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

01197/11/FR
WP 187

Avis 15/2011 sur la définition du consentement

adopté le 13 juillet 2011

Résumé

Cet avis fournit une analyse approfondie du concept de consentement, tel qu'il est actuellement utilisé dans les directives «protection des données» et «vie privée et communications électroniques». S'appuyant sur l'expérience des membres du groupe de travail «Article 29», l'avis présente de nombreux exemples de consentement valable et non valable, en se concentrant sur ses éléments fondamentaux tels que le sens des termes «manifestation de volonté», «libre», «spécifique», «indubitable», «explicite», «informée», etc. Il précise aussi certains aspects liés à la notion de consentement, comme le moment où celui-ci doit être obtenu, la différence entre le droit d'opposition et le consentement, etc.

Le consentement est l'un des fondements juridiques du traitement de données à caractère personnel. Il joue un rôle important, mais cela n'exclut pas la possibilité que, compte tenu du contexte, d'autres fondements juridiques puissent être jugés plus appropriés par le responsable du traitement ou la personne concernée. S'il est utilisé à bon escient, le consentement est un instrument qui permet à la personne concernée de contrôler le traitement de ses données. S'il est mal utilisé, en revanche, le contrôle de la personne concernée devient illusoire et le consentement constitue alors une base inappropriée pour le traitement de données.

Cet avis répond notamment à une demande formulée par la Commission dans le cadre de la révision en cours de la directive «protection des données». Il contient donc des recommandations à prendre en compte aux fins de cette révision. Parmi celles-ci, on retiendra qu'il y a lieu:

(i) de clarifier le sens de l'expression «consentement indubitable» et d'expliquer que seul un consentement fondé sur des déclarations ou des actions marquant un accord peut être considéré comme valable;

(ii) d'exiger des responsables du traitement qu'ils mettent en place des mécanismes pour démontrer le consentement (dans le cadre de l'obligation générale de rendre compte);

(iii) d'ajouter une exigence explicite concernant la qualité et l'accessibilité des informations servant de base au consentement, ainsi que

(iv) de considérer les propositions formulées concernant les mineurs et d'autres personnes juridiquement incapables.

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

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

vu l'article 29, l'article 30, paragraphe 1, point a), et l'article 30, paragraphe 3, de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

I. Introduction

Le consentement de la personne concernée a toujours été une notion clé en matière de protection des données, mais il n'est pas toujours aisé de déterminer quand un consentement est nécessaire et quelles conditions doivent être remplies pour qu'un consentement soit valable. Ce manque de clarté peut conduire à des approches différentes et à des divergences de vues sur les bonnes pratiques entre les États membres. Il peut également affaiblir la position des personnes concernées. Ce problème se pose de manière plus aiguë, dans la mesure où le traitement de données à caractère personnel est devenu une caractéristique de plus en plus marquante de la société moderne, que ce soit dans des environnements en ligne ou non, impliquant souvent différents États membres. C'est la raison pour laquelle, dans le cadre de son programme de travail 2010-2011, le groupe de travail «Article 29» a décidé d'examiner attentivement cette question.

Le consentement est également l'un des thèmes sur lesquels la Commission a demandé une contribution dans le cadre de la révision de la directive 95/46/CE. Dans sa communication intitulée «Une approche globale de la protection des données à caractère personnel dans l'Union européenne»[1], la Commission déclare: «*La Commission étudiera les moyens de clarifier et de renforcer les règles en matière de consentement*». La communication explique[2] cette déclaration comme suit:

> «*Lorsqu'un consentement éclairé est exigé, les règles en vigueur prévoient que l'accord de l'intéressé sur le traitement de données à caractère personnel le concernant devrait consister dans "toute manifestation de volonté, libre, spécifique et informée" par laquelle il accepte ce traitement. Or actuellement, dans les États membres, ces conditions font l'objet d'interprétations diverses, allant de l'obligation générale d'obtenir un consentement écrit à l'acceptation d'un consentement implicite.*
>
> *En outre, dans un environnement en ligne – vu l'opacité des politiques de protection de la vie privée –, les personnes ont souvent plus de difficulté à s'informer sur leurs droits et à donner un consentement éclairé. Cela est d'autant plus complexe que, dans certains cas, l'on ne voit pas clairement ce qui constituerait un consentement libre, spécifique et éclairé à un traitement de données, comme dans le domaine de la*

1 COM(2010) 609 final du 4.11.2010.

2 Le premier rapport de la Commission sur la mise en œuvre de la directive relative à la protection des données (95/46/CE) (COM(2003) 265 final, précisait déjà à la page 17: «La notion de "consentement indubitable" (article 7, alinéa a), doit être clarifiée davantage et interprétée de façon plus uniforme, surtout quand on la compare à la notion de "consentement explicite" dont question à l'article 8. Il est indispensable que les opérateurs sachent ce qu'est un consentement valable, en particulier en cas d'opérations en ligne.»

publicité comportementale en ligne où certains considèrent, mais pas d'autres, que les paramètres du navigateur de l'internaute expriment son consentement.

Il conviendrait donc de clarifier les conditions du consentement de la personne concernée, afin de garantir qu'il est toujours accordé en connaissance de cause, et de s'assurer que l'intéressé est pleinement conscient qu'il donne son autorisation et sait de quel traitement il s'agit, conformément à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. La clarification des notions clés peut également favoriser les initiatives en matière d'autoréglementation visant à dégager des solutions pratiques conformes au droit de l'Union.»

Afin de satisfaire la demande de contribution de la Commission et d'exécuter son programme de travail 2010-2011, le groupe de travail «Article 29» s'est engagé à rédiger un avis. Celui-ci a pour but de clarifier la situation afin de garantir une compréhension commune du cadre juridique existant. Dans le même temps, cet avis suit la logique des avis antérieurs sur d'autres dispositions essentielles de la directive[3]. Les modifications éventuelles du cadre existant prendront du temps, de sorte qu'une clarification de la notion actuelle de «consentement» et de ses principales caractéristiques présente un intérêt et des avantages intrinsèques. Cette clarification des dispositions existantes contribuera également à identifier les aspects à améliorer. Ainsi, sur la base de cette analyse, l'avis s'efforcera de formuler des recommandations afin d'aider la Commission et les décideurs au moment de modifier le cadre juridique applicable à la protection des données.

Le présent avis est structuré comme suit. Après un aperçu de la genèse législative et du rôle du consentement dans la législation relative à la protection des données, le groupe de travail analyse les différents éléments et conditions qui doivent être réunis afin qu'un consentement soit valable en vertu du droit applicable, et notamment de certaines parties pertinentes de la directive 2002/58/CE «vie privée et communications électroniques». L'analyse est illustrée par des exemples pratiques tirés des expériences nationales. Cet exercice étaye les recommandations énoncées dans la partie finale du présent avis, selon lesquelles certains éléments doivent être mis en place afin de demander et d'obtenir un consentement valable au sens de la directive. Le présent avis formule également des recommandations dont les décideurs pourront tenir compte dans le cadre de la révision de la directive 95/46/CE.

II. Observations générales et questions stratégiques

II.1. Bref historique

Si certaines législations nationales relatives à la protection des données ou à la vie privée adoptées dans les années 1970 considéraient le consentement comme l'un des fondements juridiques du traitement de données à caractère personnel[4], ce point de vue n'a pas trouvé d'écho dans la convention n° 108 du Conseil de l'Europe[5]. Aucune raison

[3] Comme l'avis 8/2010 sur le droit applicable, adopté le 16 décembre 2010 (WP 179), et l'avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant», adopté le 16 février 2010 (WP 169).

[4] Voir, par exemple, l'article 31 de la loi française n° 78-17 du 6 janvier 1973 relative à l'informatique, aux fichiers et aux libertés.

[5] La convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dénommée «Convention n° 108») est entrée en vigueur le 1er octobre 1985.

apparente n'empêche le consentement de jouer un rôle plus important dans la convention[6].

Au niveau de l'UE, dès le tout début du processus législatif ayant abouti à l'adoption de la directive 95/46/CE, il était prévu de subordonner la légitimité du traitement de données à caractère personnel au consentement de la personne concernée. En 1990, l'article 12 de la proposition de la Commission[7] énumérait les qualités que devait revêtir le consentement pour légitimer un traitement de données: il devait être «*donné expressément*» et «*spécifique*». L'article 17, portant sur les données sensibles, imposait que le consentement soit «*exprès et écrit*». La proposition modifiée de la Commission[8] de 1992 introduisait un libellé proche de la définition du consentement de la personne concernée de l'article 2, point h), actuel, qui remplace l'article 12 initial. Elle précisait que le consentement devait être «*libre et spécifique*». La référence à «*donné expressément*» avait été remplacée par un consentement en tant que «*manifestation expresse de sa volonté (de la personne concernée)*». L'exposé des motifs qui accompagnait la proposition modifiée de 1992[9] indiquait que le consentement pouvait être obtenu oralement ou par écrit. En 1992, la proposition modifiée de la Commission restructurait la proposition antérieure et introduisait un article 7 sur les fondements juridiques du traitement. L'article 7, point a), disposait que le traitement pouvait être effectué si «*la personne concernée y avait consenti*». La liste initiale comprenait, comme aujourd'hui, cinq fondements juridiques supplémentaires (en plus du consentement) pouvant servir à légitimer le traitement de données.

En 1995, la position commune du Conseil[10] a introduit la définition finale (actuelle) du consentement, à savoir «*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*». Le principal changement par rapport à la position de la Commission de 1992 consistait en la suppression du qualificatif «*expresse*» qui suivait le terme «*manifestation*». Parallèlement, le terme «*indubitablement*» a été ajouté à l'article 7, point a), de sorte qu'il se lit désormais comme suit: «*si la personne concernée a indubitablement donné son consentement*». L'exigence d'un consentement écrit pour les données sensibles a été remplacée par un «*consentement explicite*».

L'exposé des motifs du Conseil[11] n'expliquait pas précisément ces changements. Toutefois, à la page 4, on peut lire que «… *de nombreuses modifications … introduisent une certaine flexibilité; ces modifications, tout en garantissant un niveau équivalent de*

---

6 La convention n° 108 a introduit les notions de «traitement licite» et de «finalité légitime» (article 5), mais à la différence de la directive 95/46/CE, elle n'a pas dressé de liste de critères pour un traitement légitime des données. Le consentement de la personne concernée n'intervenait que dans le cadre de l'assistance mutuelle (article 15). Toutefois, l'obligation de «consentement» a été mentionnée à plusieurs reprises par la suite, dans diverses recommandations du Comité des ministres.

7 Proposition de directive du Conseil concernant la protection des données à caractère personnel et de la vie privée, COM(90) 314 final, SYN 287 et 288, Bruxelles, 13 septembre 1990.

8 Proposition modifiée de directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, COM(92) 422 FINAL, SYN 287, Bruxelles, 15 octobre 1992.

9 Voir la page 11 de la proposition modifiée de directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, COM(92) 422 FINAL, SYN 287, Bruxelles, 15 octobre 1992.

10 Position commune arrêtée par le Conseil le 15 mars 1995 sur la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (00/287) COD, adoptée le 15 mars 1995.

11 Voir la page 4 de la position commune.

protection… ne devraient pas conduire à abaisser le niveau de protection parce qu'elles permettent une application efficace et non bureaucratique des principes généraux posés en fonction de l'extrême variété des spécificités des traitements de données …».

Le rôle du consentement a été expressément reconnu dans la Charte des droits fondamentaux de l'UE en ce qui concerne la protection des données à caractère personnel. L'article 8, paragraphe 2, de cet instrument prévoit que les données à caractère personnel peuvent faire l'objet d'un traitement «*sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi*». Le consentement est donc reconnu comme un aspect essentiel du droit fondamental à la protection des données à caractère personnel. Parallèlement, le consentement inscrit dans la charte n'est pas le seul fondement juridique permettant le traitement de données à caractère personnel. En effet, la charte reconnaît explicitement que la loi peut prévoir d'autres fondements légitimes, comme dans le cas de la directive 95/46/CE.

En résumé, la genèse législative, notamment au sein de l'UE, montre que le consentement a joué un rôle majeur dans la conception de la protection des données et de la vie privée. Elle montre aussi que le consentement n'a pas été considéré comme le seul fondement juridique pouvant légitimer le traitement des données. La genèse de la directive 95/46/CE fait apparaître un consensus relatif sur les conditions d'un consentement valable, à savoir qu'il doit être *libre, spécifique et informé*. Cependant, elle met également en évidence un certain flou quant aux manières dont le consentement peut être exprimé: doit-il être explicite, écrit, etc. Cet aspect sera analysé ci-après.

II.2. Rôle du concept: condition de licéité

Condition générale/spécifique de licéité:

Dans la directive, le consentement est utilisé à la fois comme une condition générale de licéité (article 7) et comme une condition spécifique dans certains contextes particuliers [article 8, paragraphe 2, point a); article 26, paragraphe 1, point a)]. L'article 7 cite le consentement comme la première de six conditions différentes de légitimation du traitement des données à caractère personnel, tandis que l'article 8 prévoit la possibilité d'utiliser le consentement pour légitimer le traitement de catégories particulières de données (sensibles), qui, sans cela, serait interdit. Dans ce dernier cas, la condition d'obtention du consentement est plus stricte, dans la mesure où il doit aller plus loin que la condition générale d'octroi du consentement et être «explicite».

Par ailleurs, la directive autorise une interaction avec d'autres instruments législatifs, comme l'indique le considérant 23: «*les États membres sont habilités à assurer la mise en œuvre de la protection des personnes, tant par une loi générale relative à la protection des personnes à l'égard du traitement des données à caractère personnel que par des lois sectorielles*». Le fonctionnement pratique de ce système est complexe, les États membres ayant adopté leur propre approche, ce qui a parfois conduit à des divergences.

La notion du consentement n'a pas toujours été transposée littéralement au niveau national. À titre d'illustration, le consentement en tant que concept général n'est pas défini dans la loi française relative à la protection des données, mais sa signification a

été expliquée de manière précise et cohérente dans la jurisprudence de l'autorité chargée de la protection des données, la CNIL, par référence à la définition énoncée dans la directive relative à la protection des données. Au Royaume-Uni, cette notion a été développée par la *common law* par référence au libellé de la directive. En outre, le consentement a parfois été explicitement défini dans des secteurs spécifiques, comme dans le cadre de la vie privée et des communications électroniques, des services publics en ligne ou de la santé en ligne. La notion développée dans une législation spécifique va donc interagir avec celle développée dans la législation générale relative à la protection des données.

