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

01248/07/FR
WP 136

Avis 4/2007 sur le concept de données à caractère personnel

Adopté le 20 juin

Le groupe de travail a été établi par l'article 29 de la directive 95/46/CE. Il est l'organe consultatif indépendant de l'UE sur la protection des données et de la vie privée. Ses tâches sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.

Le secrétariat est assuré par la Direction C (Justice civile, droits fondamentaux et citoyenneté) de la Direction générale Justice, Liberté et Sécurité, Commission européenne, B-1049 Bruxelles, Belgique, Office No LX-46 01/43.

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

institué en vertu de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995[1],

vu l'article 29, l'article 30, paragraphe 1, point a), et l'article 30, 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 l'article 255 du traité CE et le règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission,

vu son règlement intérieur,

ADOPTE LE PRESENT AVIS :

[1] JO L 281 du 23.11.1995, p. 31, disponible à l'adresse suivante: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

I. INTRODUCTION

Le groupe de travail reconnaît la nécessité de mener une analyse approfondie du concept de données à caractère personnel. Les informations relatives aux pratiques actuelles dans les États membres de l'UE semblent indiquer un certain degré d'incertitude et de diversité dans les pratiques, d'un État membre à l'autre, sur des aspects importants de ce concept, ce qui risque d'affecter le bon fonctionnement du cadre existant en matière de protection des données dans différents contextes. Les résultats de cette analyse d'un élément capital pour l'application et l'interprétation des règles de protection des données auront nécessairement un impact considérable sur un certain nombre de questions importantes, notamment pour certains domaines, tels que la gestion de l'identité dans le contexte de l'administration en ligne («e-government») et des services de télésanté («e-health»), de même que dans le contexte de la technologie RFID (radio-identification).

L'objectif du présent avis adopté par le groupe de travail est de parvenir à une même interprétation du concept de données à caractère personnel, des cas dans lesquels la législation nationale en matière de protection des données devrait s'appliquer, et de ses modalités d'application. Élaborer une définition commune de la notion de données à caractère personnel revient à définir ce qui relève ou non du champ d'application des règles nationales de protection des données. Le corollaire de ce travail est de fournir des orientations sur les modalités d'application des règles de protection des données à certaines catégories de situations qui se présentent à l'échelle européenne, afin de

contribuer à l'application uniforme de ces normes, une mission essentielle du groupe de travail «article 29».

Des exemples tirés des pratiques nationales des autorités européennes de protection des données serviront à étayer et illustrer la présente analyse. La plupart de ces exemples n'ont été modifiés qu'aux seules fins de les rendre exploitables dans ce contexte.

II. GÉNÉRALITÉS ET QUESTIONS POLITIQUES

La directive définit largement le concept de données à caractère personnel

La définition des données à caractère personnel figurant dans la directive 95/46/CE (ci-après «la directive sur la protection des données» ou «la directive») est ainsi libellée:

«*données à caractère personnel*»: *toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*».

Il convient de relever que cette définition reflète la volonté du législateur européen de définir largement le concept de «données à caractère personnel» et ce, tout au long du processus législatif. La proposition initiale de la Commission indiquait que «*comme dans la Convention 108, une définition large est adoptée afin de couvrir toutes les informations qui peuvent être reliées à une personne*»[2]. Dans la proposition modifiée de la Commission, il était précisé que «*la proposition modifiée donne satisfaction à l'objectif du Parlement qui est d'adopter la définition la plus globale possible de la notion de «donnée à caractère personnel», afin de couvrir toutes les informations qui peuvent être reliées à une personne physique*»[3], un objectif également pris en considération par le Conseil dans la position commune[4].

Les règles contenues dans la directive visent à protéger les personnes physiques.

Les articles 1er des directives 95/46/CE et 2002/58/CE mentionnent clairement que la finalité ultime de ces règles est de protéger les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, à l'égard du traitement des données à caractère personnel. C'est un élément très important à prendre en compte dans l'interprétation et l'application des règles de ces deux instruments. Il peut jouer un rôle déterminant dans la définition des modalités d'application des dispositions de la directive dans certaines situations où les droits des personnes physiques ne sont pas menacés, et mettre en garde contre toute interprétation des mêmes règles qui pourrait priver les personnes physiques de la protection de leurs droits.

Le champ d'application de la directive exclut un certain nombre d'activités, et le texte se caractérise par une grande souplesse permettant d'apporter une solution juridique appropriée aux circonstances en jeu.

---

2 COM(90) 314 final, 13.9.1990, p. 19 (commentaire relatif à l'article 2).
3 COM(92) 422 final, 28.10.1992, p. 10 (commentaire relatif à l'article 2).
4 Position commune (CE) nº 1/95 arrêtée par le Conseil le 20 février 1995, JO C 93 du 13.4.1995, p. 20.

En dépit du concept large de «données à caractère personnel» et de «traitement» contenu dans la directive, le simple fait qu'une situation donnée soit reconnue comme impliquant «le traitement de données à caractère personnel» au sens de la définition ne préjuge pas, à lui seul, de l'application des règles de la directive dans cette situation précise, notamment en vertu de son article 3. À part les dérogations tenant au champ d'application du droit communautaire, les dérogations au titre de l'article 3 prennent en compte la technique de traitement utilisé (traitement manuel non structuré) et la finalité de l'utilisation (activités exclusivement personnelles ou domestiques d'une personne physique). Même en cas de traitement des données à caractère personnel relevant du champ d'application de la directive, toutes ses dispositions ne s'appliquent pas nécessairement au cas d'espèce. Un certain nombre de dispositions prévues par la directive laissent une souplesse considérable afin de parvenir à un juste équilibre entre, d'une part, la protection des droits de la personne concernée, et d'autre part, les intérêts légitimes des responsables du traitement des données, des tiers et l'intérêt public éventuel. Des exemples de ces dispositions se trouvent à l'article 6 (conservation de données pendant la durée nécessaire), à l'article 7, point f) (mise en balance des intérêts pour justifier le traitement), au dernier paragraphe de l'article 10, point c) et à l'article 11, paragraphe 1, point c), (le cas échéant, notification de la personne concernée afin de garantir un traitement loyal), à l'article 18 (dérogations à l'obligation de notification), pour n'en citer que quelques-uns.

Le champ d'application des règles de protection des données ne doit pas être trop étendu

Il n'est pas souhaitable que les règles de protection des données s'appliquent en définitive à des situations qui n'étaient pas destinées à être couvertes par ces règles et pour lesquelles le législateur ne les a pas conçues. Les dérogations importantes de l'article 3 évoquées plus haut et les explications des considérants 26 et 27 de la directive montrent comment le législateur entendait faire appliquer la protection des données.

L'une des restrictions concerne le type de traitement des données. À cet égard, il n'est pas inutile de rappeler que la promulgation des premières lois sur la protection des données dans les années 70 est due aux nouvelles technologies de traitement électronique des données, qui permettaient un accès plus facile et plus étendu aux données à caractère personnel que les formes traditionnelles de traitement des données. Par conséquent, la protection des données dans le cadre de la directive vise à protéger les formes de traitement présentant généralement un risque accru d'«accès facile aux données à caractère personnel» (considérant 27). Le traitement non automatisé de données à caractère personnel n'entre dans le champ d'application de la directive que dans la mesure où les données sont contenues ou appelées à figurer dans un fichier (article 3).

Le traitement des données dans les cas où les moyens permettant d'identifier la personne concernée ne sont pas «susceptibles d'être raisonnablement mis en œuvre» (considérant 26) constitue une autre restriction générale à l'application de la protection des données au sens de la directive: cette question sera examinée plus loin.

Il faut également éviter de restreindre indûment l'interprétation du concept de données à caractère personnel.

Pour les cas où une application mécanique de chacune des dispositions de la directive s'avérerait, a priori, extrêmement fastidieuse ou conduirait même à des situations absurdes, il convient de vérifier tout d'abord 1) si la situation entre dans le champ d'application de la directive, notamment en vertu de son article 3; et 2) dans le cas où elle entre dans son champ d'application, si la directive elle-même ou la législation nationale de transposition ne prévoit pas de dérogations ou de simplifications dans des situations particulières, afin d'apporter une réponse juridique appropriée, tout en assurant la protection des droits des personnes physiques et des intérêts en jeu. Il est préférable de ne pas restreindre indûment l'interprétation de la définition des données à caractère personnel, mais plutôt de prendre en compte la souplesse considérable existant dans l'application de ces règles aux données.

À cet égard, les autorités nationales de contrôle en matière de protection des données jouent un rôle essentiel dans le cadre de leur mission de contrôle de l'application de la législation en matière de protection des données, qui consiste entre autres à donner une interprétation des dispositions légales et des orientations concrètes aux responsables du traitement et aux personnes concernées. Il importe qu'elles approuvent une définition qui soit assez large pour anticiper les évolutions et incorporer toutes les «zones d'ombre» dans son champ d'application, tout en faisant légitimement usage de la souplesse qu'offre la directive. En réalité, le texte de la directive invite à élaborer une politique alliant une interprétation large de la notion de données à caractère personnel et un juste équilibre dans l'application des règles de la directive.

III. ANALYSE DE LA DÉFINITION DES «DONNÉES À CARACTÈRE PERSONNEL» AU SENS DE LA DIRECTIVE SUR LA PROTECTION DES DONNÉES

Cette définition repose sur quatre grands éléments constitutifs, qui seront analysés tour à tour aux fins du présent document:

- «toute information»
- «concernant»
- «une personne physique»
- «identifiée ou identifiable»

Ces quatre éléments constitutifs sont étroitement liés et interdépendants. Toutefois, pour respecter la méthodologie à suivre dans le présent document, chacun de ces éléments sera traité séparément.

1. PREMIER ÉLÉMENT: «TOUTE INFORMATION»

L'expression «toute information» que l'on retrouve dans la définition de la directive manifeste clairement la volonté du législateur d'élaborer un concept large des données à caractère personnel. Ce libellé appelle une interprétation large.

