le degré de probabilité et de gravité varie, peuvent résulter du traitement de données à caractère personnel qui est susceptible d'entraîner des dommages physiques, matériels ou un préjudice moral*».

nature des données, de la finalité et de la durée du traitement ainsi que de la situation dans le pays d'origine, dans le pays tiers et, le cas échéant, dans le pays de destination finale du transfert[45].

Par ailleurs, la législation exige que l'exportateur de données applique des mesures supplémentaires en guise de garanties afin de réduire au minimum les risques recensés que comporte le transfert de données pour la personne concernée[46]. La législation en a fait une exigence obligatoire afin qu'en l'absence de garanties supplémentaires, les intérêts ou les droits et libertés de la personne concernée priment dans tous les cas les intérêts du responsable du traitement pour le transfert[47]. Quant à la nature de ces garanties, il n'est pas possible de mettre en place des exigences générales applicables à tous les cas à cet égard, et celles-ci dépendront plutôt beaucoup du transfert de données en question. Les garanties peuvent par exemple inclure, selon le cas, des mesures visant à garantir la suppression des données dès que possible après le transfert, ou la limitation des finalités du traitement des données à la suite du transfert. Il convient tout particulièrement de se demander si le transfert de données pseudonymisées ou chiffrées peut suffire[48]. De plus, des mesures techniques et organisationnelles visant à garantir que les données transférées ne peuvent être utilisées à d'autres fins que celles strictement prévues par l'exportateur de données doivent être examinées.

Informations sur l'autorité de contrôle

L'obligation d'informer l'autorité de contrôle ne signifie pas que le transfert doit être autorisé par l'autorité de contrôle, mais plutôt qu'il s'agit là d'une garantie supplémentaire en permettant à l'autorité de contrôle d'évaluer le transfert de données (si elle l'estime opportun) quant à son incidence possible sur les droits et libertés des personnes concernées touchées. Dans le cadre de son obligation de responsabilité, il est recommandé à l'exportateur de données de consigner tous les aspects pertinents du transfert de données, par exemple l'intérêt légitime impérieux poursuivi, les intérêts «contradictoires» de la personne, la nature des données transférées et la finalité du transfert.

Fourniture d'informations sur le transfert et les intérêts légitimes impérieux poursuivis à la personne concernée

Le responsable du traitement doit informer la personne concernée du transfert et des intérêts légitimes impérieux poursuivis. Ces informations doivent être fournies en plus de celles requises en vertu des articles 13 et 14 du RGPD.

[45] Considérant 113.

[46] Si, dans le contexte d'une mise en balance «ordinaire» prévue par la législation, ces mesures (supplémentaires) pourraient ne pas être nécessaires dans chaque cas [voir document du groupe de travail «Article 29» relatif au projet de clauses contractuelles ad hoc «sous-traitant établi dans l'UE à sous-traitant établi hors de l'UE» (WP 214), p. 41], le libellé de l'article 49, paragraphe 1, deuxième alinéa, suggère que les mesures supplémentaires sont obligatoires pour que le transfert de données remplisse le critère de «mise en balance» et soit donc réalisable en vertu de cette dérogation.

[47] Si, dans le contexte d'une mise en balance «ordinaire» prévue par la législation, ces mesures (supplémentaires) pourraient ne pas être nécessaires dans chaque cas [voir avis 06/2014 du groupe de travail «Article 29» sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, WP 217, p. 41], le libellé de l'article 49, paragraphe 1, deuxième alinéa, suggère que les mesures supplémentaires sont obligatoires pour que le transfert de données remplisse le critère de «mise en balance» et soit donc réalisable en vertu de cette dérogation.

[48] Pour d'autres exemples de garanties possibles, voir le document du groupe de travail «Article 29» relatif au projet de clauses contractuelles ad hoc «sous-traitant établi dans l'UE à sous-traitant établi hors de l'UE» (WP 214), p. 41 à 43.

Pour le Comité européen de la protection des données

La présidente

(Andrea Jelinek)

INDEX

(les numéros renvoient aux pages de ce document)

E

F

G

I

L

M

O

P

R

S

T

V

A propos de l'AFCDP

www.afcdp.net

L'AFCDP a été créée dès 2004, dans le contexte de la modification de la Loi Informatique & Libertés qui a officialisé un nouveau métier, celui de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour Correspondant Informatique & Libertés), préfigurateur du Délégué à la protection des données créé par le RGPD.

L'AFCDP est l'association représentative des Délégués à la protection des données (DPD ou DPO pour Data Protection Officer), mais elle rassemble largement. Au-delà des professionnels de la protection des données et des Délégués désignés auprès de la CNIL, elle regroupe toutes les personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside – entre autres – dans la diversité des profils des adhérents : Délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualiticiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Quelques membres de l'AFCDP : 3 Suisses, Accor, Action contre la faim, Adecco, Aéroports de Paris, AG2R La Mondiale, American Hospital of Paris, Assemblée nationale, Association des paralysés de France, Autorité des marchés financiers, AXA, Banque de France, BP France, Carrefour, Caisse nationale des allocations familiales, CHU de Bordeaux, Clermont-Ferrand, Nice, Poitiers et Toulouse, CNES, Communauté Urbaine de Marseille Provence, Conseil Général de Seine-Maritime, CPAM des Bouches du Rhône, Crédit Immobilier de France, Départements de Charente-Maritime, de Corrèze, de Gironde, de la Manche, Ecole Polytechnique, Fédération Nationale des Tiers de Confiance, La Française des Jeux, Gendarmerie Nationale, Orange, IBM France, INRA, Institut Curie, Groupe Casino, Laboratoire Yves Rocher, Legrand, Malakoff Mederic, Michelin, La Poste, Ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche, Monnaie de Paris, Olympique de Marseille, Port autonome de Dunkerque, Randstad, RATP, Région Haute Normandie, Région Lorraine, Sénat, SNCF, Total, Ville de Metz, de Lyon, de Paris, de Saint-Etienne, Venteprivée.com, Vinci Energies, VVF Villages...

Ce document est un guide pratique destiné aux adhérents de l'AFCDP.
Il ne constitue pas une référence légale.

www.afcdp.net

Version 5.2
22 novembre 2018