Le consentement est une notion également utilisée dans d'autres domaines du droit, en particulier dans le droit des contrats. Dans ce contexte, pour qu'un contrat soit valable, d'autres critères que ceux mentionnés dans la directive seront pris en compte, comme l'âge, l'influence indue, etc. Il n'y a pas contradiction, mais bien chevauchement, entre le champ d'application du droit civil et celui de la directive. En effet, la directive ne porte pas sur les conditions générales de validité d'un consentement dans le cadre du droit civil, mais elle ne les exclut pas. Cela signifie, par exemple, que pour apprécier la validité d'un contrat au regard de l'article 7, point b), de la directive, les conditions énoncées par le droit civil devront être prises en compte. Outre l'application des conditions générales de validité d'un consentement prévues par le droit civil, le consentement requis à l'article 7, point a), doit aussi être interprété en tenant compte de l'article 2, point h), de la directive.

Cette interaction avec d'autres instruments législatifs est non seulement visible au niveau national, mais aussi à l'échelon européen. Une compréhension similaire des éléments de la directive a été tirée d'autres contextes, comme le montre un arrêt de la Cour de justice dans le domaine du droit du travail[12], où un consentement était requis pour renoncer à un droit social. La Cour a interprété la notion de consentement à la lumière de la directive 93/104/CE concernant certains aspects de l'aménagement du temps de travail. Elle a déclaré que l'«accord du travailleur» requérait le consentement du travailleur (et non d'un syndicat au nom du travailleur) et entendait le terme «accord» (…) comme un consentement informé et librement exprimé. La Cour a également jugé que le travailleur qui signe un contrat de travail se référant à une convention collective qui permet un dépassement du temps de travail ne remplissait pas les conditions pour que le consentement soit explicitement et librement exprimé, en toute connaissance de cause. Cette interprétation du consentement dans un contexte spécifique est très proche du libellé de la directive 95/46/CE.

Le consentement n'est pas la seule condition de licéité

La directive présente clairement le consentement comme une condition de licéité. Or, certains États membres le considèrent comme une condition privilégiée, parfois proche d'un principe constitutionnel, liée au statut de droit fondamental de la protection des données. D'autres peuvent le considérer comme une des six options possibles, à savoir une condition opérationnelle qui ne revêt pas plus d'importance que les autres options. Afin d'éclairer le rôle du consentement dans des cas spécifiques, il est utile de préciser le rapport entre le consentement et d'autres conditions de licéité, notamment par rapport

[12] Arrêt de la Cour (grande chambre) du 5 octobre 2004 dans les affaires jointes C-397/01 à C-403/01, Pfeiffer, Roith, Süß, Winter, Nestvogel, Zeller et Döbele.

aux contrats, aux missions d'intérêt public ou à l'intérêt légitime du responsable du traitement et au droit de s'opposer au traitement.

L'ordre dans lequel les fondements juridiques sont cités à l'article 7 est important, mais il ne signifie pas que le consentement soit toujours le fondement le plus approprié pour légitimer le traitement de données à caractère personnel. L'article 7 mentionne d'abord le consentement et poursuit en énumérant les autres fondements juridiques, comme les contrats et les obligations légales, avant de passer progressivement à l'équilibre des intérêts. Il y a lieu d'observer que les cinq fondements qui suivent le consentement imposent un critère de «nécessité», qui limite strictement le contexte dans lequel ils peuvent s'appliquer. Cela ne signifie nullement que l'obligation de consentement laisse davantage de marge de manœuvre que les autres fondements cités à l'article 7.

En outre, l'obtention d'un consentement n'annule pas les obligations imposées au responsable du traitement par l'article 6 en termes d'équité, de nécessité, de proportionnalité ainsi que de qualité des données. Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de l'utilisateur, cela ne justifie pas la collecte de données excessives au regard d'une fin particulière.

L'obtention d'un consentement n'autorise pas davantage le contournement d'autres dispositions, telles que l'article 8, paragraphe 5. Ce n'est que dans des circonstances très restreintes que le consentement peut légitimer des traitements de données qui auraient été interdits autrement, notamment dans le cas du traitement de certaines données sensibles (article 8) ou pour permettre le traitement ultérieur de données à caractère personnel, que celui-ci soit ou non compatible avec la finalité spécifiée à l'origine. En principe, le consentement ne doit pas être considéré comme une dérogation à d'autres principes applicables à la protection des données, mais bien comme une garantie. Il s'agit en premier lieu d'une condition de licéité et non d'une renonciation à l'application d'autres principes.

Le choix du fondement juridique le plus approprié n'est pas toujours évident, en particulier entre les points a) et b) de l'article 7. En vertu de l'article 7, point b), le traitement doit être nécessaire à l'exécution d'un contrat ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée, et rien de plus. Un responsable du traitement se fondant sur l'article 7, point b), dans le cadre de la conclusion d'un contrat ne peut en faire un usage extensif pour justifier le traitement de données au-delà de ce qui est nécessaire; pour ce faire, il devra justifier le traitement supplémentaire par un consentement spécifique auquel les exigences de l'article 7, point a), s'appliqueront. Cela souligne la nécessité d'une grande précision dans les termes du contrat. Dans la pratique, il peut être ainsi nécessaire d'obtenir un consentement à titre de condition supplémentaire pour une partie du traitement. Soit le traitement est nécessaire à l'exécution d'un contrat, soit un consentement (libre) doit être obtenu.

Dans certaines transactions, plusieurs fondements juridiques pourraient s'appliquer en même temps. En d'autres termes, tout traitement de données doit, à tout instant, être conforme à un ou plusieurs fondements juridiques. Cela n'exclut pas le recours simultané à plusieurs fondements, pour autant qu'ils soient utilisés à bon escient. Certaines collectes de données et certains traitements ultérieurs peuvent être nécessaires en application du contrat passé avec la personne concernée – article 7, point b); un autre

traitement peut être rendu nécessaire par une obligation légale – article 7, point c); la collecte d'informations supplémentaires peut nécessiter un consentement distinct – article 7, point a); un autre traitement encore pourrait aussi être légitime en raison de l'équilibre des intérêts – article 7, point f).

Exemple: l'achat d'une voiture
Le responsable du traitement peut être habilité à traiter des données à caractère personnel à différentes fins et sur la base de différents motifs:
- les données sont nécessaires à l'achat de la voiture: article 7, point b);
- pour traiter les documents du véhicule: article 7, point c);
- pour les services de gestion de la clientèle (par exemple, pour l'entretien du véhicule dans différentes entreprises du même groupe au sein de l'UE): article 7, point f);
- pour transférer les données à des tiers aux fins de leurs propres activités de commercialisation: article 7, point a).

II.3. Notions connexes

Contrôle

La notion de consentement est traditionnellement associée à l'idée que la personne concernée doit pouvoir contrôler l'utilisation qui est faite de ses données. Du point de vue des droits fondamentaux, le contrôle exercé par le biais du consentement est une notion importante. En même temps, la décision d'une personne d'accepter le traitement de données devrait être régie par des conditions strictes, compte tenu notamment du fait qu'en prenant cette décision, la personne pourrait renoncer à un droit fondamental.

Bien que le consentement confère un pouvoir de contrôle aux personnes concernées, il ne s'agit pas de l'unique possibilité à cet égard. La directive prévoit d'autres moyens de contrôle, en particulier le droit d'opposition, mais ce droit est un instrument différent s'exerçant à un autre stade du traitement, à savoir une fois que celui-ci a débuté et sur la base d'un fondement juridique distinct.

Le consentement est lié à la notion de libre choix en matière d'informations. L'autonomie de la personne concernée est à la fois une condition préalable et une conséquence du consentement. En effet, elle permet à la personne concernée d'influencer le traitement des données. Cependant, ainsi que le montrera la section suivante, ce principe comporte des limites, et il existe des cas où la personne concernée n'est pas en mesure de véritablement décider. Le responsable du traitement peut vouloir se servir du consentement de la personne concernée pour se décharger de sa responsabilité sur celle-ci. Ainsi, en consentant à la publication de données personnelles sur l'internet ou à un transfert vers une entité douteuse établie dans un pays tiers, la personne concernée peut être lésée et le responsable du traitement peut alors arguer qu'il s'agit seulement de ce à quoi la personne concernée avait consenti. Il importe donc de rappeler qu'un consentement parfaitement valable n'exonère pas le responsable du traitement de ses obligations et ne légitime pas un traitement qui aurait, sans cela, été considéré comme déloyal au sens de l'article 6 de la directive.

La notion de contrôle est également liée au fait que la personne concernée doit être en mesure de retirer son consentement. Le retrait n'est pas rétroactif, mais il devrait, en principe, empêcher tout traitement ultérieur des données de la personne par le responsable du traitement. Le fonctionnement pratique de ce principe sera examiné ci-après (section III).

Transparence

Un deuxième aspect du consentement concerne l'information, c'est-à-dire la transparence vis-à-vis de la personne concernée. La transparence est une condition du contrôle du traitement et est nécessaire pour que le consentement soit valable. La transparence ne suffit pas, en soi, pour légitimer le traitement de données à caractère personnel, mais elle est une condition essentielle pour garantir que le consentement est valable.

Pour être valable, le consentement doit être informé. Ceci implique que toutes les informations nécessaires doivent être données au moment de la demande du consentement et que ces informations doivent couvrir tous les aspects de fond du traitement que le consentement est censé légitimer. Cela couvre normalement les informations énumérées à l'article 10 de la directive, mais cela dépendra également du moment et des circonstances dans lesquelles le consentement est demandé.

Indépendamment du fait que le consentement soit accordé ou non, la transparence du traitement des données est également une condition de loyauté, qui a une valeur propre, même après la fourniture de l'information initiale.

Modalités/moment: manières de signifier le consentement

Cette troisième dimension du consentement se rapporte à la manière dont le contrôle est exercé. Comment le consentement est-il exprimé et quand doit-il être demandé pour garantir qu'il s'agit d'un consentement véritable? Ces questions sont déterminantes pour la manière dont le consentement est exercé et interprété.

Bien que la directive ne précise pas le moment où le consentement doit être demandé, il ressort clairement du libellé des différentes dispositions qu'en règle générale, le consentement doit être donné avant le début du traitement[13]. L'obtention du consentement avant le début du traitement des données est une condition essentielle pour légitimer ledit traitement. Cet aspect est analysé plus avant à la section III.B relative à la directive «vie privée et communications électroniques».

Le consentement, entendu comme l'autorisation donnée par une personne physique de traiter les données la concernant, peut être signifié de différentes manières. Ainsi, l'article 2, point h), mentionne une «manifestation de volonté», qui doit être «indubitable» [article 7, point a)] et explicite pour les données sensibles (article 8). Néanmoins, il est essentiel de souligner que le consentement diffère du droit d'opposition prévu à l'article 14. Alors qu'à l'article 7, point a), le responsable du traitement ne peut traiter les données tant qu'il n'a pas obtenu le consentement de la

[13] À titre d'exemple, la version allemande de la directive (et la loi fédérale allemande sur la protection des données) utilise la notion de «Einwilligung». Cette notion est définie dans le code civil allemand comme une «acceptation préalable».

personne concernée, à l'article 7, point f), il peut traiter les données sous réserve de certaines conditions et garanties, aussi longtemps que la personne concernée ne s'y est pas opposée. Ainsi que l'indiquait le document de travail 114 du groupe de travail: «*L'importance du fait que le consentement soit un acte positif exclut de facto tout système par lequel la personne concernée n'aurait le droit de s'opposer au transfert qu'après qu'il a eu lieu*»[14].

C'est pourquoi le droit d'opposition prévu à l'article 14 de la directive ne doit pas être confondu avec le consentement. Ce dernier est un fondement juridique du traitement de données à caractère personnel en vertu de l'article 7, point a), de l'article 8, paragraphe 2, point a), et de l'article 26, paragraphe 1, ou de diverses dispositions de la directive 2002/58/CE.

II.4. Utilisation adéquate du consentement comme base juridique

Il convient de souligner que le consentement n'est pas toujours le moyen principal ni le plus indiqué de légitimer le traitement de données à caractère personnel.

Le consentement constitue parfois une base insuffisante pour justifier le traitement de données à caractère personnel et il perd de sa valeur lorsqu'on en fait un usage extensif ou restrictif afin de le faire correspondre à des situations pour lesquelles il n'était nullement prévu. Il est capital que le consentement soit utilisé «à bon escient». Son utilisation dans des cas inappropriés, parce qu'il est peu probable que les éléments constitutifs d'un consentement valable soient réunis, peut aboutir à une grande vulnérabilité et risque, dans la pratique, d'*affaiblir* la position des personnes concernées.

Le groupe de travail et le CEPD ont déjà soutenu cette approche dans leurs contributions aux discussions sur le nouveau cadre de la protection des données. En particulier, il a été indiqué qu'«*[i]l n'est cependant pas toujours simple de déterminer ce qui constitue un consentement authentique, non équivoque. Certains responsables du traitement exploitent cette incertitude en recourant à des méthodes qui excluent toute possibilité de donner un consentement véritable, non équivoque*»[15], en violation des conditions visées à l'article 6 de la directive. Dans le même ordre d'idées, le groupe de travail «Article 29» a observé que «*la complexité des pratiques de collecte des données, des modèles commerciaux, des relations entre fournisseurs et des applications technologiques dépassent, bien souvent, la capacité ou la volonté d'une personne de décider, par un choix actif, de contrôler l'utilisation et le partage d'informations*»[16].

Il est donc essentiel de préciser les limites du consentement et de s'assurer que seul un consentement conforme au droit est considéré comme tel[17].

---

14 WP 114 – Document de travail du groupe de travail «Article 29» relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995.

15 Avis du contrôleur européen de la protection des données du 14 janvier 2011 sur la communication de la Commission «Une approche globale de la protection des données à caractère personnel dans l'Union européenne».

16 «L'avenir de la protection de la vie privée – Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel», 1er décembre 2009, WP 168.

17 Avis du contrôleur de la protection des données du 14 janvier 2011, op. cit.

III. Analyse des dispositions

Dans la présente analyse, la section III.A porte principalement sur la directive 95/46/CE. Certaines parties pertinentes de la directive 2002/58/CE (vie privée et communications électroniques) seront analysées à la section III.B. Il est à noter que les directives ne s'excluent pas mutuellement. Les conditions générales d'un consentement valable, prévues par la directive 95/46/CE, s'appliquent à la fois à l'environnement en ligne et hors ligne. La directive 2002/58/CE précise ces conditions pour certains services en ligne expressément identifiés, mais toujours à la lumière des conditions générales de la directive relative à la protection des données.

III.A Directive 95/46/CE

La notion de «consentement de la personne concernée» est définie à l'article 2, point h), et est ensuite utilisée dans les articles 7, 8 et 26. Le rôle du consentement est également mentionné aux considérants 30 et 45. Ces dispositions et tous les aspects pertinents seront abordés séparément dans la présente section.

III.A.1. Article 2, point h)

Conformément à l'article 2, point h), on entend par «consentement de la personne concernée» «*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*». Cette définition comporte plusieurs éléments clés qui seront examinés ci-après.