Du point de vue de la nature des informations, le concept de données à caractère personnel englobe toutes sortes de renseignements à propos d'une personne. Il peut s'agir d'informations «objectives» telles qu'une particularité sanguine de la personne concernée, comme il peut aussi s'agir d'informations «subjectives» sous forme d'avis ou d'appréciations. Ce dernier type de renseignements représente un grande partie du traitement des données à caractère personnel dans des secteurs tels que celui des banques, pour l'évaluation de la fiabilité des emprunteurs («X est un emprunteur fiable»), des assurances («X ne devrait pas mourir dans un proche avenir») ou de l'emploi («X est un bon travailleur et mérite d'être promu»).

Pour être considérées comme des «données à caractère personnel», il n'est pas nécessaire que ces informations soient vraies ou prouvées. En réalité, les règles de protection des données envisagent déjà que des informations puissent être incorrectes et prévoient pour la personne concernée le droit d'accéder à ces informations et de les contester par des voies de recours adéquates[5].

Du point de vue du contenu des informations, on entend par «données à caractère personnel» toutes sortes d'informations. Cela couvre évidemment les informations à caractère personnel considérées comme «données sensibles», au sens de l'article 8 de la directive, en raison du fort potentiel de risque qu'elles présentent, mais également des informations plus générales. L'expression «données à caractère personnel» englobe les informations touchant à la vie privée et familiale d'une personne physique, stricto sensu, mais également les informations relatives à ses activités, quelles qu'elles soient, tout comme celles concernant ses relations de travail ainsi que son comportement économique ou social. Il s'agit donc d'informations concernant des personnes physiques, indépendamment de leur situation ou de leur qualité (en tant que consommateurs, patients, employés, clients, etc.).

Exemple n° 1 − Habitudes et pratiques professionnelles

Les informations se rapportant à des ordonnances de médicaments (par exemple numéro d'identification du médicament, nom du médicament, dosage du médicament, fabricant, prix de vente, nouveau ou renouvellement, raisons de l'utilisation, raisons du non-remplacement, prénom et nom du prescripteur, numéro de téléphone, etc.), que ce soit sous forme d'ordonnances individuelles ou sous forme de tendances dégagées d'un certain nombre d'ordonnances, peuvent être considérées comme des données à caractère personnel concernant le médecin qui prescrit ce médicament, même si le patient reste anonyme. Ainsi, la fourniture d'informations concernant des ordonnances rédigées par des médecins identifiés ou identifiables à des fabricants de médicaments soumis à ordonnance constitue une communication de données à caractère personnel à des tiers destinataires au sens de la directive.

Cette interprétation est corroborée par le libellé de la directive elle-même. D'un côté, il convient de considérer que le concept de vie privée et familiale est large, comme l'a précisé la Cour européenne des droits de l'homme[6]. De l'autre, les règles de protection

[5] On peut envisager de les rectifier en ajoutant des commentaires a contrario ou en recourant aux voies de droit appropriées comme les mécanismes de recours.

[6] Arrêt de la Cour européenne des droits de l'homme dans l'affaire Amann/Suisse, rendu le 16.2.2000, point 65: *«[…]le terme «vie privée» ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de «vie privée» (arrêts Niemietz/Allemagne du 16 décembre 1992,*

des données à caractère personnel vont au-delà de la protection du concept général du droit au respect de la vie privée et familiale. À noter que la Charte des droits fondamentaux de l'Union européenne consacre la protection des données à caractère personnel dans son article 8 comme un droit autonome, séparé et différent du respect de la vie privée visé à l'article 7 de ladite charte, comme c'est d'ailleurs le cas au niveau national dans certains États membres. Cette interprétation est conforme aux dispositions de l'article 1er, paragraphe 1, qui visent à assurer la protection «des libertés et droits fondamentaux des personnes physiques, notamment [mais pas exclusivement] de leur vie privée». En conséquence, la directive se réfère spécifiquement au traitement des données à caractère personnel en dehors du contexte domestique ou familial, comme celui prévu par le droit du travail (article 8, paragraphe 2, point b)), pour les condamnations pénales, les sanctions administratives ou les jugements civils (article 8, paragraphe 5) ou en matière de prospection (article 14, point b)). La Cour de justice des Communes européennes[7] a approuvé cette approche générale.

S'agissant du format des informations ou du support utilisé pour celles-ci, le concept de données à caractère personnel englobe les informations disponibles sous n'importe quelle forme, qu'elles soient alphabétiques, numériques, graphiques, photographiques ou acoustiques. Sont par exemple concernées les informations conservées sur papier, tout comme les informations stockées dans une mémoire d'ordinateur (code binaire) ou sur une cassette vidéo. C'est une conséquence logique de l'intégration du traitement automatisé des données à caractère personnel dans son champ d'application. Il apparaît en particulier que les données constituées par des sons et des images méritent, à ce titre, d'être reconnues comme des données à caractère personnel, dans la mesure où elles peuvent représenter des informations sur une personne physique. À cet égard, la référence spécifique aux données constituées par des sons et des images, à l'article 33 de la directive, doit être interprétée comme confirmant et précisant que ce type de données relève effectivement de son champ d'application (à condition que l'ensemble des autres conditions soient remplies), et que la directive s'applique à ces données. En réalité, il s'agit là d'une hypothèse logique concernant la disposition contenue dans ledit article dont l'objectif est d'évaluer si les règles énoncées par la directive apportent des solutions juridiques appropriées dans ces domaines. Cet objectif est également spécifié au considérant 14 qui énonce que «*compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données*». Par ailleurs, il n'est pas nécessaire, pour que ces informations soient considérées comme données à caractère personnel, qu'elles soient contenues dans une base de données ou un fichier structurés. Les informations contenues sous forme de texte libre dans un document électronique peuvent également être reconnues comme des données à

---

série A n° 251-B, pp. 33-34, § 29 et Halford précité, pp. 1015-1016, § 42). Cette interprétation extensive concorde avec celle de la Convention élaborée au sein du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 […]».

7 Arrêt de la Cour du 6 novembre 2003 dans l'affaire C-101/2001 (Lindqvist): «*La notion de «données à caractère personnel» employée à l'article 3, paragraphe 1, de la directive 95/46 englobe, conformément à la définition figurant à l'article 2, sous a), de celle-ci, «toute information concernant une personne physique identifiée ou identifiable». Cette notion comprend assurément le nom d'une personne joint à ses coordonnées téléphoniques ou à des informations relatives à ses conditions de travail ou à ses passe-temps*» (point 24).

caractère personnel, pour autant que les autres critères énoncés dans la définition des données à caractère personnel soient remplis. Les courriers électroniques contiennent par exemple des «données à caractère personnel».

Exemple n° 2 − Services bancaires par téléphone

En qui concerne les services bancaires par téléphone, où la voix du client qui donne des instructions à la banque est enregistrée, il y a lieu de considérer ces instructions enregistrées comme des données à caractère personnel.

Exemple n° 3 − Vidéosurveillance

Les images de personnes physiques captées par un système de vidéosurveillance peuvent être considérées comme des données à caractère personnel, pour autant que les individus soient reconnaissables.

Exemple n° 4 − Le dessin d'un enfant

À la suite d'un test neuropsychiatrique pratiqué sur une fillette dans le contexte d'une procédure judiciaire concernant sa garde, celle-ci fait un dessin représentant sa famille. Ce dessin fournit des informations sur l'état d'esprit de la fillette et ses sentiments envers différents membres de sa famille. Ces informations pourraient, en soi, être considérées comme des «informations à caractère personnel». Ce dessin révèle, en effet, des informations concernant cet enfant (sa santé mentale), mais aussi le comportement de son père ou de sa mère par exemple. En conséquence, les parents peuvent dans ce cas user de leur droit d'accéder à cet élément d'information spécifique.

À cet égard, les données biométriques méritent une référence particulière. Ces données peuvent se définir comme des propriétés biologiques, des caractéristiques physiologiques, des caractéristiques vivantes ou des actions reproductibles lorsque ces caractéristiques et/ou actions sont à la fois propres à cette personne physique et mesurables, même si les méthodes utilisées dans la pratique pour les mesurer techniquement impliquent un certain degré de probabilité. Parmi les exemples caractéristiques de ces données biométriques figurent les empreintes digitales, la structure de la rétine, la structure faciale, la voix, mais aussi la forme des mains, le système veineux, voire des caractéristiques profondément ancrées ou d'autres caractéristiques comportementales (signature manuscrite, dynamique de frappe sur un clavier, démarche ou élocution particulières, etc.)

Ce qui caractérise, entre autres, les données biométriques, c'est qu'elles peuvent être considérées comme *contenu* des informations concernant une personne physique donnée (X a ces empreintes digitales) ainsi que comme élément permettant d'établir un *lien* entre une information et une personne physique (cet objet a été touché par quelqu'un qui présente ces empreintes digitales et celles-ci correspondent à X; par conséquent, X a touché l'objet). Elles peuvent ainsi servir d'«identificateurs». En effet, en raison du lien unique qui les relie à une personne physique spécifique, les données biométriques peuvent être utilisées pour identifier la personne physique. Cette dualité apparaît également dans le cas des données ADN qui fournissent des informations sur le corps humain et qui permettent l'identification spécifique et sans ambiguïté d'une personne.

Les prélèvements de tissus humains (comme les prélèvements de sang), bien que n'étant pas des données biométriques en soi (la structure des empreintes digitales est une donnée biométrique, alors que le doigt en lui-même n'en est pas une), sont des sources d'informations dont on peut extraire des données biométriques. Il ressort de ce qui précède que l'extraction d'informations à partir de prélèvements est assimilée à une collecte de données à caractère personnel soumises aux règles de la directive. La collecte, la conservation et l'utilisation de prélèvements de tissus peuvent elles-mêmes être soumises à diverses séries de règles[8].

2. DEUXIÈME ÉLÉMENT: «CONCERNANT»

Cet élément constitutif de la définition est crucial, dans la mesure où il est très important de déterminer avec précision les relations/liens qui importent et de pouvoir les distinguer.

