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.

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) <u>Troisième élément: «finalités et moyens du traitement»</u>

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.

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

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

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

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.

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

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.

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.

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.

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.

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».

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.

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.

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».

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.

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.

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

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.

* * *

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