«… toute manifestation de volonté par laquelle la personne concernée accepte»

En principe, il n'existe pas de limitations quant à la forme que peut revêtir un consentement. Toutefois, pour être valable au sens de la directive, le consentement doit consister en une manifestation de volonté. Même s'il peut s'agir de «toute» forme de manifestation, il convient de savoir précisément ce qui peut relever de la définition d'une manifestation de volonté.

La forme de la manifestation de volonté (c'est-à-dire la manière dont la volonté est signifiée) n'est pas définie par la directive. Pour des raisons de souplesse, le consentement «écrit» n'a pas été inscrit dans la version finale. Il y a lieu de souligner que la directive prévoit «toute» manifestation de volonté. Cela permet d'interpréter plus largement la portée d'une telle manifestation. L'expression minimale d'une manifestation de volonté pourrait être tout type de signe, suffisamment clair pour permettre d'exprimer la volonté d'une personne concernée et être compris par le responsable du traitement. Les termes «manifestation de volonté» et «accepte» indiquent qu'une action est effectivement nécessaire (à l'inverse d'une situation où le consentement pourrait être déduit d'une absence d'action).

Le consentement devrait comprendre toute manifestation de volonté par laquelle la personne concernée *accepte* le traitement. Cela pourrait inclure une signature manuscrite apposée au bas d'un formulaire papier, mais aussi une déclaration orale pour marquer un accord ou un comportement dont on peut raisonnablement déduire un accord. Au-delà de l'exemple classique d'une signature, déposer une carte de visite dans une urne

pourrait donc correspondre à la définition. Il en est de même si une personne envoie son nom et son adresse à une organisation pour lui demander des informations. Dans ce cas, son action doit être comprise comme une acceptation du traitement de ces données dans la mesure où elles sont nécessaires pour traiter la demande et y répondre.

Dans son avis sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée (WP 115), le groupe de travail a évalué la manière dont les personnes physiques devraient être mises en mesure de consentir à des services nécessitant leur localisation automatique (comme la possibilité de former un numéro spécifique pour obtenir des informations météorologiques concernant le lieu où elles se trouvent). Dans ce cas, il a été admis que, pour autant que les utilisateurs soient pleinement informés au préalable du traitement de leurs données de localisation, le fait d'appeler le numéro correspondant équivaudrait à accepter d'être localisé.

Exemple: les panneaux publicitaires Bluetooth
Un nouvel outil publicitaire est actuellement en cours de développement. Il s'agit de panneaux qui envoient des messages demandant l'établissement d'une connexion Bluetooth pour envoyer ensuite des publicités aux personnes qui passent à proximité. Les messages sont envoyés aux personnes ayant activé la fonction Bluetooth de leur téléphone portable. L'activation de la fonction Bluetooth ne constitue pas à elle seule un consentement valable (en effet, la fonction Bluetooth peut être activée à d'autres fins). En revanche, lorsqu'une personne est informée du service et s'approche à quelques centimètres du panneau avec son portable, il s'agit bel et bien d'une manifestation de volonté: cela montre que la personne est réellement intéressée par les publicités. C'est uniquement dans ce cas que les personnes doivent être réputées avoir consenti, et elles seules devraient recevoir des messages sur leur téléphone.

On peut se demander si l'absence de comportement – ou encore un comportement passif – pourraient également être interprétés comme une manifestation de volonté dans des circonstances très précises (c'est-à-dire dans un contexte totalement dénué d'ambiguïté). La notion de «manifestation de volonté» est large, mais elle semble impliquer nécessairement une action. D'autres éléments de la définition du consentement et l'exigence supplémentaire de l'article 7, point a) (caractère indubitable du consentement), corroborent cette interprétation. L'exigence selon laquelle la personne concernée doit «donner» son consentement semble indiquer qu'une simple absence d'action est insuffisante et qu'une action quelconque est nécessaire pour constituer un consentement, bien que différents types d'action, à apprécier «selon le contexte», soient possibles.

Dans la pratique, en l'absence de comportement actif de la personne concernée, il sera difficile pour le responsable du traitement de savoir si ce silence a effectivement valeur d'acceptation ou de consentement. Ainsi, un responsable du traitement peut ne pas savoir avec la certitude nécessaire s'il y a bel et bien consentement dans le cas suivant. Imaginons une situation dans laquelle, après avoir envoyé une lettre à des clients les informant qu'un transfert de leurs données est envisagé à moins qu'ils ne s'y opposent dans les deux semaines, seuls 10 % des clients répondent. Dans ce cas, il est douteux que les 90 % de clients qui n'ont pas répondu soient effectivement d'accord avec le transfert. En pareils cas, le responsable du traitement n'obtient pas de manifestation

claire de la volonté des personnes concernées. En outre, il n'aura pas de preuve et sera donc dans l'incapacité de démontrer qu'il a obtenu un consentement. Dans la pratique, une réponse passive, du fait de son ambiguïté, permet difficilement de satisfaire aux exigences imposées par la directive.

«[manifestation de volonté]… libre …»

Le consentement ne peut être valable que si la personne concernée est véritablement en mesure d'exercer un choix et s'il n'y a pas de risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement. Si les conséquences du consentement sapent la liberté de choix des personnes, le consentement n'est pas libre. La directive prévoit, à son article 8, paragraphe 2, point a), que, dans certains cas à déterminer par les États membres, l'interdiction du traitement de catégories particulières de données à caractère personnel ne peut être levée par le consentement de la personne concernée.

C'est le cas, par exemple, lorsque la personne concernée est sous l'influence du responsable du traitement, dans le cadre d'une relation de travail, notamment. Dans ce cas, même s'il n'en est pas nécessairement toujours ainsi, la personne concernée peut se trouver dans une situation de dépendance vis-à-vis du responsable du traitement – en raison de la nature de la relation ou de circonstances particulières – et peut craindre d'être traitée différemment si elle n'accepte pas le traitement de ses données.

Dans plusieurs de ses avis, le groupe de travail a étudié les limites du consentement dans des situations où il ne peut être donné librement. C'était notamment le cas des avis sur les dossiers médicaux électroniques (WP 131), le traitement des données à caractère personnel dans le contexte professionnel (WP 48) et le traitement des données par l'Agence mondiale antidopage (WP 162).

Dans le WP 131, le groupe de travail a indiqué que «*le consentement libre désigne une décision volontaire, prise par une personne en pleine possession de ses facultés, en l'absence de toute coercition, qu'elle soit sociale, financière, psychologique ou autre. Un consentement donné sous la menace de privation de traitement ou de traitement de moindre qualité dans une situation médicale ne saurait être considéré comme libre. (...) lorsque la situation médicale exige nécessairement et inévitablement que le praticien de la santé traite des données à caractère personnel dans un système DME, il est trompeur que ce praticien cherche à légitimer ce traitement par le consentement. Le recours au consentement doit être limité aux cas où la personne concernée est véritablement libre de son choix et a la possibilité de retirer ultérieurement son consentement sans subir de préjudice.*»[18].

Si, une fois le consentement retiré, le traitement de données se poursuit sur la base d'un autre fondement juridique, des doutes pourraient naître au sujet de l'utilisation première du consentement en tant que fondement juridique initial. En effet, si le traitement pouvait être effectué dès le début sur la base de cet autre fondement, on pourrait considérer qu'il est trompeur ou intrinsèquement déloyal de présenter les choses à

[18] Le WP 162 sur l'AMA parvient à la même conclusion: «*Les sanctions et les conséquences liées à un éventuel refus des participants de se soumettre aux obligations du code (par exemple, la communication d'informations sur leur localisation) ne permettent pas au groupe de considérer que le consentement est, d'une manière ou d'une autre, donné librement*».

l'intéressé comme si le traitement était subordonné à son consentement. Ce serait différent si les circonstances avaient changé, par exemple si une nouvelle base juridique devait apparaître pendant le traitement, comme une nouvelle loi régissant la base de données concernée. Si ce nouveau fondement peut valablement s'appliquer au traitement de données, ce dernier peut se poursuivre. Toutefois, dans la pratique, ces cas ne sont guère fréquents. En principe, on considère un consentement comme défaillant lorsqu'aucun retrait effectif n'est autorisé.

Le groupe de travail a adopté une approche cohérente en ce qui concerne l'interprétation d'un consentement libre dans le contexte professionnel[19]: «*si le consentement du travailleur est nécessaire et que l'absence de consentement peut entraîner un préjudice réel ou potentiel pour le travailleur, le consentement n'est pas valable au titre de l'article 7 ou de l'article 8, dans la mesure où il n'est pas donné librement. … Si le travailleur n'a pas la possibilité de refuser, il ne s'agit pas de consentement. … Une pierre d'achoppement peut exister si le consentement est une condition d'emploi. Le travailleur peut, en théorie, refuser de donner son consentement, mais il peut perdre alors une opportunité d'emploi. Dans ces circonstances, le consentement n'étant pas donné librement, n'est donc pas valable. La situation est encore plus claire, comme c'est souvent le cas, lorsque tous les employeurs imposent des conditions d'emploi identiques ou similaires.*»

Exemple: les photographies publiées sur les intranets

Comme l'illustre l'exemple suivant, un consentement peut néanmoins être parfaitement valable dans le contexte professionnel. Une entreprise décide de créer un intranet qui précise le nom et la fonction principale des différents membres de son personnel. Chaque membre du personnel doit indiquer s'il souhaite ou non qu'une photographie de lui apparaisse à côté de son nom. Dans l'affirmative, il est invité à en envoyer une à une adresse donnée. À partir du moment où la personne a été dûment informée, l'envoi d'une photographie sera considéré comme un consentement. Si l'entreprise dispose déjà d'une photographie numérique de chaque membre de son personnel et demande à chacun d'entre eux son consentement pour la mettre en ligne sur l'intranet, chaque personne qui cliquera sur un bouton pour marquer son accord sera également réputée avoir donné un consentement valable. Dans les deux cas, le libre choix des membres du personnel quant à la mise en ligne de leur photographie sur l'intranet est pleinement respecté.

Le contexte professionnel requiert une discussion distincte. Les aspects culturels et sociaux de la relation de travail jouent un rôle, tout comme la manière dont les principes applicables à la protection des données interagissent avec d'autres législations. Dans le contexte professionnel, des données à caractère personnel peuvent être traitées à différentes fins:

- données nécessaires au salarié pour exécuter ses tâches: application de l'article 7, point b) – traitement nécessaire à l'exécution d'un contrat;

[19] WP 48 sur le traitement des données à caractère personnel dans le contexte professionnel. Le WP 114 – Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, est également pertinent.

- pour déterminer le droit des salariés à obtenir des options d'achat d'actions (stock options): cela pourrait soit reposer sur un consentement [article 7, point a)], soit être considéré comme inhérent aux aspects administratifs de la relation de travail contractuelle [article 7, point b)];
- traitement du numéro de sécurité sociale à des fins de protection sociale: article 7, point c) – obligation légale, voire article 8, paragraphe 2, point b) – obligations en matière de droit du travail;
- traitement de données à caractère ethnique: dans certains pays, cela pourrait également constituer une obligation imposée par le droit du travail [article 8, paragraphe 2, point b)], tandis que dans d'autres, cela serait strictement interdit.

Bien que tout porte à croire que le consentement n'est guère solide en pareils cas, cela n'exclut pas complètement son utilisation, à condition qu'il existe des garanties suffisantes que le consentement est véritablement libre.

Alors qu'un rapport de subordination est souvent la principale raison qui empêche un consentement d'être libre, d'autres éléments contextuels peuvent influencer la décision de la personne concernée. Ces éléments peuvent, par exemple, être de nature financière, affective ou pratique. Le fait que la collecte de données soit réalisée par une autorité publique peut également avoir une influence sur la personne concernée. Néanmoins, il peut se révéler difficile d'établir une distinction entre une simple incitation et un élément qui influence véritablement la liberté de choix de la personne concernée. Les exemples qui suivent tentent d'illustrer la différence de nature des efforts ou des coûts susceptibles d'influencer la décision des personnes concernées.

Exemple: les dossiers médicaux électroniques
Dans de nombreux États membres, la tendance est à la création d'un résumé électronique du dossier médical des patients, l'idée étant de permettre aux prestataires de soins de santé d'accéder aux informations essentielles chaque fois que le patient a besoin d'un traitement.
- Dans la première hypothèse, la création du résumé du dossier médical est absolument volontaire et le patient reçoit toujours le traitement, qu'il ait ou non consenti à la création du résumé. Dans ce cas, le consentement est librement donné parce que le patient ne subit pas de préjudice s'il refuse de le donner ou s'il le retire.
- Dans la deuxième hypothèse, il existe une incitation financière modérée à opter pour le dossier médical électronique. Les patients qui le refusent ne subissent pas de préjudice en ce sens que les coûts ne changent pas pour eux. Dans ce cas aussi, on pourrait considérer que les patients sont libres d'accepter ou non le nouveau système.
- Dans la troisième hypothèse, les patients qui refusent le système de santé en ligne (télésanté) doivent payer des frais supplémentaires considérables par rapport au système tarifaire antérieur et le traitement de leur dossier est fortement retardé. Ces inconvénients manifestes pour les personnes qui refusent de donner leur consentement visent à amener toute la population à adhérer au système de santé en ligne dans un délai fixé. Le consentement n'est donc pas suffisamment libre. Il conviendrait dès lors d'examiner s'il existe d'autres motifs légitimes de traiter les données à caractère personnel ou si l'article 8, paragraphe 3, de la directive 95/46/CE s'applique ou non.

Exemple: les scanners corporels
L'utilisation des scanners corporels est de plus en plus fréquente dans certains lieux publics, en particulier dans les aéroports pour accéder à la zone d'embarquement. Compte tenu du fait que les données des passagers sont traitées au moment où le scannage a lieu[20], le traitement doit respecter l'un des fondements juridiques visés à l'article 7. Le passage dans un scanner personnel est parfois présenté comme une option pour les passagers, laissant entendre que le traitement pourrait être justifié par leur consentement. Toutefois, le refus de passer dans un scanner corporel pourrait éveiller les soupçons ou provoquer des contrôles supplémentaires, comme une fouille corporelle. De nombreux passagers consentiront à passer dans un scanner afin d'éviter tout problème ou retard potentiel, leur priorité étant de monter à bord de leur avion à temps. Ce consentement n'est pas suffisamment libre. Étant donné qu'il doit être démontré que le traitement est nécessaire (pour des raisons de sécurité publique), la base légitime ne devrait pas être l'article 7, point a), mais bien un acte législatif – article 7, point c) ou e) – imposant une obligation de coopération aux passagers. La base juridique du contrôle par un scanner corporel devrait donc être la législation. Celle-ci pourrait toujours prévoir un choix entre le scannage et une fouille corporelle; néanmoins, ce choix ne serait proposé à l'intéressé qu'à titre complémentaire, dans le cadre de mesures additionnelles.