D'une manière générale, on peut considérer que les informations «concernent» une personne physique, lorsqu'elles ont *trait* à cette personne physique.

Dans nombre de situations, ce lien est facile à établir. Par exemple, dans le cas de données enregistrées dans le dossier personnel d'un employé dans un service du personnel, il s'agit clairement de données «concernant» la situation de la personne en sa qualité d'employé. Il en va de même des données relatives aux résultats de l'examen médical d'un patient dans son dossier médical, ou de l'image d'une personne filmée sur une vidéo lors d'une interview.

On peut citer un certain nombre d'autres situations où il n'est pas toujours aussi évident que dans les cas précédents de déterminer que les informations «concernent» une personne physique.

Dans certaines situations, les informations découlant des données concernent en premier lieu des objets, et non des personnes. Ces objets appartiennent en général à quelqu'un, ou peuvent subir l'influence particulière de personnes ou exercer une influence particulière sur des personnes ou se trouver d'une manière ou d'une autre à proximité physique ou géographique de personnes ou d'autres objets. Ce n'est donc que de manière indirecte que l'on pourra considérer que ces informations concernent ces personnes ou ces objets.

Exemple n° 5 − La valeur d'une maison

La valeur d'une maison constitue un élément d'information sur un objet. À l'évidence, les règles de protection des données ne s'appliquent pas si cet élément d'information n'est utilisé que pour illustrer le niveau des prix de l'immobilier dans un certain quartier. Toutefois, dans certaines circonstances, ces informations méritent également d'être considérées comme des données à caractère personnel. En effet, une maison constitue le patrimoine d'un propriétaire, qui servira, par exemple, à déterminer si cette personne est imposable à ce titre. Dans ce contexte, il est incontestable que ces informations doivent relever de la catégorie des données à caractère personnel.

Ce principe vaut également pour les données concernant en premier lieu des processus ou des événements, par exemple des informations sur le fonctionnement d'une machine

[8] Voir recommandation du 15.3.2006 du Conseil de l'Europe (Rec. (2006) 4) du Comité des ministres aux États membres sur la recherche utilisant du matériel biologique d'origine humaine.

nécessitant une intervention humaine. Il est, dès lors, possible de considérer ce type d'informations comme «concernant» une personne physique.

Exemple n° 6 − Service entretien/réparation automobile

Le registre entretien/réparation tenu par un mécanicien ou un garage contient des informations sur le véhicule, le kilométrage, les dates des entretiens effectués, les problèmes techniques et son état matériel. Ces informations sont associées dans le dossier à une plaque minéralogique et à un numéro de moteur, que l'on peut rattacher, à leur tour, au propriétaire. Lorsque le garage établit un lien entre le véhicule et le propriétaire, aux fins de la facturation, ces informations «concernent» le propriétaire ou le conducteur. Si le lien est établi avec le mécanicien qui s'est occupé de la voiture, aux fins de l'évaluation de sa productivité, ces informations «concernent» également le mécanicien.

Le groupe de travail s'est déjà penché sur la question de savoir dans quelles circonstances on peut considérer ces informations comme «concernant» une personne. Dans le contexte de l'examen des questions de protection des données soulevées par les marqueurs RFID, le groupe de travail relève que: «*les données concernent une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée*»[9].

Vu les cas évoqués ci-dessus, et dans le même ordre d'idées, il convient de souligner que pour considérer que les données «concernent» une personne physique, la présence d'un élément de **«contenu»** OU de **«finalité»** OU de «**résultat**» est indispensable.

L'élément de **«contenu»** est présent lorsque − conformément à la perception la plus évidente et la plus commune dans une société du mot «concerner» − des informations ayant trait à une personne particulière sont communiquées, indépendamment de toute finalité de la part du responsable du traitement des données ou du tiers, ou de l'impact de ces informations sur la personne concernée. Les informations «concernent» une personne lorsqu'elles ont «trait» à cette personne, et une évaluation s'impose à la lumière de l'ensemble des circonstances du cas d'espèce. Par exemple, les résultats d'une analyse médicale concernent manifestement le patient, tout comme les informations contenues dans le dossier au nom d'un certain client concernent celui-ci. De la même façon, les informations contenues dans des marqueurs RFID ou des codes-barres intégrés dans le document d'identité d'une personne donnée concernent cette personne, comme cela sera le cas dans les futurs passeports qui seront dotés d'une puce RFID.

L'élément de **«finalité»** peut lui aussi jouer un rôle pour déterminer si des informations «concernent» une certaine personne. Cet élément de «finalité» sera considéré comme présent lorsque les données sont utilisées ou susceptibles d'être utilisées, compte tenu de l'ensemble des circonstances du cas d'espèce, afin d'évaluer, de traiter d'une certaine manière ou d'influer sur le statut ou le comportement d'une personne physique.

[9] Document de travail du groupe de travail n° WP 105: «Document de travail sur les questions de protection des données liées à la technologie RFID», adopté le 19.1.2005, p. 9.

Exemple n° 7 − Historique des appels d'un poste téléphonique

L'historique des appels d'un poste téléphonique au sein d'une entreprise fournit des informations sur les appels effectués à partir de cet appareil connecté à une certaine ligne. Ces informations peuvent être rattachées à différents sujets. D'une part, la ligne est mise à la disposition de l'entreprise qui, en contrepartie, s'engage à payer les appels effectués dans ce cadre. L'appareil téléphonique est utilisé par un employé pendant les heures de travail et on part du principe qu'il est l'auteur des appels effectués. L'historique des appels peut également fournir des informations sur la personne appelée. Ce poste téléphonique peut également être utilisé par toute autre personne autorisée à pénétrer dans les locaux en l'absence de l'employé (par exemple le personnel de nettoyage). À des fins diverses, les informations sur l'utilisation de cet appareil peuvent concerner l'entreprise, l'employé ou le personnel de nettoyage (par exemple pour vérifier l'heure à laquelle le personnel de nettoyage quitte son lieu de travail, puisqu'il est censé confirmer par téléphone l'heure à laquelle il quitte les locaux avant de les fermer à clé). À noter qu'en l'occurrence le concept de données à caractère personnel s'étend à la fois aux appels sortants et aux appels entrants, dans la mesure où tous les appels contiennent des informations concernant la vie privée, les relations sociales et les communications des personnes concernées.

Un troisième type de lien avec des personnes spécifiques intervient lorsque l'on se trouve en présence d'un élément de **«résultat»**. Même en l'absence de tout élément de «contenu» ou de «finalité», on peut considérer que des données «concernent» une personne physique lorsque leur utilisation est susceptible d'avoir un impact sur certains des droits et intérêts d'une personne, compte tenu de l'ensemble des circonstances du cas d'espèce. Il convient de relever qu'il n'est pas nécessaire que le résultat potentiel ait un impact majeur. Il suffit qu'une personne physique puisse être traitée différemment par rapport à d'autres personnes à la suite du traitement de ces données.

Exemple n° 8 − Impact sur les conducteurs du contrôle de la position des taxis pour optimiser le service

Une compagnie de taxis met en place un système de localisation par satellite permettant de localiser les taxis disponibles en temps réel. La finalité du traitement est d'offrir un meilleur service et d'économiser du carburant, en attribuant à chaque client qui commande un taxi le véhicule le plus proche de l'adresse du client. À proprement parler, les données nécessaires au fonctionnement de ce système sont des données concernant les véhicules, et non pas les conducteurs. La finalité du traitement n'est pas d'évaluer les performances des chauffeurs de taxi, par exemple en optimisant leurs itinéraires. Toujours est-il que ce système permet de contrôler les performances des chauffeurs de taxis et de contrôler s'ils respectent les limitations de vitesse, choisissent les itinéraires appropriés, sont au volant ou se reposent hors du véhicule, etc. Dès lors, ce système peut avoir un impact considérable sur ces personnes, et on peut considérer que ces données en tant que telles concernent également des personnes physiques. Leur traitement doit donc être soumis aux règles de protection des données.

Ces trois éléments (contenu, finalité, résultat) sont à considérer comme des conditions alternatives, et non cumulatives. Lorsque l'élément de contenu est présent, il n'est pas nécessaire que les autres éléments le soient pour considérer que ces informations concernent la personne. Le corollaire de ce constat est que la même information peut

concerner simultanément différentes personnes, selon l'élément en présence pour chacune d'entre elles. Les mêmes informations peuvent concerner X en raison de l'élément de «contenu» (les données ont manifestement trait à X), ET Y en raison de l'élément de «finalité» (elles sont utilisés afin de traiter Y d'une certaine manière) ET Z en raison de l'élément de «résultat» (elles sont susceptibles d'avoir un impact sur les droits et intérêts de Z). Cela signifie qu'il n'est pas nécessaire que les données «soient axées» sur une personne pour considérer qu'elles la concernent. Il découle de l'analyse précédente qu'il est indispensable de vérifier, pour chaque donnée spécifique, sur la base de ses qualités intrinsèques, si elle concerne une personne donnée. De la même façon, le fait que des informations puissent concerner différentes personnes doit être pris en considération dans l'application de dispositions de fond (par exemple concernant l'étendue du droit d'accès).

Exemple n° 9 − Informations contenues dans le procès-verbal d'une réunion

Un exemple de la nécessité de se prêter à l'analyse précédente pour chaque information séparément est fourni par les informations contenues dans le procès-verbal d'une réunion, qui fait généralement état de la présence des participants X, Y et Z, des interventions effectuées par X et Y et d'un compte rendu des travaux sur certains thèmes tels que résumés par l'auteur du procès-verbal, à savoir Z. S'agissant des données à caractère personnel concernant X, les seules informations à considérer à ce titre sont sa présence à la réunion à une certaine heure, en un certain lieu, et ses interventions. La présence d'Y à cette réunion, ses interventions et les travaux sur une question telle que résumée par Z NE sont PAS des données à caractère personnel concernant X. Et ce, même si ces informations figurent dans le même document, et même si c'est X qui a lancé la question à discuter lors de la réunion. Ces informations sont donc exclues du droit d'accès de X à ses propres données à caractère personnel. Quant à savoir si ces informations peuvent être considérées comme des données à caractère personnel d'Y et de Z et dans quelle mesure, il conviendra de le déterminer séparément en les soumettant à l'analyse décrite ci-dessus.