La nature du responsable du traitement peut également être déterminante pour le choix du fondement juridique régissant le traitement de données à caractère personnel. Cela vaut en particulier pour les responsables du traitement dans le secteur public, où le traitement de données est normalement lié à l'exécution d'une obligation légale au sens de l'article 7, point c), ou à l'exécution d'une mission d'intérêt public au sens de l'article 7, point e). En conséquence, le recours au consentement de la personne concernée pour légitimer le traitement de données ne constitue pas la base juridique adéquate. Cela est particulièrement clair dans le cas du traitement de données à caractère personnel par des pouvoirs publics investis d'une autorité – tels que les autorités répressives dans l'exercice de leurs fonctions policières ou judiciaires. Les autorités policières ne peuvent, en effet, se prévaloir du consentement de la personne concernée pour prendre des mesures qui n'ont pas été prévues ou qui ne seraient pas autrement autorisées par la loi.

Il y a toutefois lieu de reconnaître que même si les États peuvent être légalement tenus de traiter des données à caractère personnel, l'intéressé n'est pas toujours tenu de collaborer. Il peut y avoir des cas où des «services à valeur ajoutée» sont fournis aux personnes concernées, qui peuvent décider d'y recourir ou non. Cependant, dans la plupart des cas, le traitement est effectivement obligatoire. Il est souvent assez difficile de déterminer si le traitement de données à caractère personnel par des pouvoirs publics repose légitimement sur le consentement de la personne concernée. Le traitement de données à caractère personnel dans le secteur public implique donc souvent des systèmes hybrides, ce qui peut créer une insécurité juridique et engendrer des abus si le consentement est invoqué à tort pour légitimer le traitement.

[20] Voir la lettre du 11 février 2009 du président du groupe de travail «Article 29» à l'attention de M. Daniel CALLEJA CRESPO, directeur de la DG TREN, sur les scanners corporels, en réponse à la consultation lancée par la Commission sur «l'impact de l'utilisation de scanners corporels dans le domaine de la sûreté aérienne sur les droits de l'homme, la vie privée, la dignité de la personne, la santé et la protection des données». Disponible sur: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm (en anglais).

Si le consentement peut, dans des cas exceptionnels, constituer un fondement valable pour le traitement de données à caractère personnel par les États, il importe de procéder à un contrôle approfondi au cas par cas afin d'apprécier si le consentement est bel et bien suffisamment libre. Comme l'illustre l'exemple suivant, lorsqu'une autorité publique est responsable du traitement, le fondement juridique légitimant le traitement sera le respect d'une obligation légale en vertu de l'article 7, point c), ou l'exécution d'une mission d'intérêt public en vertu de l'article 7, point e), plutôt que le consentement.

Exemple: les services publics en ligne

Les États membres développent actuellement de nouvelles cartes d'identité dotées de fonctions électroniques contenues dans une puce. L'activation des services électroniques de la carte ne peut être obligatoire. Cependant, sans cette activation, l'usager pourrait ne pas avoir accès à certains services administratifs, qui seraient autrement très difficiles à joindre (transfert de certains services en ligne, réduction des heures d'ouverture des bureaux). Le consentement ne saurait être invoqué comme fondement légitime pour justifier le traitement. Dans ce cas, c'est la loi régissant le développement des services publics en ligne, assortie de toutes les garanties appropriées, qui devrait être la base juridique pertinente.

Exemple: les données PNR

La question de savoir si le consentement des passagers peut être valablement invoqué pour légitimer le transfert des données de réservation («données PNR») par les compagnies aériennes européennes aux autorités américaines a été examinée. Le groupe de travail estime que le consentement des passagers ne peut pas être donné librement, car les compagnies aériennes sont tenues d'envoyer les données avant le décollage et les passagers n'ont donc pas réellement le choix s'ils veulent prendre leur vol[21]. En l'espèce, la base juridique n'est pas le consentement du passager, mais bien, conformément à l'article 7, point c), les obligations découlant de l'accord international conclu entre l'UE et les États-Unis sur le traitement et le transfert des données des dossiers passagers (données PNR).

Exemple: les recensements nationaux

Lors d'un recensement national, la population est invitée à répondre à diverses questions sur sa situation personnelle et professionnelle. Il est obligatoire d'y répondre. En outre, le recensement comprend également une question, dont la réponse est clairement signalée comme facultative, qui porte sur les moyens de transport utilisés par la personne. Bien qu'il n'y ait certainement pas de consentement libre pour la majeure partie du recensement, cette dernière question facultative offre un vrai choix. Cela ne doit toutefois pas masquer le fait que l'objectif principal de l'État qui adresse ce questionnaire est d'obtenir des réponses. En règle générale, le consentement ne constitue pas un fondement valable dans ce contexte.

[21] Voir avis 6/2002 du groupe de travail «Article 29» sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis.

«[manifestation de volonté]… spécifique …»

Pour être valable, le consentement doit être spécifique. En d'autres termes, un consentement général, sans préciser la finalité exacte du traitement, n'est pas acceptable.

Pour être spécifique, le consentement doit être intelligible. Il doit mentionner, de façon claire et précise, l'étendue et les conséquences du traitement des données. Il ne peut pas s'appliquer à un ensemble illimité d'activités de traitement. En d'autres termes, le contexte dans lequel le consentement s'applique est limité.

Le consentement doit être donné sur les différents aspects, clairement définis, du traitement. Il couvre notamment les données qui sont traitées et les finalités pour lesquelles elles le sont. Cette compréhension doit reposer sur les attentes raisonnables des parties. Un «consentement spécifique» est dès lors intrinsèquement lié au fait que le consentement doit être informé. Il existe une obligation de «détail» du consentement par rapport aux différents éléments qui constituent le traitement de données. En effet, il ne saurait être considéré comme couvrant «toutes les finalités légitimes» poursuivies par le responsable du traitement. Le consentement devrait renvoyer au traitement qui est raisonnable et nécessaire compte tenu de sa finalité.

En principe, il devrait suffire que les responsables du traitement obtiennent un consentement unique pour les différentes opérations, si celles-ci relèvent des attentes raisonnables de la personne concernée.

La Cour de justice de l'Union européenne a récemment rendu une décision préjudicielle[22] sur l'article 12, paragraphe 2, de la directive «vie privée et communications électroniques» en ce qui concerne la nécessité du renouvellement du consentement des abonnés qui ont déjà consenti à la publication de leurs données personnelles dans un annuaire, afin que celles-ci soient transférées en vue de leur publication par d'autres services d'annuaire. La Cour a jugé que, dès lors que l'abonné a été correctement informé de la possible transmission des données à caractère personnel le concernant à une entreprise tierce et que celui-ci a consenti à la publication desdites données dans un tel annuaire, la transmission de ces données n'exige pas de nouveau consentement de la part de l'abonné, *s'il est garanti que les données concernées ne seront pas utilisées à des fins autres que celles pour lesquelles elles ont été collectées en vue de leur première publication (point 65 des motifs).*

Un consentement distinct peut néanmoins être nécessaire lorsque le responsable du traitement a l'intention de traiter les données à d'autres fins. Par exemple, un consentement pourrait être donné pour couvrir à la fois des informations sur de nouveaux produits et des actions promotionnelles spécifiques, étant donné que cela pourrait être considéré comme relevant des attentes raisonnables de la personne concernée. En revanche, un consentement distinct et supplémentaire devrait être demandé pour autoriser la transmission des données de la personne concernée à des

[22] Arrêt de la Cour du 5 mai 2001 dans l'affaire C-543/09, Deutsche Telekom AG. Cette affaire repose sur une demande de décision préjudicielle introduite par le Tribunal administratif fédéral allemand concernant les annuaires de télécommunications et, en particulier, l'interprétation à donner à l'article 25, paragraphe 2, de la directive concernant le service universel (2002/22/CE) et à l'article 12, paragraphe 2, de la directive «vie privée et communications électroniques» (2002/58/CE). Cet arrêt est clairement lié au rôle particulier des annuaires dans la directive concernant le service universel.

tiers. Il convient d'évaluer au cas par cas la nécessité de «détailler» le consentement, en fonction de la ou des finalités envisagées ou des destinataires des données.

Il y a lieu de rappeler que le traitement pourrait reposer sur plusieurs fondements juridiques différents: certaines données pourraient être traitées parce qu'elles sont nécessaires à l'exécution d'un contrat passé avec la personne concernée, comme dans le cas de la réalisation d'un produit et de la gestion d'un service, tandis qu'un consentement spécifique pourrait être requis pour le traitement allant au-delà de ce qui est nécessaire à l'exécution du contrat, par exemple pour évaluer les capacités de paiement (évaluation de la solvabilité) de la personne concernée.

Le groupe de travail a clarifié cet aspect du consentement dans le WP 131 sur les dossiers médicaux électroniques (DME): un consentement «spécifique» doit se rapporter à une situation concrète et bien définie dans laquelle le traitement de données médicales est envisagé. Par conséquent, un «accord général» de la personne concernée – par exemple, concernant la collecte de ses données médicales en vue de la création d'un DME et toute transmission future de ces données médicales à des professionnels de la santé impliqués dans le traitement – ne constituerait pas un consentement au sens de l'article 2, point h), de la directive.

Le même raisonnement est suivi dans le WP 115 sur l'utilisation de données de localisation aux fins de la fourniture de services à valeur ajoutée: «*[cette] définition exclut expressément que le consentement de la personne fasse partie de l'acceptation des conditions générales du service de communications électroniques proposé. … Néanmoins, selon la nature du service proposé, le consentement peut porter sur une opération ponctuelle de localisation ou sur l'acceptation d'une localisation continue.*»

Dans la décision de la Cour citée à la section II sous l'intitulé «Rôle du consentement», même si le terme «spécifique» n'est pas expressément employé, le raisonnement insiste également sur la nécessité que le consentement soit spécifique lorsque la Cour déclare qu'«*il ne suffit pas que le contrat de travail de l'intéressé se réfère à une convention collective qui permet un tel dépassement*».

Exemple: les réseaux sociaux
L'accès aux services d'un réseau social est souvent subordonné à l'acceptation de différents types de traitement de données à caractère personnel.

L'utilisateur peut être invité à accepter de recevoir de la publicité comportementale pour pouvoir s'inscrire sur un réseau social, sans autre précision ni autre possibilité. Compte tenu de l'importance qu'ont pris certains réseaux sociaux, certaines catégories d'utilisateurs (comme les adolescents) consentiront à recevoir de la publicité comportementale pour éviter le risque d'être exclus de certaines interactions sociales. Or l'utilisateur devrait être en mesure de donner un consentement libre et spécifique à la réception de publicités comportementales, indépendamment de son accès au réseau social. Une fenêtre distincte pourrait être utilisée pour proposer cette possibilité à l'utilisateur.

Le réseau social offre la possibilité d'utiliser des applications externes. Dans la pratique, il est fréquent que l'utilisateur ne puisse pas utiliser une application s'il n'accepte pas la transmission de ses données au développeur de l'application à différentes fins, y compris la publicité comportementale et la revente à des tiers. Étant donné que l'application peut fonctionner sans qu'il soit nécessaire de transférer des données à son développeur, le groupe de travail recommande de «détailler» le consentement de l'utilisateur, c'est-à-dire de lui demander un consentement distinct pour la transmission de ses données au développeur à ces différentes fins. Divers dispositifs, comme des fenêtres contextuelles, pourraient être utilisés pour proposer à l'utilisateur la possibilité de sélectionner l'utilisation des données à laquelle il consent (transmission au développeur, services à valeur ajoutée, publicité comportementale, transmission à des tiers, etc.).

La spécificité du consentement signifie également que si les finalités du traitement de données par le responsable du traitement changent à un moment donné, l'utilisateur doit en être informé et être mis en mesure de consentir à ou aux nouvelles finalités du traitement. Les informations fournies doivent, notamment, expliquer les conséquences entraînées par un refus des changements proposés.

«[manifestation de volonté]… informée …»

Le dernier élément de la définition du consentement – mais pas la dernière exigence, ainsi que nous le verrons plus loin – est qu'il doit être informé.

Les articles 10 et 11 de la directive imposent l'obligation de fournir des informations aux personnes concernées. L'obligation d'information est donc distincte du consentement, bien qu'elle y soit, dans de nombreux cas, manifestement liée. Si le consentement ne suit pas toujours la fourniture des informations (un autre fondement prévu à l'article 7 peut être utilisé), l'information doit toujours précéder le consentement.

Dans la pratique, cela signifie qu'«*un consentement … doit être fondé sur l'appréciation et la compréhension des faits et des conséquences d'une action. La personne concernée doit recevoir, de façon claire et compréhensible, des informations exactes et complètes sur tous les éléments pertinents, en particulier ceux spécifiés aux articles 10 et 11 de la directive, tels que la nature des données traitées, les finalités du traitement, les destinataires d'éventuels transferts et ses droits. Cela suppose également la connaissance des conséquences du refus de consentir au traitement des données en question*»[23].

Bien souvent, le consentement sera obtenu au moment de la collecte des données à caractère personnel, lorsque le traitement commence. Dans ce cas, les informations à fournir sont celles qui sont énumérées à l'article 10 de la directive. Toutefois, le consentement peut également être demandé «en aval», lorsque la finalité du traitement change. Dans ce cas, les informations à fournir devront essentiellement porter sur ce qui est nécessaire dans ce cas particulier, compte tenu de la finalité du traitement.

[23] WP 131 – Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME).

Un consentement informé est particulièrement décisif dans le cas de la transmission de données à caractère personnel vers des pays tiers: «*elle requiert que la personne concernée soit correctement informée du risque spécifique que les données la concernant soient transférées vers un pays n'assurant pas une protection adéquate*»[24].

Deux types d'exigences pouvant garantir la fourniture d'informations appropriées peuvent être citées:

- la qualité des informations: la manière dont les informations sont communiquées (texte en clair, sans jargon, compréhensible, visible) est capitale pour apprécier si le consentement est «informé». La manière dont les informations doivent être fournies dépend du contexte. Un utilisateur régulier/moyen devrait être en mesure de les comprendre;

- l'accessibilité et la visibilité des informations: les informations doivent être communiquées directement à la personne concernée. Il ne suffit pas que les informations soient «disponibles» quelque part. La Cour de justice a insisté sur ce point dans son arrêt de 2004[25] relatif à un contrat de travail contenant des conditions qui n'étaient pas énoncées dans le contrat proprement dit, mais auxquelles il était fait référence. Les informations doivent être bien visibles (type et taille de la police de caractères), mises en évidence et complètes. Des boîtes de dialogue peuvent être utilisées pour fournir des informations spécifiques au moment où le consentement est demandé. Comme indiqué précédemment au sujet du caractère «spécifique» du consentement, des outils d'information en ligne sont particulièrement utiles dans le domaine des réseaux sociaux pour détailler et clarifier suffisamment les paramètres de confidentialité. Les avis superposés peuvent également se révéler utiles à cet égard, en ce qu'ils contribuent à fournir les informations requises de façon aisément accessible.

Au fil du temps, des doutes peuvent survenir quant à la question de savoir si le consentement initialement fondé sur des informations valides et suffisantes reste valable. Les gens changent souvent d'avis pour diverses raisons, parce que leur choix initial a été opéré sans y prendre garde ou parce que les circonstances ont changé, comme un enfant qui grandit et gagne en maturité[26]. C'est la raison pour laquelle, à titre de bonne pratique, les responsables du traitement devraient s'efforcer de réexaminer, au bout d'un certain temps, le choix d'une personne, en l'informant par exemple de son choix actuel et en lui offrant la possibilité de le confirmer ou de l'infirmer[27]. La fréquence dépendrait naturellement du contexte et des circonstances de chaque cas particulier.

---

[24] WP 12 – Document de travail – Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données. Voir aussi le WP 114 – Document de travail du groupe de travail «Article 29» relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995.

[25] Voir la note de bas de page n° 12 (section II.2).

[26] Document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant, WP 147, 18 février 2008.

[27] Le groupe de travail «Article 29» a formulé une recommandation similaire dans son avis 171 sur la publicité comportementale en ligne, adopté le 22 juin 2010.

Exemple: la cartographie de la criminalité
Certains services de police envisagent actuellement de publier des cartes, ou de divulguer d'autres données, indiquant où certains types d'infractions ont été commis. En règle générale, les garanties prévues à cet égard empêchent la publication de données à caractère personnel concernant les victimes, car les infractions ne sont reliées qu'à des régions géographiques relativement vastes. Cependant, certaines autorités policières souhaitent localiser plus précisément les infractions, lorsque les victimes y consentent. Dans ce cas, il devient possible d'établir un lien plus précis entre la personne concernée et le lieu de l'infraction. Pourtant, la victime n'est pas informée clairement que des informations susceptibles de permettre son identification seront publiées sur l'internet ou de la manière dont ces informations peuvent être utilisées. Le consentement n'est donc pas valable dans ce cas parce que les victimes ne peuvent pas prendre toute la mesure de la publication des données les concernant.

Plus le traitement de données est complexe, plus on est en droit d'attendre des informations précises de la part du responsable du traitement. Plus il est difficile pour un citoyen moyen de surveiller le traitement des données le concernant et d'en comprendre les tenants et aboutissants, plus grands devraient être les efforts déployés par le responsable du traitement pour démontrer que le consentement a été obtenu sur la base d'informations spécifiques et compréhensibles.

La définition du consentement énoncée à l'article 2, point h), devrait être lue en combinaison avec les autres exigences mentionnées plus loin dans le dispositif de la directive. L'article 7 ajoute le terme «indubitable» aux éléments de la définition, tandis que l'article 8 y ajoute le terme «explicite» lorsque le traitement concerne des catégories particulières de données.

III.A.2. Article 7, point a)

Conformément à l'article 7, point a), de la directive, le consentement indubitable de la personne concernée constitue la base juridique du traitement de données à caractère personnel. Pour être valable, outre les critères énoncés à l'article 2, point h), le consentement doit donc également être *indubitable*.

Pour qu'un consentement soit indubitable, la procédure relative à l'obtention et à l'octroi du consentement ne doit laisser *aucun doute* quant à l'intention de la personne concernée de donner son consentement. En d'autres termes, la manifestation de volonté par laquelle la personne concernée marque son accord ne doit laisser aucune ambiguïté quant à son intention. S'il existe un doute raisonnable sur l'intention de la personne concernée, il y a ambiguïté.

Ainsi qu'elle est décrite plus en détail ci-après, cette exigence oblige les responsables du traitement à mettre en place des procédures solides pour que les personnes concernées donnent leur consentement, à savoir soit demander un consentement exprès et clair, soit recourir à certains types de procédures qui aboutissent à un consentement implicite clair des personnes concernées. Le responsable du traitement doit également être suffisamment sûr que la personne qui donne son consentement est bel et bien la

personne concernée. Cela vaut en particulier lorsque le consentement est donné par téléphone ou en ligne.

Une question connexe est celle de la preuve du consentement. Les responsables du traitement qui se fondent sur un consentement peuvent souhaiter ou devoir démontrer que le consentement a été obtenu, par exemple en cas de litige avec la personne concernée. En effet, ils peuvent parfois être amenés à produire de telles preuves dans le cadre d'actions répressives. Par conséquent et à titre de bonne pratique, les responsables du traitement devraient établir et conserver les preuves attestant que le consentement a effectivement été donné; en d'autres termes, le consentement devrait être vérifiable.

Nous allons à présent analyser les modes de consentement suivants et examiner s'ils permettent de donner un consentement indubitable.

Des déclarations expresses pour marquer un accord, comme un accord signé ou une déclaration écrite attestant la volonté de consentir sont des procédures ou des mécanismes qui se prêtent bien à la fourniture d'un consentement indubitable. Dans le même temps, ces mécanismes fournissent, en principe, au responsable du traitement la preuve que le consentement a bien été obtenu.

Exemple: le consentement à la réception par courrier d'informations sur des actions promotionnelles
Un hôtel demande à ses clients d'indiquer leur adresse postale sur un formulaire s'ils souhaitent être informés de ses actions promotionnelles par courrier. Si le client, après avoir inscrit son adresse postale, signe le formulaire pour marquer son accord, cela constitue un consentement indubitable. Dans ce cas, le consentement sera à la fois exprès et écrit. Cette procédure confère au responsable du traitement une preuve suffisante du fait qu'il a obtenu le consentement de tous les clients, dès lors qu'il conserve tous les formulaires signés.

Cependant, tous les formulaires de consentement qui peuvent paraître explicites n'aboutissent pas forcément à un consentement. Cette question a été examinée dans une récente affaire de la Cour de justice (Volker und Markus Schecke GbR/Land de Hesse), qui concernait la publication des noms des bénéficiaires de différents Fonds de l'UE[28] et des montants reçus par chaque bénéficiaire. L'avocat général s'est penché sur la question de savoir si les conditions d'un consentement indubitable étaient satisfaites dans le cas où des personnes avaient signé une déclaration contenant la mention suivante: «Je reconnais avoir pris connaissance du fait que l'article 44 bis du règlement (CE) n° 1290/2005 impose la publication d'informations relatives aux bénéficiaires du FEAGA et du FEADER ainsi qu'aux montants reçus par chaque bénéficiaire». L'avocat général a conclu comme suit: «*L'information préalable selon laquelle on prend acte qu'une publication quelconque interviendra n'est pas la même chose que le fait de consentir "indubitablement" à un certain type de publication détaillée. On ne peut davantage la décrire comme une "manifestation libre [et] spécifique [de la] volonté" des requérantes, conformément à la définition du consentement de la personne concernée qui figure à l'article 2, sous h)*». L'avocat général en a donc conclu que les demandeurs n'avaient pas donné leur consentement au

[28] Fonds européen agricole de garantie (FEAGA) et Fonds européen agricole pour le développement rural (FEADER).

traitement (c'est-à-dire à la publication) de leurs données à caractère personnel au sens de l'article 7, point a), de la directive 95/46/CE[29].

Un consentement exprès peut également être donné dans l'environnement en ligne. Comme dans l'environnement hors ligne, il existe des moyens tout à fait adaptés de donner un consentement indubitable, comme l'illustre l'exemple suivant.

Exemple: le consentement en ligne à l'inscription à un programme de fidélité
Le site internet d'un hôtel comprend un formulaire de réservation qui permet de réserver des chambres en ligne. Le formulaire en ligne dans lequel les clients saisissent les dates souhaitées et les informations relatives au paiement contient également une case bien visible, que doivent cocher les personnes qui souhaitent que leurs données soient utilisées à des fins d'inscription à un programme de fidélité. Le fait de cocher la case après avoir reçu les informations pertinentes constitue un consentement exprès et indubitable, car l'action de cocher la case est suffisamment claire pour ne pas laisser de doute quant à la volonté de la personne de s'inscrire au programme de fidélité.

Un consentement exprès peut également être donné oralement, par le biais d'une déclaration destinée à marquer un accord. Un consentement oral exprès serait, par exemple, donné dans la situation suivante.

Exemple: le consentement oral à la réception d'informations promotionnelles
Lors du paiement de la note d'hôtel, le réceptionniste demande aux clients s'ils souhaitent donner leur adresse afin que l'hôtel puisse leur envoyer des informations sur ses actions promotionnelles. Les personnes qui répondent par l'affirmative en donnant leur adresse postale, après avoir reçu les informations pertinentes, donnent un consentement exprès. Si l'action de communiquer son adresse peut constituer une manifestation sans équivoque de la volonté d'une personne, le responsable du traitement peut aussi décider de mettre en place des mécanismes afin de prouver d'une manière plus fiable qu'un consentement a été donné.

Dans certains cas, un consentement indubitable peut être *déduit* de certaines actions; c'est notamment le cas lorsque ces actions conduisent à la conclusion indubitable qu'un consentement a été donné. Cela dépend toutefois des informations pertinentes, relatives au traitement des données, qui ont été fournies à la personne et lui ont permis de prendre sa décision (identité du responsable du traitement, finalités du traitement, etc.).

[29] Conclusions de l'avocat général Sharpston présentées le 17 juin 2010 dans les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke GbR. Il convient de noter que la Cour a déclaré, dans son arrêt du 9 novembre 2010, que le traitement des données ne reposait pas sur un consentement: «*63. La réglementation de l'Union en cause, qui se borne à prévoir que les bénéficiaires d'aides seront informés au préalable de la publication des données les concernant, ne cherche donc pas à fonder le traitement de données à caractère personnel qu'elle instaure sur le consentement des bénéficiaires concernés.*»

Exemple: le consentement en matière de photographie
Lors de l'enregistrement dans un hôtel, le réceptionniste informe les clients qu'une séance photo aura lieu dans l'une des cafétérias de l'hôtel durant l'après-midi, les images sélectionnées devant être utilisées pour du matériel promotionnel, notamment des brochures sur l'hôtel. Les clients souhaitant être pris en photo sont invités à se rendre à la cafétéria aux heures indiquées, une autre cafétéria restant disponible pour les personnes qui ne souhaitent pas être photographiées.

On peut dès lors considérer que les clients de l'hôtel qui, après avoir été informés, décident de se rendre à la cafétéria durant les heures de la séance photo ont accepté d'être photographiés. Leur consentement est déduit de leur action de se rendre à la cafétéria où se déroule la séance photo. Le fait de se rendre à la cafétéria constitue une manifestation de la volonté de la personne qui peut, en principe, être considérée comme indubitable, étant donné qu'il n'y a guère de doute que la personne qui se rend à la cafétéria souhaite être photographiée. Toutefois, l'hôtel peut juger prudent de disposer d'une preuve documentaire du consentement, dans le cas où la validité de ce consentement viendrait à être contestée ultérieurement.

Comme indiqué plus haut, les mêmes exigences, dont le consentement indubitable, s'appliquent aux environnements hors ligne et en ligne. Le groupe de travail constate néanmoins que le risque de consentement ambigu est probablement plus élevé dans l'environnement en ligne et que cet aspect mérite une attention particulière. Dans l'exemple suivant, le consentement déduit de l'action de participer à un jeu en ligne ne satisfait pas aux conditions qui doivent être remplies pour que le consentement soit valable.

Exemple: les jeux en ligne
Un fournisseur de jeux en ligne demande aux joueurs d'indiquer leur âge, leur nom et leur adresse pour participer à un jeu en ligne (répartition des joueurs par âge et par adresse). Le site internet contient un avis, accessible via un lien (mais l'accès à cet avis n'est pas nécessaire pour participer au jeu), qui mentionne qu'en utilisant ce site internet (et, partant, en fournissant des informations), les joueurs consentent à ce que leurs données soient traitées en vue de recevoir des informations promotionnelles de la part du fournisseur de jeux en ligne et de tiers.

Or l'accès et la participation au jeu n'équivalent pas à donner un consentement indubitable au traitement ultérieur de données personnelles à des fins autres que la participation au jeu elle-même. Cette dernière ne suppose pas, en effet, l'intention de la personne de consentir à un traitement allant au-delà de ce qui est nécessaire pour jouer. Ce type de comportement ne constitue donc pas une manifestation indubitable de la volonté d'une personne de voir ses données utilisées à des fins commerciales.

Exemple: les paramètres de confidentialité par défaut
Les paramètres par défaut d'un réseau social, auxquels les utilisateurs ne doivent pas nécessairement accéder pour l'utiliser, permettent à l'ensemble de la catégorie «amis d'amis» de rendre toutes les informations personnelles de chaque utilisateur visibles par tous les «amis d'amis». Les utilisateurs qui ne souhaitent pas que leurs informations soient vues par les «amis d'amis» doivent cliquer sur un bouton. S'ils restent passifs ou manquent d'effectuer l'action consistant à cliquer sur ce bouton, le responsable du traitement considère qu'ils ont consenti à ce que leurs données soient visibles. Or il est très douteux que le fait de *ne pas* cliquer sur ce bouton signifie que les personnes dans leur ensemble *consentent* à rendre leurs informations visibles par tous les amis d'amis. Du fait de l'incertitude liée à la question de savoir si l'absence d'action doit être comprise comme un consentement, le fait de ne pas cliquer ne peut pas être considéré comme un consentement indubitable.

L'exemple ci-dessus illustre le cas où l'intéressé reste passif (par exemple, en cas d'absence d'action ou de «silence»). Un consentement indubitable ne cadre pas bien avec les procédures d'obtention d'un consentement reposant sur l'inaction ou le silence des personnes concernées. En effet, le silence ou l'inaction d'une partie comporte une ambiguïté intrinsèque (la personne concernée pourrait avoir voulu donner son accord ou pourrait simplement avoir voulu ne pas exécuter l'action). L'exemple suivant en est une nouvelle illustration.

Il y a ambiguïté lorsque des personnes sont réputées avoir donné leur consentement lorsqu'elles n'ont pas répondu à une lettre les informant que l'absence de réponse vaut consentement. Dans ce type de situation, le comportement de la personne (ou plutôt son absence d'action) soulève de sérieux doutes sur le fait que la personne ait voulu marquer son accord. Le fait que la personne n'ait pas effectué d'action positive ne permet pas de conclure qu'elle a donné son consentement. Par conséquence, l'exigence de consentement indubitable ne sera pas satisfaite. En outre, comme illustré ci-dessous, il sera très difficile au responsable du traitement de prouver que la personne a effectivement donné son consentement.

Le groupe de travail a déclaré qu'un consentement fondé sur le silence de la personne est inadéquat dans le contexte de l'envoi de courriers électroniques à des fins de prospection directe. «*Un consentement présumé à recevoir des messages électroniques n'est pas non plus conforme à la définition du consentement de la directive 95/46/CE … Dans le même ordre d'idées, les cases pré-cochées, par exemple sur des sites web, ne sont pas davantage compatibles avec la définition de la directive*»[30]. L'exemple suivant le confirme.