3. TROISIÈME ÉLÉMENT: [PERSONNE PHYSIQUE] «IDENTIFIÉE OU IDENTIFIABLE»

La directive exige que les informations concernent une personne physique «identifiée ou identifiable». Ce principe appelle les considérations qui suivent.

D'une manière générale, on peut considérer une personne physique comme «identifiée» lorsque, au sein d'un groupe de personnes, elle se «distingue» de tous les autres membres de ce groupe. La personne physique est donc «identifiable» lorsque, même sans avoir encore été identifiée, il est possible de le faire (comme l'exprime le suffixe «-able»). Cette seconde option constitue donc en pratique la condition de base qui détermine si les informations entrent dans le champ d'application du troisième élément.

L'identification se fait normalement au moyen d'informations spécifiques que l'on peut appeler «identifiants» et qui présentent une relation particulièrement privilégiée et étroite avec la personne physique concernée. Il peut s'agir, par exemple, de signes extérieurs concernant l'apparence de cette personne comme sa taille, la couleur de ses cheveux, ses vêtements, etc. ou d'une caractéristique de cette personne qui n'est pas immédiatement perceptible, comme une profession, une fonction, un nom, etc. La directive fait référence à ces «identifiants» dans la définition des «données à caractère personnel» visée à l'article 2, qui énonce qu'une personne physique «*peut être*

identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale».

Identifiable «directement» ou «indirectement»

De plus amples explications se trouvent dans le commentaire sur les articles de la proposition modifiée de la Commission, en ce sens qu'il y est précisé qu'«*une personne peut être identifiée soit directement par un nom soit indirectement par un numéro de téléphone, de voiture, de sécurité sociale, de passeport ou par un croisement de critères significatifs, permettant de la reconnaître à l'intérieur d'un petit groupe par exemple (âge, fonction occupée, adresse, etc.)*». Ce libellé montre clairement que c'est le contexte du cas d'espèce qui déterminera si certains identifiants sont suffisants pour permettre l'identification. Un nom de famille très courant sera insuffisant pour identifier quelqu'un − c'est-à-dire pour distinguer quelqu'un − dans l'ensemble de la population d'un pays, alors qu'il sera probablement suffisant pour identifier un élève dans une classe. Même des informations accessoires, comme «l'homme portant un costume noir» peuvent permettre d'identifier une personne parmi les passants se trouvant près de feux de signalisation. Ainsi, la question de savoir si une personne à laquelle se rapportent les informations est identifiée ou pas dépend des circonstances du cas d'espèce.

S'agissant des personnes «directement» identifiées ou identifiables, le **nom** de la personne est évidemment l'identifiant le plus courant et, dans la pratique, la notion de «personne identifiée» implique le plus souvent une référence au nom de cette personne.

Afin de s'assurer de son identité, le nom de la personne doit parfois être associé à d'autres éléments d'information (date de naissance, nom des parents, adresse ou photo d'identité) afin d'éviter toute confusion entre cette personne et d'éventuels homonymes. À titre d'exemple, l'information selon laquelle X est redevable d'une certaine somme d'argent peut être considérée comme concernant une personne identifiée, car elle est liée au nom de cette personne. Le nom est un élément d'information qui révèle que la personne utilise cette combinaison de lettres et de sons pour se distinguer d'autres personnes et être distinguée par d'autres personnes avec lesquelles elle établit des relations. Le nom peut également être le point de départ conduisant à des informations sur le domicile de la personne ou l'endroit où elle se trouve et à des informations sur les membres de sa famille (par le biais du nom de famille) et sur différentes relations juridiques et sociales associées à ce nom (scolarité/études, dossier médical, comptes bancaires). Il est même possible de connaître l'apparence d'une personne si sa photographie est associée à ce nom. Tous ces nouveaux éléments d'information liés au nom peuvent permettre à quelqu'un de «zoomer» sur la personne en chair et en os, et grâce aux identifiants, l'élément d'information initial est alors associé à une personne physique que l'on peut distinguer d'autres personnes.

S'agissant des personnes «indirectement» identifiées ou identifiables, cette catégorie relève en général du phénomène des «combinaisons uniques», à quelque degré que ce soit. Pour les cas où, de prime abord, les identifiants sont insuffisants pour permettre à quiconque de distinguer une personne particulière, cette personne peut néanmoins être «identifiable», car ces informations combinées à d'autres éléments d'information (que ces derniers soient conservés par le responsable du traitement ou non) permettent de la distinguer parmi d'autres personnes. C'est pourquoi la directive précise «un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique,

psychique, économique, culturelle ou sociale». Certaines caractéristiques, de par leur spécificité, permettent d'identifier quelqu'un sans difficulté («actuel premier ministre espagnol»), mais une combinaison de détails à un niveau catégoriel (tranche d'âge, origine régionale, etc.) peut également s'avérer assez concluante dans certaines circonstances, notamment si l'on a accès à des informations supplémentaires. Ce phénomène a été étudié de manière approfondie par les statisticiens toujours soucieux de ne pas commettre de violation de la confidentialité.

Exemple n° 10 − Informations fragmentaires dans la presse

Des informations sont publiées sur une ancienne affaire pénale qui, à l'époque, avait suscité un grand intérêt du public. Dans la publication en question, aucun identifiant habituel n'est utilisé, en particulier aucune mention du nom ni de la date de naissance des personnes impliquées dans l'affaire.

Il ne semble pas particulièrement difficile d'obtenir des informations supplémentaires permettant de retrouver les principales personnes concernées, par exemple en consultant les journaux parus lors de la période concernée. En effet, on peut supposer qu'il y a une certaine probabilité que quelqu'un puisse effectuer ce genre de démarches (comme de consulter d'anciens journaux) qui permettraient vraisemblablement d'obtenir les noms et d'autres identifiants concernant les personnes évoquées dans cet exemple. Il semble donc justifié de considérer les informations de l'exemple cité comme des «informations concernant les personnes identifiables» qui entrent donc dans la catégorie des «données à caractère personnel».

À cet égard, il convient de relever que si l'identification par le nom constitue, dans la pratique, le moyen le plus répandu, un nom n'est pas toujours nécessaire pour identifier une personne, notamment lorsque d'autres «identifiants» sont utilisés pour distinguer quelqu'un. En effet, les fichiers informatiques enregistrant les données à caractère personnel attribuent habituellement un identifiant spécifique aux personnes enregistrées pour éviter toute confusion entre deux personnes se trouvant dans un même fichier. Sur l'internet aussi, les outils de surveillance du trafic permettent de cerner facilement le comportement d'une machine et, derrière celle-ci, de son utilisateur. On reconstitue ainsi la personnalité de l'individu pour lui attribuer certaines décisions. Sans même s'enquérir du nom et de l'adresse de la personne, on peut la caractériser en fonction de critères socio-économiques, psychologiques, philosophiques ou autres et lui attribuer certaines décisions dans la mesure où le point de contact de la personne (l'ordinateur) ne nécessite plus nécessairement la révélation de son identité au sens étroit du terme. En d'autres termes, la possibilité d'identifier une personne n'implique plus nécessairement la faculté de connaître son identité. La définition des données à caractère personnel reflète ce constat[10].

La Cour de justice des Communautés européennes a statué dans ce sens, considérant que la «*l'opération consistant à faire référence, sur une page Internet, à diverses personnes et à les identifier soit par leur nom, soit par d'autres moyens, par exemple leur numéro de téléphone ou des informations* ***relatives à*** *leurs conditions de travail et*

[10] Poullet Y. et son équipe, «Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications», Conseil de l'Europe, Comité consultatif T-PD, point 2.3.1, T-PD (2004) 04 final.

à leurs passe-temps, constitue un «traitement de données à caractère personnel […]» au sens […] de la directive 95/46»[11].

Exemple n° 11 − Demandeurs d'asile

À des fins administratives, on a attribué dans un foyer d'accueil un numéro de code à des demandeurs d'asile qui cachent leur véritable nom. Ce numéro sert d'identifiant, de sorte que différents éléments d'information concernant le séjour du demandeur d'asile dans le foyer lui seront attribués, et au moyen d'une photographie et d'autres indicateurs biométriques, il y aura un lien étroit et direct entre ce numéro de code et cette personne physique, permettant de la distinguer des autres demandeurs d'asile et de lui attribuer différents éléments d'information se référant alors à une personne physique «identifiée».

L'article 8, paragraphe 7, prévoit également que: «les États membres déterminent les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement.» Il est utile de relever le sens de cette disposition, qui ne contient aucune indication particulière quant à la nature des conditions que les États membres sont censés adopter, bien qu'elle figure dans l'article consacré aux données sensibles. Le considérant 33 qualifie ces données de «*données qui sont susceptibles, de par leur nature, de porter atteinte aux libertés fondamentales ou à la vie privée*». On peut raisonnablement penser que le législateur a éprouvé les mêmes inquiétudes concernant les numéros d'identification nationaux en raison des fortes probabilités d'établir facilement et clairement un lien avec différents éléments d'information sur une personne donnée.