[30] Avis 5/2004 portant sur les communications de prospection directe non sollicitées selon l'article 13 de la directive 2002/58/CE, adopté le 27 février 2004 (WP 90).

Exemple: le consentement non valable aux utilisations ultérieures des données des clients
Un détaillant de livres en ligne envoie un courriel aux clients faisant partie de son programme de fidélité afin de les informer que leurs données vont être transmises à une entreprise publicitaire qui envisage de les utiliser à des fins commerciales. Les utilisateurs disposent de deux semaines pour répondre à ce courriel. Ils sont informés qu'en cas d'absence de réponse, ils seront réputés avoir consenti à la transmission. Ce type de mécanisme, par lequel le consentement est déduit de l'absence de réaction des personnes concernées, n'aboutit pas à un consentement valable et indubitable. En effet, il n'est pas possible de déduire, avec certitude, de leur absence de réponse que les personnes ont accepté la transmission de leurs données.

Il découle de ce qui précède que, du fait de l'exigence que le consentement soit *indubitable*, les responsables du traitement sont de facto encouragés à mettre en place des procédures et des mécanismes ne laissant aucun doute sur l'octroi du consentement, que ce soit par une action explicite de la personne concernée ou par une déduction claire d'une action effectuée par la personne concernée.

Comme indiqué ci-dessus, à titre de bonne pratique, les responsables du traitement devraient envisager de mettre en œuvre des mesures et des procédures prouvant qu'un consentement a été donné. Plus l'environnement dans lequel ils sont actifs est complexe, plus des mesures seront nécessaires pour garantir que le consentement est vérifiable. Cette information devrait être mise à la disposition de l'autorité chargée de la protection des données sur demande.

III.A.3. Article 8, paragraphe 2, point a)

L'article 8 de la directive prévoit une protection spéciale pour des «*catégories particulières de données*» qui, par leur nature, sont considérées comme très sensibles. Le traitement de ces données est interdit sauf si au moins une des dérogations prévues s'applique. L'article 8, paragraphe 2, point a), précise que cette interdiction ne s'applique pas si la personne concernée a donné son *consentement explicite* au traitement.

En droit, l'expression «consentement explicite» a le même sens que «consentement exprès». Le consentement explicite couvre toutes les situations où il est proposé à une personne d'accepter ou de rejeter une utilisation particulière ou la divulgation des informations la concernant et qu'elle répond activement à la question, que ce soit oralement ou par écrit. En règle générale, un consentement explicite ou exprès est donné par écrit et est attesté par une signature manuscrite. Ainsi, un consentement explicite est donné lorsque la personne concernée signe un formulaire de consentement qui explique clairement pourquoi un responsable du traitement souhaite collecter et traiter ultérieurement des données à caractère personnel.

Bien qu'un consentement explicite soit traditionnellement donné par écrit, sur papier ou sous forme électronique, comme illustré ci-dessus à la section III.A.2, cela ne doit pas nécessairement être le cas: il peut également être donné oralement, ce que confirme la suppression, dans la version finale de la directive, de l'exigence que le consentement

visé à l'article 8 soit écrit. Toutefois, comme l'a montré cette même section, un consentement oral peut être difficile à prouver et, dans la pratique, il est donc recommandé aux responsables du traitement de recourir à un consentement écrit pour des raisons de preuve.

L'exigence d'un consentement explicite signifie qu'un consentement qui est déduit ne satisfera normalement pas à la condition imposée par l'article 8, paragraphe 2. À cet égard, il convient de rappeler l'avis du groupe de travail «Article 29» sur les dossiers médicaux électroniques[31], qui mentionne que «*[c]ontrairement aux dispositions de l'article 7 de la directive, le consentement dans le cas de données à caractère personnel sensibles, et donc d'un DME, doit être* ***explicite****. Les solutions qui prévoient un droit de refus ne remplissent pas le critère du caractère "explicite" …*»

Exemple: les données médicales destinées à la recherche
Le cas d'un patient qui est informé par une clinique que son dossier médical va être transmis à un chercheur à moins qu'il ne s'y oppose (en appelant un numéro de téléphone) ne satisfera pas à l'exigence d'un consentement explicite.

Comme indiqué ci-dessus à la section II.A.2, les personnes peuvent donner un consentement explicite, oralement et aussi par écrit, en effectuant une action positive pour exprimer leur souhait d'accepter une forme de traitement des données. Dans un environnement en ligne, un consentement explicite peut être donné au moyen d'une signature électronique ou numérique. Il peut, toutefois, être également donné en cliquant sur des boutons, selon le contexte, en envoyant un courriel de confirmation, en cliquant sur des icônes, etc.[32]. L'acceptation de procédures impliquant une action positive de la personne est expressément reconnue au considérant 17 de la directive «vie privée et communications électroniques», qui mentionne que «*[l]e consentement peut être donné selon toute modalité appropriée permettant à l'utilisateur d'indiquer ses souhaits librement, de manière spécifique et informée, y compris en cochant une case lorsqu'il visite un site Internet*».

Pour être valable, le consentement ne doit pas être enregistrable. Toutefois, il est dans l'intérêt du responsable du traitement d'en conserver des preuves. Il va de soi que la qualité des preuves peut varier d'un mécanisme à l'autre et que le consentement peut être plus ou moins bien démontré. Un consentement obtenu au moyen d'un bouton cliquable et où l'identité de la personne ne consiste qu'en une adresse électronique aura une valeur probante nettement moindre qu'une procédure similaire étayée, par exemple, par un mécanisme de consentement enregistrable[33]. La nécessité de disposer de preuves

31 WP 131 – Document de travail sur le traitement des données à caractère personnel relatives à la santé contenues dans les dossiers médicaux électroniques (DME).

32 Cette interprétation est conforme à la législation de l'UE sur le commerce électronique et sur l'utilisation plus large des signatures numériques, essentiellement, qui a imposé aux États membres de modifier leur législation nationale contenant des exigences formelles de documents «écrits» et «manuscrits», de sorte que leurs équivalents électroniques soient également acceptés sous réserve de certaines conditions.

33 À cet égard, voir, par exemple, la législation grecque et la législation allemande concernant les exigences liées à l'octroi d'un consentement par des moyens électroniques, qui imposent que le consentement soit enregistré de manière sûre et que l'utilisateur ou l'abonné ait la possibilité d'y accéder et de le révoquer à tout moment (article 5, paragraphe 3, de la loi grecque n° 3471/2006 sur la protection des données à caractère personnel dans le secteur des communications électroniques; article 13, paragraphe 2, de la loi allemande sur les téléservices, article 94 de la loi allemande sur les télécommunications et article 28, paragraphe 3, point a), de la loi fédérale allemande sur la protection des données).

solides dépendra également de la nature des données collectées et de la finalité poursuivie. En effet, une signature électronique ne sera pas nécessaire pour consentir à recevoir des offres commerciales, mais pourra l'être pour consentir au traitement de certains types de données financières en ligne. Un consentement explicite donné dans un environnement en ligne devra être enregistrable de manière à être accessible et à pouvoir servir de référence ultérieurement[34].

Eu égard à ce qui précède, les formulaires d'inscription en ligne que les personnes physiques doivent remplir pour s'identifier et consentir au traitement de données les concernant seront réputés satisfaire à l'exigence de consentement explicite pour autant que toutes les autres conditions soient satisfaites. Ainsi, pour ouvrir un dossier médical personnel en ligne, les patients peuvent donner leur consentement en communiquant leurs coordonnées et en cochant une case spécifique pour marquer leur accord. Le recours à des méthodes d'authentification plus strictes – par exemple, l'utilisation de signatures numériques – donnera naturellement le même résultat et constituera une preuve plus solide[35].

Dans certains cas, les États membres peuvent décider de subordonner un traitement de données particulier au consentement de l'intéressé et préciser le type de consentement requis. Ainsi, pour demander une carte de santé donnant accès aux antécédents médicaux, les États membres peuvent décider que les personnes physiques qui s'inscrivent en ligne doivent signer au moyen d'une signature numérique particulière. Cette option garantira le caractère exprès du consentement et permettra au responsable du traitement d'être plus à même de prouver le consentement de la personne concernée.

III.A.4. Article 26, paragraphe 1

L'article 26, paragraphe 1, point a), exige le consentement indubitable de la personne concernée pour déroger à l'interdiction de transférer des données vers des pays tiers n'assurant pas un niveau de protection adéquat. Les considérations exposées ci-dessus au sujet de l'article 7, point a), s'appliquent ici également. En d'autres termes, outre les conditions nécessaires à un consentement valable énoncées à l'article 2, point h), le consentement doit être également indubitable.

Le groupe de travail «Article 29» a déployé beaucoup d'énergie pour fournir des orientations en ce qui concerne l'application des articles 25 et 26 de la directive, y compris la dérogation en cas consentement de la personne concernée. Dans ce contexte, il convient de rappeler le document WP 12 du groupe de travail[36] sur la signification du consentement indubitable: «*Le consentement devant être donné de manière indubitable, tout doute sur le fait qu'il a bien été donné rendrait également la dérogation inapplicable. Cela signifiera vraisemblablement que de nombreuses situations où le*

[34] L'analyse des spécifications techniques que doivent remplir les documents électroniques et les signatures numériques pour se voir accorder une valeur probante équivalente à leurs équivalents manuscrits ne relève pas du champ d'application du présent avis. Cette question va au-delà de la législation en matière de protection des données et de ce qui est couvert par la réglementation de l'UE.

[35] En effet, certains types de signatures numériques (signatures électroniques avancées fondées sur un certificat qualifié et générées par un appareil de création de signatures sécurisées) sont automatiquement présumés avoir la même valeur probante en droit que des signatures manuscrites.

[36] WP 12 – Document de travail – Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données, adopté le 24 juillet 1998.

consentement est implicite (par exemple, parce qu'une personne a eu connaissance d'un transfert, sans s'y opposer) ne pourront pas être couvertes par cette dérogation».

Compte tenu de ce qui précède, il est plus probable d'obtenir un consentement indubitable lorsque les intéressés effectuent une action positive pour marquer leur accord au transfert, par exemple, en signant un formulaire de consentement ou en accomplissant d'autres actions qui étayent indéniablement la conclusion qu'un consentement a été donné.

Dans le WP 114[37], en ce qui concerne l'utilisation du consentement aux fins des transferts de données, le groupe de travail a déclaré que «*le consentement n'est pas susceptible de fournir un cadre adéquat à long terme pour les responsables du traitement, en cas de transferts répétitifs ou même structurels pour le traitement en question. De fait, et en particulier si le transfert fait partie intrinsèque du traitement principal (par exemple, la centralisation d'une base de données mondiale de ressources humaines, dont le fonctionnement nécessite des transferts de données permanents et systématiques), les responsables du traitement risqueraient de se trouver eux-mêmes dans des situations insolubles si ne fût-ce qu'une personne concernée par le transfert décidait ultérieurement de retirer son consentement. Les données concernant une personne ayant retiré son consentement ne pourraient plus stricto sensu faire l'objet d'un transfert; à défaut, le transfert resterait partiellement fondé sur le consentement de personnes concernées, mais une solution de remplacement (contrat, règles d'entreprises contraignantes, etc.) devrait être trouvée pour les données des personnes ayant retiré leur consentement. Le recours au consentement peut donc se révéler être une "fausse bonne solution", simple de prime abord, mais en réalité complexe et lourde à gérer.*»

II.A.5. <u>Consentement donné par des personnes physiques ne jouissant pas de la pleine capacité juridique</u>

Aux termes de la directive 95/46/CE, il n'existe pas de règle particulière régissant l'obtention du consentement des personnes physiques ne jouissant pas de la pleine capacité juridique, comme les enfants. Il est important que cette réalité soit prise en compte dans le cadre de la révision de la directive relative à la protection des données. Outre les questions soulevées ci-dessus, le consentement de ces personnes pose des problèmes spécifiques.

S'agissant des enfants, les conditions d'un consentement valable varient d'un État membre à l'autre. Le groupe de travail «Article 29» s'est penché, à plusieurs reprises, sur la question du consentement des enfants et sur les pratiques nationales en vigueur[38].

Il ressort des travaux passés que lorsque le consentement d'un enfant est recherché, les exigences légales peuvent imposer l'obtention du consentement de l'enfant et de son tuteur légal ou le consentement du seul enfant, s'il est déjà mûr. Les âges auxquels l'une

[37] Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, adopté le 25 novembre 2005.

[38] WP 147 – Document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles). WP 160 – Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles).

ou l'autre règle s'applique varient. Il n'existe pas de procédure harmonisée pour contrôler l'âge d'un enfant.

L'absence de règles générales en la matière aboutit à une approche fragmentée et ne reconnaît pas la nécessité d'une protection spécifique de l'enfant dans certaines circonstances, en raison de sa vulnérabilité, et parce qu'elle crée une insécurité juridique, notamment en ce qui concerne la manière dont le consentement de l'enfant est obtenu.

Le groupe de travail est d'avis que cette absence d'harmonisation a des conséquences sur la sécurité juridique. En effet, l'harmonisation des conditions permettant à des personnes incapables d'exercer leurs droits au niveau de l'UE, en particulier en ce qui concerne l'âge minimum, apporterait certainement des garanties supplémentaires. Le groupe de travail est toutefois conscient que cela peut largement dépasser le champ d'application de la protection des données, dans la mesure où cela concerne plus généralement des aspects du droit civil. Le groupe de travail attire l'attention de la Commission sur les défis soulevés par cette question.

Par ailleurs, le groupe de travail «Article 29» estime que l'intérêt de l'enfant et d'autres personnes ne jouissant pas de la pleine capacité juridique serait mieux protégé si la directive contenait des dispositions supplémentaires visant spécifiquement la collecte et le traitement ultérieur de leurs données. Ces dispositions pourraient prévoir les circonstances dans lesquelles le consentement du tuteur légal est requis, en plus ou au lieu du consentement de la personne incapable, ainsi que les cas où il ne devrait pas être possible d'utiliser le consentement pour légitimer le traitement de données à caractère personnel. Il conviendrait également de rendre obligatoire l'utilisation de mécanismes de contrôle en ligne de l'âge. Il existe actuellement des mécanismes et des âges minimums différents. Par exemple, plutôt que d'appliquer une règle unique, la vérification de l'âge pourrait être fondée sur une «échelle mobile», le mécanisme à utiliser dépendant des circonstances, telles que la nature du traitement (ses finalités), les risques, le type de données collectées, les utilisations envisagées (divulgation ou non des données), etc.

III.B. Directive 2002/58/CE

La directive «vie privée et communications électroniques» (directive 2002/58/CE)[39], qui a été récemment modifiée, est une *lex specialis* par rapport à la directive 95/46/CE, dans la mesure où elle propose un régime spécifique de protection de la vie privée dans le secteur des communications électroniques. La plupart de ses dispositions ne s'appliquent qu'aux fournisseurs de services de communications électroniques accessibles au public (par exemple, les fournisseurs de services de téléphonie, les fournisseurs de services internet, etc.).

Dans certaines dispositions de la directive «vie privée et communications électroniques», le consentement sert de base juridique au traitement de données par les

[39] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, 18.12.2009.

fournisseurs de services de communications électroniques accessibles au public[40]. Tel est notamment le cas de l'utilisation des données relatives au trafic ou de localisation.

Le groupe de travail «Article 29» juge utile d'examiner certains aspects, présentant un intérêt particulier, de l'utilisation du consentement en vertu de la directive «vie privée et communications électroniques». À cet effet, les cinq questions suivantes seront analysées:

a) le rapport entre la directive 95/46/CE et la directive «vie privée et communications électroniques» en ce qui concerne la définition et le sens général du consentement. Cette question se rapporte à l'article 2, paragraphe 2, point f), de la directive «vie privée et communications électroniques»;

b) la question de savoir si, pour rompre la confidentialité des communications (par exemple, pour surveiller ou intercepter une communication téléphonique), il est nécessaire d'obtenir le consentement de l'une ou des deux parties à la communication. Cette question est régie par l'article 6, paragraphe 3, et par l'article 5, paragraphe 1;

c) la question du moment où le consentement doit être obtenu. Cet aspect est abordé dans plusieurs dispositions de la directive «vie privée et communications électroniques», notamment son article 5, paragraphe 3, et ses articles 6 et 13;

d) le champ d'application du droit d'opposition et en quoi il se distingue du consentement. Cette distinction peut être analysée à la lumière de l'article 13 de la directive «vie privée et communications électroniques»;

e) la possibilité de retirer un consentement, telle qu'elle est explicitement prévue à l'article 6, paragraphe 3, et à l'article 9, paragraphes 3 et 4, de la directive «vie privée et communications électroniques».

III.B.1. Article 2, point f) – Consentement et rapport avec la directive 95/46/CE

«consentement d'un utilisateur ou d'un abonné»

L'article 2 de la directive «vie privée et communications électroniques» dispose expressément que les définitions figurant dans la directive 95/46/CE s'appliquent aux fins de la directive 2002/58/CE. L'article 2, point f), est libellé comme suit: «*le "consentement" d'un utilisateur ou d'un abonné correspond au "consentement de la personne concernée" figurant dans la directive 95/46/CE*».

En d'autres termes, chaque fois qu'un consentement est requis en vertu de la directive «vie privée et communications électroniques», les critères permettant de déterminer si le consentement est valable sont les mêmes que ceux énoncés dans la directive 95/46/CE, à savoir la définition figurant à l'article 2, point h), et la spécificité prévue à l'article 7, point a). L'interprétation selon laquelle le consentement au sens de la directive «vie privée et communications électroniques» doit être compris par

[40] On entend par données relatives au trafic les données traitées aux fins de la transmission d'une communication sur un réseau de communications électroniques ou de la facturation de cette communication, y compris les données relatives au routage, à la durée ou à l'heure d'une communication.

référence à l'article 2, point h), et à l'article 7, point a), lus conjointement, est confirmée par le considérant 17[41].

III.B.2. Article 5, paragraphe 1 - Le consentement de l'une ou des deux parties est-il nécessaire?

«… consentement des utilisateurs concernés …»

L'article 5, paragraphe 1, de la directive «vie privée et communications électroniques» protège la confidentialité des communications en interdisant tout type d'interception ou de surveillance des communications sans le consentement de tous les utilisateurs concernés.

Dans ce cas, l'article 5, paragraphe 1, requiert le consentement de «*tous les utilisateurs concernés*», c'est-à-dire les deux parties à une communication. Le consentement de l'une des parties n'est pas suffisant.

Dans le cadre de l'élaboration de son avis 2/2006[42], le groupe de travail «Article 29» a examiné plusieurs services impliquant la vérification du contenu des courriers électroniques et, dans certains cas, le traçage de l'ouverture des courriels. Le groupe de travail s'est inquiété du fait que, dans ces services, l'une des parties à la communication n'était pas informée. Pour garantir la conformité de ces services avec l'article 5, paragraphe 1, le consentement des deux parties est nécessaire.

III.B.3 Article 6, paragraphe 3, articles 9, 13 et 5, paragraphe 3 – Moment où le consentement est requis

«... après avoir reçu … une information claire et complète …»

Plusieurs dispositions de la directive «vie privée et communications électroniques» contiennent un libellé explicite ou implicite indiquant qu'un consentement est requis avant le traitement. Cette obligation est conforme à la directive 95/46/CE.

L'article 6, paragraphe 3, de la directive «vie privée et communications électroniques» contient une référence explicite au consentement préalable de l'abonné ou de l'utilisateur concerné, faisant obligation au fournisseur de fournir des informations et d'obtenir un consentement préalable au traitement des données relatives au trafic à des fins de commercialisation de services de communications électroniques ou de services à valeur ajoutée. Pour certains types de services, le consentement de l'abonné peut être obtenu lors de la souscription au service. Dans d'autres cas, il peut être possible de l'obtenir directement auprès de l'utilisateur. Une approche similaire est suivie à l'article 9 en ce qui concerne le traitement de données de localisation autres que les données relatives au trafic. Le fournisseur de service doit informer les utilisateurs ou les abonnés – *avant d'obtenir leur consentement* – du type de données de localisation autres

[41] Ce considérant est libellé comme suit: «Aux fins de la présente directive, le consentement … devrait avoir le même sens que le consentement de la personne concernée tel que défini et précisé davantage par la directive 95/46/CE.»

[42] Avis 2/2006 sur les problèmes de protection de la vie privée liés à la fourniture de services de vérification du contenu des courriers électroniques, adopté le 21 février 2006 (WP 118).

que les données relatives au trafic, qui *sera traité*. L'article 13 subordonne au consentement préalable des abonnés l'utilisation de systèmes automatisés d'appel sans intervention humaine, de télécopieurs ou de courrier électronique à des fins de prospection directe.

L'article 5, paragraphe 3, contient une règle spécifique concernant le stockage des informations ou l'accès à des informations stockées dans l'équipement terminal d'un utilisateur, y compris dans le but de suivre les activités en ligne de l'utilisateur. Bien que l'article 5, paragraphe 3, n'utilise pas le qualificatif «préalable», telle est la conclusion claire et évidente que l'on peut tirer de son libellé.

Le bon sens commande d'obtenir le consentement *avant* le début du traitement des données. À défaut, le traitement effectué entre le moment où le traitement a commencé et le moment où le consentement a été obtenu serait illégal, car dénué de fondement juridique. En outre, en pareils cas, si la personne décidait de ne pas donner son consentement, tout traitement de données ayant déjà eu lieu serait illégal pour ce motif également.

Il résulte de ce qui précède que chaque fois qu'un consentement est *requis*¸ il doit être obtenu avant le début du traitement des données. La possibilité d'entamer le traitement sans avoir préalablement obtenu de consentement n'est licite que lorsque la directive relative à la protection des données ou la directive «vie privée et communications électroniques», plutôt que d'exiger un consentement, prévoit un autre fondement et fait référence au droit d'opposition ou de refus du traitement. Ces mécanismes sont tout à fait distincts du consentement. Dans ces cas, le traitement peut avoir déjà commencé et la personne a le droit de s'y opposer ou de le refuser.

L'article 5, paragraphe 3, de l'ancienne directive «vie privée et communications électroniques», selon lequel (soulignement ajouté) «*l'utilisation des réseaux de communications électroniques en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permise qu'à condition que l'abonné ou l'utilisateur, soit muni, dans le respect de la directive 95/46/CE, d'une information claire et complète, entre autres sur les finalités du traitement, et que l'abonné ou l'utilisateur ait le droit de refuser un tel traitement par le responsable du traitement*», en donne un exemple. Il convient de comparer cette version avec le nouveau libellé de l'article 5, paragraphe 3, de la directive «vie privée et communications électroniques», telle que modifiée par la directive 2009/136/CE[43], qui prévoit que «*(...) le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord (...)*». Les effets de cette modification du libellé de l'article 5, paragraphe 3, ont été expliqués par le groupe de travail «Article 29» dans son avis 2/2010 sur la publicité comportementale

[43] Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, texte présentant de l'intérêt pour l'EEE, JO L 337 du 18.12.2009, p. 11.

en ligne[44]. La distinction entre refus et consentement est également explicitée à la section suivante.

Lorsque la directive «vie privée et communications électroniques» ou la directive relative à la protection des données prévoit une possibilité de refuser le traitement de données à caractère personnel, cette possibilité s'explique souvent par le fait que la base juridique du traitement initial des données repose sur un *autre* fondement juridique que le consentement, comme un contrat existant. La section suivante, qui traite de l'article 13 de la directive «vie privée et communications électroniques», illustre aussi ce point.

III.B.4. Article 13, paragraphes 2 et 3 – droit d'opposition et distinction entre ce droit et le consentement

«…les clients se voient donner clairement et expressément la faculté de s'opposer …»

L'article 13 de la directive «vie privée et communications électroniques» prévoit le recours au consentement pour envoyer légalement des communications électroniques à des fins de prospection directe. Pour ce faire, il s'appuie sur un principe général et sur une disposition spécifique.

S'agissant de l'utilisation de systèmes automatisés d'appel, de télécopieurs et de courrier électronique, l'article 13 requiert le consentement préalable de la personne concernée.

Si le destinataire de la communication commerciale est un client existant et que la communication a pour objet de promouvoir les produits ou services du fournisseur ou des produits ou services similaires, le consentement du client n'est pas requis, mais celui-ci doit «*se voi[r] donner la faculté de s'opposer*» en vertu de l'article 13, paragraphe 2. Le considérant 41 explique pourquoi, dans ce cas, le législateur n'a pas exigé de consentement: «*Dans le cadre d'une relation client-fournisseur existante, il est raisonnable d'autoriser l'entreprise … à exploiter ces coordonnées électroniques pour proposer au client des produits ou des services similaires*». Ainsi, en principe, la relation contractuelle entre la personne concernée et le fournisseur de service sert de fondement juridique aux fins du premier contact par courrier électronique. Cependant, les personnes concernées devraient avoir la faculté de s'opposer à tout contact ultérieur. Comme le groupe de travail l'a déjà indiqué: «*Il convient de continuer d'offrir cette possibilité lors de chaque message de prospection directe ultérieur, et ce, sans frais hormis les coûts liés à la transmission du refus*»[45].

Il y a lieu d'établir une distinction entre la nécessité d'un consentement et ce droit d'opposition. Comme illustré ci-dessus à la section III.A.2, un consentement fondé sur l'absence d'action de la part d'une personne, par exemple dans le cas de cases précochées, ne satisfait pas aux conditions de validité du consentement prévues dans la

[44] Avis du 22 juin 2010, WP 171: la question de savoir si un consentement peut être exprimé par «l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application» [considérant 66 de la directive 2009/136/CE] est expressément abordée au point 4.1.1 du document WP 171.

[45] Avis 5/2004 portant sur les communications de prospection directe non sollicitées selon l'article 13 de la directive 2002/58/CE, adopté le 27 février 2004.

directive 95/46/CE. La même conclusion s'applique aux paramètres d'un navigateur qui accepteraient, par défaut, le ciblage de l'utilisateur (au moyen de cookies). Cela ressort clairement du nouveau libellé de l'article 5, paragraphe 3, cité à la section III.B.3 ci-dessus. Ces deux exemples ne satisfont pas notamment aux exigences d'une manifestation de volonté indubitable. Il est essentiel que la personne concernée se voie donner la faculté de prendre une décision et de l'exprimer, par exemple en cochant elle-même la case correspondante, compte tenu de la finalité du traitement des données.

Dans son avis sur la publicité comportementale, le groupe de travail a conclu qu'«*il paraît essentiel que les navigateurs soient munis de paramètres de protection de la confidentialité par défaut. En d'autres termes, il faut qu'ils incluent le paramètre "non-acceptation et non-transmission de cookies tiers". Pour compléter cette disposition et la rendre plus efficace, les navigateurs devraient imposer aux utilisateurs de recourir à un "assistant de protection de la confidentialité" lorsqu'ils installent leur navigateur pour la première fois ou le mettent à jour, et prévoir une procédure simple leur permettant de choisir en cours d'installation*»[46].

III.B.5. Article 6, paragraphe 3, article 9, paragraphes 3 et 4 – possibilité de retirer un consentement

«… possibilité de retirer à tout moment leur consentement …»

La possibilité de retirer un consentement, qui est implicite dans la directive 95/46/CE, apparaît dans diverses dispositions de la directive «vie privée et communications électroniques». L'avis du groupe de travail sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée[47] le mentionnait déjà explicitement:

«L'article 9 de la directive 2002/58/CE permet aux personnes qui ont donné leur consentement au traitement des données de localisation autres que les données relatives au trafic de retirer à tout moment leur consentement et d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données. Le groupe de travail considère que ces droits – qui peuvent être vus comme l'application du droit d'opposition au traitement des données de localisation – sont essentiels au regard du caractère sensible desdites données. Le groupe de travail considère qu'une condition préalable à l'exercice de ce droit réside dans l'information des personnes, non seulement lors de l'inscription au service, mais aussi lors de son utilisation. Si un service nécessite le traitement continu des données de localisation, le groupe 29 estime que le fournisseur dudit service devrait rappeler régulièrement à la personne concernée que son terminal a été, sera, ou peut être localisé. Cette information permettra à la personne en question d'exercer, le cas échéant, les droits de retrait qui lui sont reconnus par l'article 9 de la directive 2002/58/CE.»

Ainsi que cela a été signalé plus haut, cela implique que le retrait soit exercé à l'égard du traitement futur et non à l'égard du traitement de données effectué dans le passé, au cours de la période où les données ont été légitimement collectées. Les décisions prises ou les processus engagés dans le passé sur la base de ces informations ne peuvent donc pas être purement et simplement annulés. Cependant, s'il n'existe pas d'autre base

[46] Avis du 22 juin 2010, WP 171, op.cit.

[47] Avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, adopté le 25 novembre 2005 (WP 115).

juridique justifiant le stockage ultérieur des données, ces dernières devraient être supprimées par le responsable du traitement.

IV. Conclusions

Le présent avis porte sur le cadre juridique relatif à l'utilisation du consentement en application des directives 95/46/CE et 2002/58/CE. Cet exercice poursuit un double objectif. Il tend tout d'abord à clarifier les exigences légales existantes et à illustrer leur fonctionnement dans la pratique. Ce faisant, il fournit une réflexion sur la question de savoir si le cadre existant est toujours adapté, compte tenu des nombreux nouveaux modes de traitement des données à caractère personnel, et sur la nécessité de le modifier ou non.