Moyens d'identification

Le considérant 26 de la directive accorde une attention particulière au terme «identifiable», en énonçant que «*pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne*». Cela signifie que la simple possibilité hypothétique de distinguer une personne n'est pas suffisante pour considérer cette personne comme «identifiable». Si, compte tenu de «*l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne*», cette possibilité n'existe pas ou qu'elle est négligeable, la personne ne saurait être considérée comme «identifiable» et les informations ne seraient pas des «données à caractère personnel». Le critère de «*l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne*» doit notamment prendre en compte tous les facteurs en jeu. Les coûts engendrés par l'identification constituent un facteur, mais pas le seul. La finalité visée, la manière dont le traitement est structuré, l'intérêt escompté par le responsable du traitement, les intérêts en jeu pour les personnes, les risques de dysfonctionnements organisationnels (par exemple violations du devoir de confidentialité) et les défaillances techniques sont autant d'aspects qu'il convient de prendre en considération. Par ailleurs, ce critère présente un caractère dynamique d'où la nécessité de tenir compte de l'état d'avancement technologique au moment du traitement et de changements éventuels pendant la période pour laquelle les données seront traitées. Il se peut que l'identification ne soit pas possible aujourd'hui avec l'ensemble des moyens existants auxquels l'on peut raisonnablement

[11] Arrêt du 6 novembre 2003 dans l'affaire C-101/2001 (Lindqvist), point 27.

recourir. Si les données doivent être conservées pendant une durée d'un mois, il est probable que l'identification ne pourra intervenir pendant la «durée de vie» des informations, et elles ne sauraient dès lors être considérées comme des données à caractère personnel. Cependant, si elles doivent être conservées pendant dix ans, le responsable du traitement doit envisager la possibilité d'une identification pouvant intervenir même au cours de la neuvième année, ce qui en ferait à ce moment-là des données à caractère personnel. Il est souhaitable que le système puisse s'adapter à ces développements lorsqu'ils interviennent, et intégrer alors les mesures techniques et organisationnelles appropriées en temps utile.

Exemple n° 12 − Publication de clichés radiographiques portant le prénom d'une patiente

Le cliché radiographique d'une patiente a été publié dans un journal scientifique, associé au prénom de celle-ci, un prénom très rare. Le prénom de cette personne associée à la connaissance qu'avaient ses proches de l'affection dont elle souffrait rendaient cette personne identifiable à un certain nombre de personnes; ce cliché radiographique entre alors dans la catégorie des données à caractère personnel.

Exemple n° 13 − Données de recherche pharmaceutique

Les hôpitaux ou les médecins, à titre individuel, transfèrent des informations médicales concernant leurs patients à une société à des fins de recherche médicale. Aucun nom de patient n'est utilisé, mais seulement un numéro de série attribué de manière aléatoire à chacun des cas cliniques, afin d'assurer la cohérence et d'éviter toute confusion avec des informations concernant différents patients. Seuls les médecins, qui sont tenus au secret médical, sont en possession des noms de leurs patients. Les données ne contiennent aucune autre information susceptible de rendre les patients identifiables par recoupement. De plus, toutes les autres mesures ont été prises pour éviter que les personnes concernées puissent être identifiées ou deviennent identifiables, que ce soit sur le plan juridique, technique ou organisationnel. Dans ces circonstances, l'autorité chargée de la protection des données peut considérer qu'il n'existe aucun moyen, dans le cadre du traitement des données réalisé par la société pharmaceutique, susceptible d'être raisonnablement mis en œuvre pour identifier les personnes concernées.

Comme mentionné plus haut, un facteur essentiel pour évaluer «*l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre*» pour identifier les personnes sera, en réalité, la finalité visée par le responsable du traitement dans le cadre du traitement des données. Les autorités nationales de protection des données ont été confrontées à des cas où, d'une part, le responsable du traitement prétend que seules des informations éparses sont traitées, sans aucune référence ni au nom ni à aucun autre identifiant direct, et fait valoir que ces données ne sauraient être assimilées à des données à caractère personnel ni soumises aux règles de protection des données. D'autre part, le traitement de ces informations n'a de sens que s'il permet l'identification de personnes spécifiques et un certain type de traitement. Lorsque la finalité du traitement implique l'identification de personnes physiques, il est permis de penser que le responsable du traitement ou toute autre personne concernée dispose ou disposera de moyen «susceptibles d'être raisonnablement mis en œuvre» pour identifier la personne concernée. En réalité, prétendre que les personnes physiques ne sont pas identifiables alors que la finalité du traitement est précisément de les identifier serait une contradiction absolue in terminis. Il est dès lors essentiel de considérer ces informations comme concernant des personnes

physiques identifiables et d'appliquer les règles de protection des données à leur traitement.

Exemple n° 14 − Vidéosurveillance

Cela est particulièrement important dans le contexte de la vidéosurveillance, où les responsables du traitement prétendent souvent que l'identification n'interviendrait que pour un faible pourcentage des éléments collectés et que dès lors, avant que l'identification n'intervienne dans ces cas limités, il ne saurait être question de traitement de données à caractère personnel. Étant donné que la finalité de la vidéosurveillance est néanmoins d'identifier les personnes apparaissant sur des images, lorsque le responsable du traitement juge cette identification nécessaire, l'ensemble de l'application relève du traitement de données concernant des personnes identifiables, même si certaines personnes enregistrées ne sont pas concrètement identifiables.

Exemple n° 15 − Adresses IP dynamiques

Le groupe de travail a considéré les adresses IP comme des données concernant une personne identifiable. Il a d'ailleurs précisé dans un document de travail que «*les fournisseurs d'accès Internet et les gestionnaires des réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs Internet auxquels ils ont attribué des adresses IP, du fait qu'ils enregistrent systématiquement dans un fichier les date, heure, durée et adresse dynamique IP donnée à l'utilisateur Internet. Il en va de même pour les fournisseurs de services internet qui conservent un fichier-registre sur le serveur HTTP. Dans ces cas, on peut parler, sans l'ombre d'un doute, de données à caractère personnel au sens de l'article 2, point a), de la directive*».[12]

Il apparaît notamment que lorsque le traitement d'adresses IP été effectué pour identifier les utilisateurs de l'ordinateur (par exemple, par des titulaires de droits d'auteur afin de poursuivre ces utilisateurs d'ordinateurs pour violation de droits de la propriété intellectuelle), le responsable du traitement part du principe que les «moyens susceptibles d'être raisonnablement mis en œuvre» pour identifier les personnes seront disponibles, par exemple par l'intermédiaire des tribunaux saisis (sinon la collecte d'informations serait inutile), de sorte qu'il convient de considérer ces informations comme des données à caractère personnel.

À noter toutefois le cas particulier de certains types d'adresses IP qui, dans certaines circonstances, ne permettent en fait pas l'identification de l'utilisateur, et ce, pour diverses raisons d'ordre technique et organisationnel. L'exemple des adresses IP attribuées à un ordinateur dans un café internet illustre cette situation, puisque dans ce cas aucune identification des clients n'est requise. On pourrait faire valoir que les données collectées sur l'utilisation d'un ordinateur X pendant un certain laps de temps ne permettent pas l'identification de l'utilisateur à l'aide de moyens raisonnables, et que celles-ci ne sont donc pas des données à caractère personnel. Toutefois, il convient de relever qu'il est très probable que les fournisseurs d'accès internet ignorent si l'adresse IP en question permet ou non l'identification, et qu'ils traitent les données associées à cette IP de la même manière qu'ils traitent les informations associées aux adresses IP d'utilisateurs dûment enregistrés et identifiables. Ainsi, à moins que les fournisseurs d'accès internet soient en mesure de déterminer avec une certitude absolue que les

[12] WP 37: «Le respect de la vie privée sur Internet - Une approche européenne intégrée sur la protection des données en ligne», adopté le 21.11.2000.

données correspondent à des utilisateurs non identifiables, par mesure sécurité, ils devront traiter toutes les informations IP comme des données à caractère personnel.

Exemple n° 16 − Dommages causés par des graffiti

Des véhicules destinés au transport de passagers d'une société de transport subissent régulièrement des dommages occasionnés par des graffiti. Afin d'évaluer les dommages et de faciliter les poursuites judiciaires contre les auteurs de ces graffiti, la société tient un registre contenant des informations sur les circonstances des dommages ainsi que des photographies des véhicules endommagés et des «tags» ou de la «signature» des auteurs. Lorsque ces informations sont inscrites dans ce registre, les auteurs des dommages ne sont pas connus pas plus que l'on ne sait à qui appartient la «signature». Il est bien possible que l'on ne le découvre jamais. Toutefois, la finalité du traitement est précisément d'identifier les personnes physiques auxquelles se rapportent les informations en tant qu'auteurs des dommages afin de pouvoir les traduire en justice. Ce type de traitement n'a de sens que si le responsable du traitement des données considère comme «raisonnablement probable» qu'un jour il disposera des moyens pour identifier des personnes. Les informations contenues dans les images sont à considérer comme des données relatives à des personnes physiques «identifiables», les informations dans ce registre comme des «données à caractère personnel», et le traitement doit être soumis aux règles de protection des données qui considèrent ce type de traitement comme légitime, dans certaines circonstances et moyennant certaines garanties.

Lorsque l'identification de la personne concernée ne figure pas dans la finalité du traitement, les mesures techniques visant à empêcher l'identification ont un rôle très important à jouer. La mise en place des mesures techniques et organisationnelles les plus appropriées existantes pour protéger les données contre l'identification peut être déterminante pour considérer que les personnes ne sont pas identifiables, compte tenu de «*l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne*» pour identifier les personnes physiques. Dans ce cas, la mise en œuvre de telles mesures n'est pas la *conséquence* de l'obligation légale découlant de l'article 17 de la directive (qui ne s'applique que si les informations sont, en premier lieu, des données à caractère personnel), mais plutôt une *condition* pour que les informations ne puissent justement pas être considérées comme des données à caractère personnel et que leur traitement ne soit pas soumis à la directive.

Données pseudonymisées

La pseudonymisation est un traitement qui consiste à dissimuler l'identité. L'objectif de ce traitement est de permettre la collecte de données supplémentaires relatives à la même personne sans qu'il soit nécessaire de connaître son identité. Il s'agit là d'un aspect particulièrement important dans le contexte de la recherche et des statistiques.

La pseudonymisation peut s'effectuer de manière retraçable en utilisant soit des listes de correspondance des identités et leurs pseudonymes, soit des algorithmes de cryptage à double sens pour la pseudonymisation. Il est également possible de dissimuler les identités de manière à rendre toute réidentification impossible, par exemple, grâce à un cryptage à sens unique qui génère en général des données anonymisées.