IV.1. Clarification des aspects essentiels du cadre actuel

L'article 2, point h), de la directive 95/46/CE définit le consentement comme «toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement». L'article 7 de la directive, qui énonce la base juridique du traitement de données à caractère personnel, définit le consentement *indubitable* comme l'un des fondements juridiques. L'article 8 requiert un consentement *explicite* comme fondement juridique du traitement de données sensibles. L'article 26, paragraphe 1, de la directive 95/46/CE et plusieurs dispositions de la directive «vie privée et communications électroniques» exigent un consentement pour le traitement des données particulières relevant de leur champ d'application. Les points développés dans le présent avis visent à clarifier les différents aspects de ce cadre juridique afin d'en faciliter l'application par les parties prenantes en général.

Éléments/observations à caractère général

- Le consentement constitue l'un des six fondements juridiques du traitement de données à caractère personnel (l'un des cinq fondements en ce qui concerne les données sensibles). Il s'agit d'un fondement important dans la mesure où il confère à la personne concernée un certain contrôle sur le traitement de ses données. Il importe, toutefois, que le consentement en tant que facteur d'autonomie et d'autodétermination soit utilisé à bon escient et dans le respect des conditions applicables.

- D'une manière générale, le cadre juridique de la directive 95/46/CE s'applique chaque fois qu'un consentement est demandé, qu'il s'agisse de l'environnement hors ligne ou en ligne. De ce fait, les règles qui s'appliquent lorsqu'un détaillant en matériaux de construction demande à ses clients de signer un formulaire papier pour obtenir une carte de fidélité sont les mêmes que s'il le faisait par l'intermédiaire de son site internet. En outre, la directive «vie privée et communications électroniques» précise les traitements de données qui sont subordonnés à l'obtention d'un consentement: ils concernent principalement le traitement de données en rapport avec la fourniture de services de communications électroniques accessibles au public. Les conditions à satisfaire pour qu'un consentement soit valable en vertu de la directive 2002/58/CE sont identiques à celles qui sont énoncées dans la directive 95/46/CE.

- Il convient de ne pas confondre les situations dans lesquelles le responsable du traitement fonde le traitement des données à caractère personnel sur le consentement et celles où il s'appuie sur d'autres fondements juridiques impliquant un droit d'opposition de la personne concernée. Cela peut être le cas lorsque le traitement repose sur les «intérêts légitimes» du responsable du traitement au sens de l'article 7, point f), de la directive 95/46/CE, mais la personne concernée a néanmoins le droit de s'y opposer en vertu de l'article 14, point a), de ladite directive. Un autre exemple est celui d'un responsable du traitement qui envoie des communications par courrier électronique à des clients existants afin de promouvoir ses produits ou services ou des produits ou services similaires; les clients ont toutefois le droit de s'opposer à ces communications en vertu de l'article 13, paragraphe 2, de la directive 2002/58/CE. Dans les deux cas, la personne concernée a le droit de s'opposer au traitement, ce qui n'équivaut pas à un consentement.

- Le recours au consentement pour traiter des données à caractère personnel ne dispense pas le responsable du traitement de son obligation de satisfaire aux autres exigences imposées par le cadre juridique relatif à la protection des données, comme le respect du principe de proportionnalité en vertu de l'article 6, paragraphe 1, point c), la sécurité du traitement prévue à l'article 17, etc.

- Un consentement valable présuppose la capacité de consentir de la personne concernée. Or les règles relatives à la capacité de consentir ne sont pas harmonisées et peuvent donc varier d'un État membre à l'autre.

- Des personnes qui ont donné leur consentement devraient être en mesure de le retirer pour empêcher tout traitement ultérieur des données les concernant. Ceci est également confirmé par la directive «vie privée et communications électroniques» en ce qui concerne le traitement de catégories particulières de données fondé sur un consentement, tel que le traitement de données de localisation autres que les données relatives au trafic.

- Le consentement doit être donné avant le début du traitement des données à caractère personnel, mais il peut aussi être requis durant un traitement lorsqu'une nouvelle finalité vient s'ajouter aux finalités initialement prévues. Plusieurs dispositions de la directive 2002/58/CE insistent sur ce point, soit en exigeant que le consentement soit «préalable» (par exemple, l'article 6, paragraphe 3), soit par le libellé des dispositions (par exemple, l'article 5, paragraphe 3).

Éléments spécifiques du cadre juridique relatifs au consentement

- Pour être valable, un consentement doit être *libre*. En d'autres termes, il ne doit pas y avoir de risque de tromperie, d'intimidation ou de conséquences négatives importantes pour la personne concernée si elle ne donne pas son consentement. Le traitement de données dans le cadre professionnel, lorsqu'il existe un rapport de subordination, ainsi que dans le cadre de services publics, comme la santé, peut requérir une évaluation approfondie de la question de savoir si les personnes concernées sont libres de donner leur consentement.

- Un consentement doit être *spécifique*. Un consentement général, sans précision des finalités exactes du traitement, ne satisfait pas à cette exigence. Plutôt que d'insérer ces informations dans les conditions générales du contrat, il y a lieu de recourir à des clauses de consentement spécifiques, distinctes des conditions générales.

- Un consentement doit être *informé*. Les articles 10 et 11 de la directive dressent la liste des informations qui doivent nécessairement être fournies aux personnes concernées. En tout état de cause, les informations fournies doivent être suffisantes pour garantir une prise de décision éclairée des personnes sur le traitement des données les concernant. Cette obligation de consentement «informé» se traduit par deux exigences supplémentaires. Premièrement, les informations doivent être transmises dans un langage adapté permettant à la personne concernée de comprendre à quoi elle consent et quelles sont les finalités du traitement. Cette exigence sera fonction du contexte. L'utilisation d'un jargon juridique ou technique excessivement pointu ne répondrait pas aux exigences de la législation. Deuxièmement, l'information fournie aux utilisateurs doit être claire et suffisamment visible afin qu'elle ne puisse pas leur échapper. L'information doit être directement communiquée aux personnes concernées. Il ne suffit pas qu'elle soit simplement disponible quelque part.

- Quant à la manière dont le consentement doit être donné, l'article 8, paragraphe 2, point a), exige un consentement *explicite* au traitement de données sensibles, ce qui signifie une réponse active, orale ou écrite, par laquelle la personne marque son accord au traitement des données la concernant à certaines fins. Par conséquent, un consentement exprès ne saurait être obtenu au moyen d'une case précochée. La personne concernée doit effectuer une action positive pour signifier son consentement et doit être libre de refuser le traitement.

- Pour des données autres que les données sensibles, l'article 7, point a), requiert que le consentement soit *indubitable*. Cette exigence de consentement «indubitable» impose le recours à des mécanismes de consentement ne laissant aucun doute sur l'intention de la personne de marquer son accord. Dans la pratique, cette exigence permet aux responsables du traitement d'utiliser différents types de mécanismes pour demander le consentement de la personne concernée, allant de déclarations marquant un accord (consentement exprès) à des mécanismes requérant une action particulière à cette fin.

- En principe, un consentement fondé sur l'inaction ou le silence de la personne concernée, en particulier dans l'environnement en ligne, ne constitue pas un consentement valable. Cette question se pose, notamment, dans le cas de l'utilisation de paramètres par défaut que la personne concernée est tenue de modifier pour refuser le traitement. Il peut s'agir, par exemple, de l'utilisation de cases précochées ou des paramètres d'un navigateur internet configurés par défaut pour autoriser la collecte de données.

IV.2 Appréciation du cadre actuel et de la nécessité éventuelle de le modifier

Appréciation globale

Le groupe de travail considère que le cadre actuel de la protection des données comporte un ensemble bien pensé de règles fixant les conditions d'un consentement valable pour légitimer un traitement de données. Ces conditions s'appliquent aussi bien à l'environnement hors ligne qu'à l'environnement en ligne.

Le cadre actuel parvient à trouver un juste milieu entre une série de préoccupations. D'une part, il garantit que seul un consentement réel et informé soit réputé comme tel. À

cet égard, l'article 2, point h), qui requiert expressément que le consentement soit libre, spécifique et informé, est pertinent et satisfaisant. D'autre part, cette exigence n'est pas un carcan rigide, mais offre une souplesse suffisante en évitant des règles spécifiques sur le plan technique, comme l'illustre ce même article 2, point h), qui définit le consentement comme toute manifestation de la volonté de la personne concernée. Cela laisse une marge de manœuvre suffisante en ce qui concerne les façons dont cette manifestation peut être exprimée. Les articles 7 et 8, qui requièrent, respectivement, un consentement indubitable et explicite, saisissent bien la nécessité de trouver un équilibre entre ces deux aspects, en apportant une certaine souplesse et en évitant des structures excessivement rigides tout en garantissant une protection.

Il en résulte un cadre qui, s'il est correctement appliqué et mis en œuvre, est de nature à s'adapter au large éventail de traitements de données qui découlent bien souvent de l'évolution technologique.

Or, dans la pratique, il n'est pas toujours aisé de déterminer quand un consentement est nécessaire et, plus précisément, quelles sont les conditions à satisfaire pour que le consentement soit valable, faute de règles uniformes dans les États membres. Les mesures de transposition adoptées dans les États membres ont abouti à des approches différentes. Des lacunes plus spécifiques ont été recensées lors des discussions du groupe de travail «Article 29» qui ont donné lieu au présent avis. Ces lacunes sont décrites ci-après.

Modifications éventuelles

- La notion de consentement indubitable contribue à la mise en place d'un système qui, sans être exagérément rigide, offre un niveau élevé de protection. Si elle est de nature à déboucher sur un système raisonnable, elle est hélas souvent mal comprise ou purement et simplement ignorée. Si les explications et exemples donnés ci-dessus devraient contribuer à renforcer la sécurité juridique et la protection des droits des personnes concernées lorsqu'un consentement est utilisé comme base juridique, la situation actuelle semble néanmoins appeler un certain nombre de modifications.
- En particulier, le groupe de travail «Article 29» considère que le libellé proprement dit («indubitable») mériterait d'être précisé dans le contexte de la révision du cadre général applicable à la protection des données. Cette clarification devrait insister sur le fait qu'un consentement indubitable impose de recourir à des mécanismes qui ne laissent aucun doute sur l'intention de la personne concernée de consentir au traitement. Dans le même temps, il conviendrait d'expliquer que l'utilisation d'options par défaut, que la personne concernée doit modifier pour refuser le traitement (consentement fondé sur le silence), ne constitue pas, en soi, un consentement indubitable. Cette observation vaut tout particulièrement dans l'environnement en ligne.
- Outre ce besoin de clarification, le groupe de travail «Article 29» formule les propositions suivantes:

    i. *Premièrement*, inclure dans la définition du consentement visée à l'article 2, point h), le qualificatif «indubitable» (ou un équivalent) afin de renforcer l'idée que seul un consentement fondé sur une déclaration ou une action destinée à marquer un accord constitue un consentement valable. En plus de clarifier les choses, cet ajout permettrait d'aligner la notion de consentement au sens de l'article 2, point h), sur les

conditions de validité du consentement énoncées à l'article 7. En outre, la signification de l'adjectif «indubitable» pourrait être précisée dans un considérant du futur cadre juridique.

ii. *Deuxièmement*, dans le cadre de l'obligation générale de rendre compte, les responsables du traitement devraient être en mesure de démontrer qu'un consentement a été obtenu. En effet, si la charge de la preuve est renforcée de telle sorte que les responsables du traitement soient tenus de prouver qu'ils ont effectivement obtenu le consentement de la personne concernée, ils seront contraints de mettre en place des pratiques et des mécanismes types pour demander un consentement indubitable et le prouver. La nature de ces mécanismes dépendra du contexte et devrait tenir compte des faits et des circonstances ainsi que du traitement et, plus particulièrement, des risques qu'il comporte.

- Le groupe de travail «Article 29» n'est pas persuadé que le cadre juridique doive exiger un consentement explicite en tant que règle générale pour tous les types de traitement, y compris ceux actuellement couverts par l'article 7 de la directive. Il considère, en effet, qu'un consentement indubitable pouvant consister soit en un consentement explicite soit en un consentement découlant *d'actions* indubitables devrait rester la norme. Ce choix offrirait aux responsables du traitement une plus grande souplesse dans l'obtention du consentement, et la procédure complète pourrait s'en trouver accélérée et devenir plus conviviale.

- Plusieurs aspects du cadre juridique applicable au consentement sont déduits du libellé, de la genèse législative ou ont été développés par la jurisprudence et les avis du groupe de travail «Article 29». Néanmoins, la sécurité juridique se verrait renforcée si ces aspects étaient expressément intégrés dans le nouveau cadre législatif applicable à la protection des données. Les éléments suivants pourraient être pris en compte:

  i. l'insertion d'une clause expresse instituant le droit de la personne concernée à retirer son consentement;

  ii. le renforcement de la notion selon laquelle le consentement doit être donné avant le début du traitement ou avant toute utilisation ultérieure des données pour des finalités qui n'étaient pas couvertes par le consentement initial, lorsqu'il n'existe pas d'autre fondement juridique au traitement;

  iii. l'ajout d'exigences explicites concernant la qualité (obligation de fournir des informations sur le traitement des données d'une manière aisément compréhensible et dans un langage clair et simple) et l'accessibilité des informations (obligation que les informations soient évidentes, visibles et directement accessibles). Ceci est essentiel pour permettre aux personnes concernées de prendre une décision en toute connaissance de cause.

- Enfin, s'agissant des personnes ne jouissant pas de la capacité juridique, des dispositions pourraient être prévues afin de renforcer leur protection, par exemple:

i. des précisions sur les circonstances dans lesquelles le consentement des parents ou du tuteur légal d'une personne incapable est requis, y compris l'âge en dessous duquel ce consentement serait obligatoire;

ii. l'obligation d'utiliser des mécanismes de vérification de l'âge, qui pourraient varier en fonction de circonstances telles que l'âge de l'enfant, la nature du traitement, les risques possibles, la conservation ou non des informations par le responsable du traitement ou encore leur transmission ou non à des tiers;

iii. l'obligation d'adapter les informations fournies aux enfants dans la mesure où cela leur permettrait de mieux comprendre ce que recouvre la collecte de données et faciliterait leur décision de consentir ou non au traitement;

iv. des garanties spécifiques à certains traitements de données, tels que la publicité comportementale, pour lesquels le consentement ne devrait pas pouvoir servir de fondement pour légitimer le traitement de données à caractère personnel.

Le groupe de travail «Article 29» réexaminera la question du consentement. Plus précisément, les autorités nationales chargées de la protection des données et le groupe de travail pourraient décider ultérieurement d'élaborer des lignes directrices sur la base du présent avis, en donnant des exemples concrets supplémentaires.

Fait à Bruxelles, le 13 juillet 2011

Pour le groupe de travail

Le président
Jacob KOHNSTAMM