L'efficacité de la procédure de pseudonymisation dépend d'un certain nombre de facteurs (le stade auquel on y recourt, son niveau de sécurité en ce qui concerne la possibilité de retracer les informations, l'importance de la population dans laquelle la personne est dissimulée, la possibilité de rattacher des transactions/enregistrements individuels à une même personne, etc.). Les pseudonymes doivent faire l'objet d'un choix aléatoire et non prévisible. La quantité de pseudonymes possible doit être assez grande pour que le même pseudonyme ne puisse jamais être choisi deux fois au hasard. Pour garantir un niveau de sécurité élevé, il importe que l'ensemble des pseudonymes potentiels soit au moins équivalent à l'éventail des valeurs des fonctions de hachage cryptographique sûres[13].

Les données pseudonymisées de manière retraçable peuvent être considérées comme des informations sur des personnes physiques *indirectement identifiables*. En effet, les pseudonymes permettent d'établir une correspondance avec une personne de telle façon que l'identité de cette personne ne soit reconnaissable que dans des cas spécifiques définis à l'avance. Dans ce cas, bien que les règles de protection des données s'appliquent, les risques que présente pour les personnes physiques le traitement de ces informations indirectement identifiables seront le plus souvent minimes, si bien que l'application de ces règles sera à juste titre, plus souple que dans le cas de traitement d'informations concernant des personnes physiques directement identifiables.

Données codées

Les données codées sont un exemple classique de pseudonymisation. Les informations correspondent à des personnes physiques possédant chacune un code, la clé permettant d'établir une correspondance entre ce code et des identifiants courants de ces personnes physiques (comme le nom, la date de naissance, l'adresse) étant conservée séparément.

Exemple n° 17 − Données non agrégées à des fins statistiques

Un exemple illustrant l'importance la prise en compte de toutes les circonstances pour évaluer si les moyens d'identification sont «susceptibles d'être raisonnablement» utilisés, pourrait être celui des informations à caractère personnel traitées par l'institut national de la statistique, lorsqu'à un certain stade les informations sont conservées sous une forme non agrégée et concernent des personnes physiques spécifiques, mais sont désignées par un code plutôt que par un nom (par exemple la personne portant le code X1234 boit un verre de vin par jour plus de trois fois par semaine). L'institut de la statistique conserve la clé permettant d'accéder à ces codes séparément (la liste des codes correspondant aux noms des personnes). Cette clé peut être considérée comme susceptible d'être «raisonnablement utilisée» par l'institut de la statistique, de sorte que l'ensemble des informations relatives à une personne physique peuvent être considérées comme des données à caractère personnel et l'institut doit les soumettre aux règles de protection des données. Or, on peut imaginer qu'une liste de données concernant les habitudes de consommation de vin de consommateurs soit transférée à l'organisation viticole nationale, afin de lui permettre d'appuyer sa stratégie publique sur des statistiques. Pour déterminer si cette liste d'informations constitue toujours des données personnelles, il convient de vérifier si les différents consommateurs de vin peuvent être

[13] Voir document de travail «Techniques améliorant la protection des données» réalisé par le groupe de travail «Techniques améliorant la protection des données» du comité «Questions techniques et organisationnelles relatives à la protection des données» des commissaires chargés de la protection des données du Bund et des Länder allemands (octobre 1997), disponible à l'adresse suivante: http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

identifiés, compte tenu de «*l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne*».

Si les codes utilisés sont uniques et correspondent à une personne spécifique, le risque d'identification existe à partir du moment où il est possible d'avoir accès à la clé d'encryptage utilisée. Par conséquent, les risques de piratage externe, la probabilité qu'un membre de l'entreprise expéditrice − même s'il est tenu au secret professionnel − transmette la clé *et* la faisabilité d'une identification indirecte sont autant de facteurs qui méritent d'être pris en compte pour déterminer si les personnes peuvent être identifiées, *compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne*, et donc s'il faut considérer les informations comme des «données à caractère personnel». Si tel est le cas, les règles de protection des données s'appliquent. Un autre problème réside dans le fait qu'il est possible que ces règles de protection des données prennent en considération le degré de risque pour les personnes physiques, ce qui signifie que le traitement serait soumis à des conditions plus ou moins strictes, en faisant usage de la souplesse prévue par les dispositions de la directive.

Par contre, si les codes ne sont pas uniques, mais que le même numéro de code (par exemple «123») est utilisé pour désigner des personnes résidant dans des villes différentes, et portent sur des données issues de différentes années (la distinction d'une personne physique particulière n'intervient que dans le cadre d'une année et au sein de l'échantillon d'une même ville), le responsable du traitement ou un tiers ne pourrait identifier une personne physique spécifique qu'à condition de savoir à quelle année et à quelle ville les données se réfèrent. Si ces informations supplémentaires disparaissaient, et qu'elles ne sont pas *susceptibles d'être raisonnablement* récupérées, on pourrait alors considérer que ces informations ne se rapportent pas à des personnes physiques identifiables et qu'elles ne sauraient être soumises aux règles de protection des données.

Ce type de données est couramment utilisé dans les essais cliniques de médicaments. Ces activités sont régies par le cadre juridique établi par la directive 2001/20/CE du 4 avril 2001 relative à l'application de bonnes pratiques cliniques dans la conduite d'essais cliniques[14]. Le professionnel/chercheur en médecine («investigateur») qui effectue des essais sur des médicaments collecte des données sur les résultats cliniques de patients identifiés chacun par un code. Le chercheur ne communique les informations à la société pharmaceutique ou à d'autres parties intéressées («promoteurs») que sous forme codée, car leurs intérêts ne portent que sur les informations biostatistiques. Toutefois, l'investigateur conserve séparément la clé permettant d'associer le code à des informations générales pour identifier les patients séparément. Pour protéger la santé des patients s'il s'avère que les médicaments comportent des risques, l'investigateur est tenu de conserver cette clé, de manière à pouvoir identifier les patients individuellement pour leur permettre, le cas échéant, de recevoir un traitement approprié.

La question qui se pose ici est de savoir si les données utilisées aux fins d'essais cliniques peuvent être considérées comme concernant des personnes physiques «identifiables» et donc être soumises aux règles de protection des données. Conformément à l'analyse décrite ci-dessus, pour déterminer si une personne est identifiable, il convient de prendre en compte l'ensemble des moyens susceptibles

[14] JO L 121 du 1.5.2001, p. 34.

d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne pour identifier ladite personne. Dans ce cas, l'identification des personnes physiques (pour appliquer le traitement approprié, le cas échéant) est l'une des finalités du traitement des données codées. La société pharmaceutique a analysé les moyens destinés au traitement, a prévu les mesures organisationnelles et ses relations avec le chercheur qui détient la clé de telle manière que l'identification des personnes physiques *peut* non seulement intervenir, mais *doit* aussi intervenir dans certaines circonstances. Ainsi, l'identification des patients figure parmi les finalités et les moyens du traitement. En l'occurrence, on peut conclure que ces données codées constituent des informations concernant des personnes physiques identifiables par toutes les parties concernées par l'identification éventuelle, et doivent être soumises aux règles de protection des données. Cela ne signifie pas pour autant que tout autre responsable du traitement des données qui traite le même ensemble de données codées doive être considéré comme traitant des données à caractère personnel, si le système spécifique dans lequel ces autres responsables du traitement opèrent exclut expressément la réidentification et que des mesures techniques ont été prises à cet effet.

Dans d'autres domaines de la recherche ou dans le cadre du même projet, il est possible que la réidentification de la personne concernée ait été exclue lors de la conception des protocoles et de la procédure, par exemple lorsqu'aucun aspect thérapeutique n'est concerné. Pour des raisons techniques ou autres, il peut toujours être possible de découvrir à quelles personnes correspondent telles données cliniques, mais cette identification n'est en aucun cas censée se produire ou escomptée, et des mesures techniques appropriées (par exemple cryptographie, hachage irréversible) ont été mises en place pour prévenir cette éventualité. En l'occurrence, même si l'identification de certaines personnes concernées peut se produire malgré tous les protocoles et mesures (en raison de circonstances imprévisibles telles qu'une correspondance accidentelle des caractéristiques de la personne concernée qui révèlent son identité), les informations traitées par le responsable initial peuvent ne pas être considérées comme concernant des personnes physiques identifiées ou identifiables, compte tenu *de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne*. Leur traitement peut ainsi ne pas être soumis aux dispositions de la directive. Il en va tout autrement pour le nouveau responsable du traitement qui a effectivement eu accès aux données identifiables qui seront, elles, sans aucun doute considérées comme des «données à caractère personnel».

FAQ 14-7 sur le régime de la «sphère de sécurité»

La question des données codées dans la recherche pharmaceutique a été traitée dans le cadre du régime de la «sphère de sécurité[15]. La FAQ (frequently asked question – question souvent posée) 14-7 est ainsi libellée:

FAQ 14 - Produits pharmaceutiques et médicaux

7. Q: Les données de la recherche sont habituellement codées à leur source uniquement par le chercheur principal, pour ne pas révéler l'identité des intéressés. Les sociétés pharmaceutiques qui commanditent ce type de recherche ne reçoivent pas la clé de ce code. Le code de la clé unique est détenu par le seul chercheur, pour qu'il puisse identifier la personne concernée dans des circonstances spéciales (par exemple, si un suivi médical est requis). Le transfert de l'Union européenne aux États-Unis de données

[15] Décision de la Commission 2000/520/CE du 26.7.2000, JO L 215 du 25.8.2000, p. 7.

personnelles ainsi codées représente-t-il un transfert de données soumis aux principes de la «sphère de sécurité»?

7. R: Non. Cela ne représenterait pas un transfert de données personnelles soumis à ces principes.

Le groupe de travail estime que cet avis exprimé dans le cadre du régime de la «sphère de sécurité» ne va pas à l'encontre de l'argumentation exposée ci-dessus qui aurait tendance à considérer ces informations comme des données à caractère personnel soumises à la directive. En réalité, cette FAQ n'est pas suffisamment précise, dans la mesure où elle n'indique ni le destinataire ni les modalités de transfert de ces données. Selon le groupe de travail, la FAQ se réfère au cas dans lequel les données codées sont communiquées à un destinataire aux États-Unis (par exemple, la société pharmaceutique) qui ne reçoit que les données codées et n'aura jamais connaissance de l'identité des patients qui n'est connue et ne sera connue, si un traitement s'avère nécessaire, que par le professionnel/chercheur en médecine, mais jamais par la société américaine.

Données anonymes

Par «données anonymes» au sens de la directive, on entend toute information concernant une personne physique lorsque cette personne ne peut être identifiée, ni par le responsable du traitement des données ni par une autre personne, *compte tenu de l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne* pour identifier ladite personne. Les «données anonymisées» sont donc des données anonymes qui concernaient auparavant une personne identifiable, mais ne permettent plus cette identification. Le considérant 26 évoque également ce concept lorsqu'il énonce que «*les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable*». Une fois encore, pour vérifier si les données permettent l'identification d'une personne physique et si ces informations peuvent être considérées comme anonymes ou pas, il faut tenir compte des circonstances, et un examen au cas par cas s'impose et s'attachera notamment à vérifier dans quelle mesure les moyens sont susceptibles d'être raisonnablement mis en œuvre pour l'identification, comme décrit au considérant 26. Cela s'avère particulièrement important dans le cas des informations statistiques où, en dépit du fait que lesdites informations peuvent se présenter sous forme agrégée, l'échantillon initial n'est pas suffisamment important et d'autres éléments d'information peuvent permettre d'identifier les personnes physiques.

Exemple n° 18 − Enquêtes statistiques et association d'informations éparses

En dehors de leur obligation générale de respecter les règles de protection des données afin d'assurer l'anonymat des enquêtes statistiques, les statisticiens sont soumis à une obligation spécifique de secret professionnel et, en vertu de ces règles, il leur est interdit de publier des données non anonymes. Ils sont donc contraints de publier des données statistiques agrégées qui ne peuvent en aucun cas être attribuées à une personne identifiée dissimulée derrière les statistiques. Cette règle est particulièrement importante en ce qui concerne la publication de données de recensement. Il convient de déterminer, dans chaque situation, un seuil en dessous duquel on estime qu'il est possible d'identifier les personnes concernées. S'il apparaît qu'un critère conduit à une identification dans une catégorie de personnes donnée, quelle que soit sa taille (par

exemple un seul médecin opère dans une ville de 6 000 habitants), il importe d'éliminer complètement ce critère «discriminatoire» ou d'ajouter d'autres critères pour «diluer» les résultats sur une personne donnée, afin de garantir le secret statistique.

Exemple n° 19 − Publication d'informations résultant d'un système de vidéosurveillance

Un commerçant installe un système de surveillance par caméra dans son magasin. Il affiche, dans son magasin, des photos de gens pris en flagrant délit de vol grâce au système de surveillance par caméra. Après l'intervention de la police, il occulte les visages des voleurs, en les assombrissant. Néanmoins, malgré cette précaution, il est toujours possible que ces personnes soient reconnues sur des photos par des amis, des proches ou des voisins, par exemple parce que leur silhouette, leur coupe de cheveux et leurs vêtements sont encore reconnaissables.

4. QUATRIEME ELEMENT: «PERSONNE PHYSIQUE»

La protection assurée par les dispositions de la directive s'applique aux personnes physiques, c'est-à-dire aux êtres humains. Le droit à la protection des données à caractère personnel est, en ce sens, un droit universel qui n'est pas limité aux ressortissants ou résidents d'un certain pays. Le considérant 2 de la directive s'y réfère explicitement en énonçant que «*les systèmes de traitement de données sont au service de l'homme» et qu'ils «doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter les libertés et droits fondamentaux de ces personnes*».

Le concept de «personne physique» est évoqué à l'article 6 de la Déclaration universelle des droits de l'homme qui se lit comme suit: «*Chacun a le droit à la reconnaissance en tous lieux de sa personnalité juridique*.» La législation des États membres, généralement dans le domaine du droit civil, décrit plus précisément le concept de la personnalité des êtres humains, considérée comme la capacité à être un sujet de droit, de la naissance de l'individu jusqu'à son décès. Les données personnelles sont dès lors en principe des données concernant des *personnes vivantes* identifiées ou identifiables. Cela soulève un certain nombre de questions aux fins de la présente analyse.

Données relatives à des personnes décédées

Les informations relatives à des personnes décédées ne sauraient, en principe, être considérées comme des données à caractère personnel soumises aux règles de la directive, étant donné qu'en vertu du droit civil les personnes décédées ne sont plus des personnes physiques. Cependant, les données des personnes décédées peuvent, dans certains cas, encore bénéficier indirectement d'un certain niveau de protection.

D'une part, les responsables du traitement de données ne sont peut-être pas en mesure de vérifier si la personne à laquelle se rapportent les données est encore vivante ou éventuellement décédée. Même en admettant qu'ils le soient, les informations relatives à la personne décédée peuvent être traitées selon le même système que si elle était en vie, sans distinction aucune. Étant donné que le responsable du traitement des données est soumis aux obligations de protection des données énoncées par la directive en ce qui concerne les données sur les personnes vivantes, il sera probablement plus facile pour lui, dans la pratique, de traiter également les données relatives aux personnes

décédées dans les conditions imposées par les règles de protection des données, plutôt que de séparer les deux ensembles de données.

D'autre part, les informations relatives à des personnes décédées peuvent concerner également des personnes vivantes. À titre d'exemple, les informations révélant que la personne décédée X était atteinte d'hémophilie indiquent que son fils souffre aussi de la même maladie, étant donné que celle-ci est due à un gène contenu dans le chromosome X. Ainsi, lorsque des informations qui sont des données relatives à des personnes décédées peuvent être considérées comme concernant en même temps des personnes vivantes et constituer des données à caractère personnel soumises aux dispositions de la directive, les données à caractère personnel des personnes décédées peuvent bénéficier indirectement de la protection des règles de protection des données.

Troisièmement, les informations relatives aux personnes décédées peuvent bénéficier d'une protection spécifique accordée par une série de règles autres que la législation sur la protection des données, fixant les limites de ce que d'aucuns appellent la *personalitas praeterita*. L'obligation de confidentialité du personnel médical ne s'éteint pas avec le décès du patient. La législation nationale sur le droit au respect de l'image et de l'honneur peut également prévoir une protection de la mémoire de la personne décédée.

Quatrièmement, rien ne s'oppose à ce qu'un État membre étende la portée de la législation nationale transposant les dispositions de la directive 95/46/CE à des domaines non inclus dans le champ d'application de ladite directive, pour autant qu'aucune autre disposition du droit communautaire n'y fasse obstacle, comme l'a rappelé la Cour de justice des Communautés et européennes[16]. On peut imaginer que certains législateurs nationaux décident d'étendre les dispositions de la législation nationale en matière de protection des données à certains aspects concernant le traitement des données relatives à des personnes décédées, lorsqu'un intérêt légitime le justifie[17].

Enfants à naître

L'applicabilité des règles de protection des données avant la naissance dépend de l'orientation générale adoptée dans les ordres juridiques nationaux à propos de la protection des enfants à naître. Pour tenir essentiellement compte des droits de succession, certains États membres reconnaissent le principe selon lequel les enfants conçus mais pas encore nés sont considérés comme s'ils étaient nés s'agissant de certains droits (ils peuvent par exemple hériter ou accepter une donation), sous réserve qu'ils naissent effectivement. Dans d'autres États membres, ils bénéficient d'une protection spécifique régie par des dispositions légales particulières, également subordonnée à la même condition. Afin de déterminer si les dispositions nationales de protection des données protègent également les informations concernant les enfants à naître, il convient de considérer l'approche générale de l'ordre juridique national, tout en gardant à l'esprit que la finalité des règles de protection des données est de protéger la personne physique.

---

16 Arrêt du 6 novembre 2003 dans l'affaire C-101/2001 (Lindqvist), point 98.

17 Procès-verbal du Conseil de l'Union européenne, 8.2.1995, document n° 4730/95: Ad article 2a : «*Le Conseil et la Commission confirment qu'il appartient aux États membres de déterminer si et dans quelle mesure la présente directive est susceptible de s'appliquer aux personnes décédées*.»

Une deuxième question réside dans le fait que l'attitude générale de l'ordre juridique se fonde sur le principe selon lequel la situation des enfants à naître est limitée dans le temps à la durée de la grossesse. Le fait que cette situation puisse, en réalité, se prolonger bien au-delà, comme dans le cas d'embryons congelés, n'est pas pris en compte. Enfin, il arrive que des solutions juridiques spécifiques soient prévues en particulier dans les dispositions régissant les techniques de reproduction, qui traitent de l'utilisation des informations médicales ou génétiques sur les embryons.

Personnes morales

Étant donné que la définition des données à caractère personnel se réfère à des particuliers, c'est-à-dire à des personnes physiques, les informations concernant les personnes morales ne sont en principe pas couvertes par la directive, de sorte qu'elles ne bénéficient pas de la protection qu'elle prévoit[18]. Toutefois, certaines règles de protection des données peuvent malgré tout s'appliquer indirectement à des informations concernant des entreprises ou des personnes morales, dans certaines circonstances particulières.

Certaines dispositions de la directive 2002/58/CE relative à la vie privée dans le secteur des communications électroniques s'étendent aussi aux personnes morales. Son article 1er est libellé comme suit: «*2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales*». Par conséquent, les articles 12 et 13 étendent l'application de certaines dispositions concernant respectivement les annuaires d'abonnés et les communications non sollicitées aux personnes morales.

Les informations ayant trait à des personnes morales peuvent également être considérées comme «concernant» des personnes physiques en tant que telles, selon les critères énoncés dans le présent document. Cela peut être le cas lorsque le nom de la personne morale est dérivé de celui d'une personne physique. Un autre cas de figure est celui du courrier électronique d'une entreprise qui est normalement utilisé par un employé, ou des informations concernant une petite entreprise (du point de vue juridique, un «objet» plutôt qu'une personne morale) qui peuvent éventuellement décrire le comportement de leur propriétaire. Dans tous ces cas, lorsque les critères de «contenu», de «finalité» ou de «résultat» permettent de considérer les informations relatives à une personne morale ou à une entreprise comme «concernant» une personne physique, il y a lieu de les considérer comme des données à caractère personnel, et dès lors les règles de protection des données doivent s'appliquer.

Comme l'a précisé la Cour de justice des Communautés européennes, rien ne s'oppose à ce qu'un État membre étende la portée de la législation nationale transposant les dispositions de la directive 95/46 à des domaines non inclus dans le champ d'application de cette dernière, pour autant qu'aucune autre disposition du droit communautaire n'y fasse obstacle[19]. Ainsi, certains États membres, tels que l'Italie, l'Autriche et le Luxembourg, ont étendu l'application de certaines dispositions de leur législation nationale transposant la directive (comme celles sur les mesures de sécurité) au traitement de données concernant des personnes morales.

---

18 Considérant 24 de la directive: «*considérant que les législations relatives à la protection des personnes morales à l'égard du traitement des données qui les concernent ne sont pas affectées par la présente directive*».

19 Arrêt du 6 novembre 2003 dans l'affaire C-101/2001 (Lindqvist), point 98.

Comme dans le cas des informations relatives aux personnes décédées, il peut arriver qu'en vertu des modalités pratiques mises en place par le responsable du traitement des données, des données relatives à des personnes morales soient soumises de facto aux règles sur la protection des données. Lorsque le responsable du traitement collecte sans distinction des données relatives à des personnes physiques et morales, et les inclut dans les mêmes séries de données, la conception des mécanismes de traitement des données et le système d'audit peuvent être établis de manière à satisfaire aux règles de protection des données. En réalité, il peut s'avérer plus facile pour le responsable du traitement d'appliquer les règles de protection des données à tous les types d'informations qu'il traite plutôt que d'établir une distinction entre les informations relatives aux personnes physiques et celles relatives aux personnes morales.

IV. QUE SE PASSE-T-IL SI LES DONNÉES NE RELÈVENT PAS DU CHAMP D'APPLICATION DE LA DÉFINITION?

Comme nous l'avons vu tout au long du présent document, il se peut que, dans certaines circonstances, les informations ne soient pas considérées comme des données à caractère personnel. Il en est ainsi lorsque les données ne peuvent être considérées comme concernant une personne physique, ou parce que les personnes physiques ne peuvent pas être considérées comme identifiées ou identifiables. Lorsque les informations traitées ne relèvent pas du concept de «données à caractère personnel», il s'ensuit que la directive ne s'applique pas, conformément à son article 3. Cela ne signifie pas pour autant que les personnes physiques soient privées de toute forme de protection dans cette situation particulière. Les éléments suivants méritent d'être pris en considération.

Si la directive ne s'applique pas, en revanche, la législation nationale sur la protection des données peut, elle, s'appliquer. Comme prévu à l'article 34, les États membres sont destinataires de ladite directive. En dehors de son champ d'application, les États membres ne sont pas soumis aux obligations qu'elle impose, à savoir mettre en vigueur les dispositions législatives, règlementaires et administratives nécessaires pour se conformer à ladite directive. Cependant, comme l'a précisé la Cour de justice des Communautés européennes, rien ne s'oppose à ce qu'un État membre étende la portée de la législation nationale transposant les dispositions de la directive 95/46 à des domaines non inclus dans le champ d'application de cette dernière, pour autant qu'aucune autre disposition du droit communautaire n'y fasse obstacle. Il est donc tout à fait possible que certaines situations n'impliquant pas le traitement de données à caractère personnel telles que définies dans la directive fassent tout de même l'objet de mesures de protection en vertu du droit national. Cela peut s'appliquer par exemple à un domaine tel que celui des données codées, qu'il s'agisse de données à caractère personnel ou non.

Lorsque les règles de protection des données ne s'appliquent pas, certaines activités peuvent néanmoins être contraires à l'article 8 de la Convention européenne des droits de l'homme, qui protège le droit à la vie privée et familiale, à la lumière de la jurisprudence étendue de la CEDH. D'autres séries de règles telles que la législation sur les délits civils, le droit pénal ou la législation interdisant la discrimination peuvent également offrir une protection aux personnes physiques lorsque les règles de protection des données ne s'appliquent pas et que divers intérêts légitimes sont éventuellement en jeu.

V. CONCLUSIONS

Dans le présent avis, le groupe de travail a donné des orientations sur la manière dont il convient d'interpréter le concept de données à caractère personnel dans la directive 95/46/CE et la législation communautaire connexe, et de l'appliquer dans diverses situations.

Le constat général est que l'intention du législateur européen était d'adopter une notion large de données à caractère personnel, bien qu'il existe certaines limites à cette notion. Il ne faut jamais perdre de vue que l'objectif des règles contenues dans la directive est d'assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de la vie privée, à l'égard du traitement des données à caractère personnel. Ces règles ont donc été conçues pour s'appliquer à des situations où les droits des personnes physiques pourraient être menacés et nécessitent par conséquent d'être protégés. Le champ d'application des règles de protection des données ne doit pas être trop étendu, mais il faut également éviter de restreindre indûment l'interprétation du concept de données à caractère personnel. La directive a défini son champ d'application, en excluant un certain nombre d'activités, et permet une certaine souplesse dans l'application des règles aux activités qui relèvent de son champ d'application. Les autorités de protection des données jouent un rôle essentiel pour parvenir à un équilibre approprié dans cette application (voir partie II).

L'analyse du groupe de travail reposait sur quatre grands éléments constitutifs apparaissant dans la définition des «données à caractère personnel», à savoir «toute information», «concernant», «personne physique», «identifiée ou identifiable». Ces éléments sont étroitement liés et interdépendants, mais déterminent ensemble les éléments d'information à considérer comme «données à caractère personnel». Cette analyse est étayée par des exemples tirés de la pratique nationale des autorités européennes de protection des données.

- Le premier élément − «toute information» − appelle une interprétation large du concept, indépendamment de la nature ou du contenu des informations, et du format technique de présentation. Cela signifie que tant les informations objectives que subjectives concernant une personne, à quelque titre que ce soit, peuvent être considérées comme «données à caractère personnel», indépendamment du support technique sur lequel elles se trouvent. Dans le présent avis, le groupe de travail aborde également les données biométriques et les distinctions juridiques concernant les prélèvements humains dont elles peuvent être extraites (voir point III.1).

- Le deuxième élément − «concernant» − a jusqu'à présent été souvent négligé, bien qu'il joue un rôle crucial pour déterminer la portée matérielle du concept, notamment en ce qui concerne les objets et les nouvelles technologies. Dans son avis, le groupe de travail avance trois autres éléments - le contenu, la finalité ou le résultat − pour déterminer si les informations «concernent» une personne physique. Ils s'appliquent également aux informations susceptibles d'avoir une influence manifeste sur la manière dont une personne physique est traitée ou évaluée (voir point III.2).

- Le troisième élément − «identifiée ou identifiable» − se concentre sur les conditions dans lesquelles il convient de considérer une personne physique comme «identifiable», et notamment sur «les moyens susceptibles d'être raisonnablement mis en œuvre» soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne. Le contexte particulier et les circonstances liées à un cas

spécifique sont déterminants dans cette analyse. Le groupe de travail aborde aussi les «données pseudonymisées» et l'utilisation de «données codées» dans la recherche statistique ou pharmaceutique (voir point III.3).

- Le quatrième élément − «personne physique» − concerne l'exigence voulant que les «données à caractère personnel» portent sur des «personnes physiques vivantes». Le groupe examine en outre les interfaces avec les données relatives à des personnes décédées, des enfants à naître et des personnes morales (voir point III.4).

La dernière partie est consacrée à ce qui se produit si les données ne relèvent pas du champ d'application de la définition des «données à caractère personnel». Différentes solutions sont envisageables pour remédier aux problèmes posés en l'occurrence, notamment par le biais de la législation nationale en dehors du champ d'application de la directive, sous réserve du respect des autres dispositions du droit communautaire (voir point IV).

Le groupe de travail invite toutes les parties intéressées à examiner soigneusement les orientations fournies dans le présent avis et d'en tenir compte dans leur interprétation et leur application des dispositions de droit national conformément à la directive 95/46/CE.

Les membres du groupe de travail qui, dans leur majorité, représentent des autorités nationales de contrôle de la protection des données s'engagent à approfondir ces orientations dans le cadre de leurs compétences et de veiller à la bonne application de leur législation nationale conformément à la directive 95/46/CE.

Le groupe de travail entend appliquer et approfondir les orientations fournies dans le présent avis, lorsque cela s'avère nécessaire, et en tenir soigneusement compte dans ses futurs travaux, en particulier lorsqu'il traitera de thèmes tels que la gestion de l'identité dans le contexte de l'administration électronique («e-government») et des services de télésanté («e-health»), de même que dans le contexte de la technologie RFID (radio-identification). Dans ce dernier secteur, le groupe de travail entend contribuer à une nouvelle analyse de l'influence des règles de protection des données sur l'utilisation de la technologie RFID et l'éventuel besoin de prendre les mesures complémentaires indispensables au respect des droits et des intérêts en matière de protection des données dans ce contexte.

Enfin, le groupe de travail accueillera avec satisfaction tout retour d'information des parties intéressées et des autorités de contrôle concernant leur expérience pratique des orientations fournies dans le présent avis, notamment tout autre exemple complétant ceux évoqués dans le présent document. Il entend revenir sur ce sujet en temps voulu, en vue de parvenir à une perception commune du concept clé de données à caractère personnel, et d'assurer une application harmonisée et une meilleure mise en œuvre de la directive 95/46/CE et, sur cette base, de la législation communautaire connexe.

Pour le groupe de travail

Le président
Peter SCHAAR