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

1021/00/FR
WP207

Avis 6/2013 sur la réutilisation des informations du secteur public (ISP) et des données ouvertes

Adopté le 5 juin 2013

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

Le secrétariat est assuré par la Direction C (Droits fondamentaux et citoyenneté de l'Union) de la direction générale de la justice de la Commission européenne, B-1049 Bruxelless, Belgique, bureau MO-59 02/013.

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

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

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

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

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

I. Introduction

1.1. Révision de la directive ISP

Le 26 juin 2013, l'Union européenne a adopté la directive 2013/37/UE du Parlement européen et du Conseil (la «modification ISP») modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public (la «directive ISP»)[1].

L'objectif de la directive ISP consiste à faciliter la réutilisation des informations du secteur public par l'harmonisation des conditions de réutilisation dans toute l'Union européenne et par l'élimination de tous les obstacles inutiles à la réutilisation sur le marché intérieur.

Le texte original de 2003 de la directive ISP harmonisait les conditions de la réutilisation, mais n'imposait pas aux organismes du secteur public une obligation de rendre disponibles des données à des fins de réutilisation. La question de la mise à disposition des données à des fins de réutilisation était essentiellement optionnelle: la décision était laissée à l'appréciation des États membres et des organismes du secteur public. Partant, de nombreux organismes du secteur public dans toute l'Europe choisissaient simplement de ne pas autoriser la réutilisation de leurs informations.

Dans ce contexte, l'un des principaux objectifs politiques de la modification ISP consiste à introduire le principe selon lequel toutes les informations publiques (à savoir toutes les informations du secteur public accessibles au public en vertu du droit national) sont réutilisables à des fins commerciales et non commerciales. Certaines exclusions du champ d'application de la directive ISP modifiée sont prévues dans certains cas, notamment pour des motifs de protection des données[2].

La directive ISP impose donc aux organismes du secteur public l'obligation d'autoriser la réutilisation de toutes les informations publiques qu'ils détiennent. Toutefois, comme le présent avis le montre plus loin, cette obligation ne couvre pas la divulgation publique de données à caractère personnel, mais uniquement la réutilisation des informations qui sont déjà accessibles au public en vertu du droit national et, même dans ce cas, à condition que la réutilisation ne porte pas atteinte aux dispositions de la législation applicable en matière de protection des données.

1 JO L 175 du 27.6.2013, p. 1.

2 Concernant le champ d'application de la directive ISP modifiée et les dispositions relatives à la protection des données, voir la section V ci-dessous.

D'autres nouvelles dispositions pertinentes de la modification ISP étendent le champ d'application de la directive ISP aux bibliothèques (y compris les bibliothèques universitaires), aux archives et aux musées.

À la lumière de ce qui précède, la directive ISP modifiée peut fortement augmenter l'accessibilité des informations détenues par des organismes publics.

1.2. Réutilisation des ISP et des données à caractère personnel

Les initiatives de réutilisation des ISP impliquent en général (i) de rendre disponibles des bases de données entières (ii) dans un format électronique normalisé (iii) à toute personne qui en fait la demande sans processus de sélection, (iv) gratuitement (ou à un prix limité), et (v) à toutes fins commerciales ou non commerciales sans conditions (ou dans des conditions non restrictives par le biais d'une licence, le cas échéant)[3].

Cela peut comporter des avantages conduisant à une plus grande transparence et à une réutilisation innovante des ISP. Cependant, l'accessibilité accrue des informations qui en résulte n'est pas sans risque.

Pour réduire ces risques au minimum, lorsqu'il s'agit de données à caractère personnel, la législation sur la protection des données doit contribuer à orienter le processus de sélection des données à caractère personnel qui peuvent ou non être rendues disponibles à des fins de réutilisation, ainsi que des mesures à prendre pour protéger lesdites données. Une approche équilibrée est nécessaire chaque fois que la protection de la vie privée et des données à caractère personnel est en jeu. D'une part, les règles relatives à la protection des données à caractère personnel ne devraient pas constituer un obstacle excessif au développement du marché de la réutilisation. D'autre part, il faut respecter le droit à la protection des données à caractère personnel et le droit à la vie privée. Il importe de souligner que le concept de données ouvertes est axé sur la transparence et la responsabilité des organismes du secteur public, ainsi que sur la croissance économique, pas sur la transparence des citoyens en tant que particuliers.

Lorsqu'il applique la directive ISP et la législation sur la protection des données dans le domaine de la réutilisation des données à caractère personnel, l'organisme du secteur public est susceptible de prendre l'une des trois décisions suivantes:

1. ne pas rendre disponibles des données à caractère personnel à des fins de réutilisation dans les conditions prévues par la directive ISP;
2. rendre anonymes les données à caractère personnel (généralement sous forme de données statistiques agrégées)[4] et ne mettre que ces données rendues anonymes à disposition à des fins de réutilisation;
3. rendre les données à caractère personnel disponibles à des fins de réutilisation (si nécessaire, sous réserve de conditions spécifiques et de garanties adéquates).

[3] Conformément à l'article 8, paragraphe 1, de la directive ISP, telle que modifiée, les «conditions (de la licence) ne limitent pas indûment les possibilités de réutilisation et ne sont pas utilisées pour restreindre la concurrence».

[4] Concernant la réutilisation des ensembles de données agrégées et rendues anonymes issus de données à caractère personnel, voir la section VI ci-dessous.

II. Objectif de l'avis

2.1. Orientations cohérentes et meilleures pratiques

Le présent avis vise à garantir une compréhension commune du cadre juridique applicable et à fournir des orientations cohérentes et des exemples de meilleure pratique sur la manière de mettre en œuvre la directive ISP (telle que modifiée) à l'égard du traitement des données à caractère personnel.

Le présent avis ne cherche pas à harmoniser les approches nationales concernant le niveau de transparence, les règles nationales en matière d'accès aux documents et la disponibilité des informations en vertu de ces règles. Toutefois, la législation nationale de transposition de la directive ISP et l'interprétation nationale de la directive 95/46/CE[5] concernant la réutilisation des ISP diffèrent parfois à un degré tel qu'il excède ce qui est nécessaire pour tenir compte de la diversité des règles nationales en matière d'accès et des différents niveaux de transparence.

À cet égard, la recommandation politique de septembre 2012 préparée par le réseau thématique LAPSI illustre clairement les disparités inutiles dans la manière dont la directive ISP a été transposée dans les États membres concernant la protection des données à caractère personnel[6]. La directive ISP elle-même avertit également que l'incidence des incertitudes et des différences législatives grandira encore avec l'essor de la société de l'information, qui a déjà considérablement accru l'exploitation transfrontière de l'information[7].

L'absence d'approche homogène peut affaiblir la position des personnes concernées. Elle peut également imposer une charge réglementaire inutile aux entreprises et autres organisations exerçant des activités transfrontières et constituer ainsi un obstacle au développement d'un marché européen commun de la réutilisation. D'une part, les personnes concernées doivent être assurées que leurs données seront protégées en permanence, indépendamment de leur transfert vers un pays tiers à des fins de réutilisation. D'autre part, il faut éviter une complexité et une fragmentation excessives afin de permettre la libre circulation des données à caractère personnel en Europe, un autre objectif premier de la directive 95/46/CE.

2.2. Nécessité d'actualiser l'avis 7/2003

La modification ISP survient une décennie après l'adoption de la directive ISP en 2003. À l'époque, le groupe de travail «article 29» avait adopté un avis sur les questions liées à la protection des ISP («avis 7/2003»)[8]. Si les principes directeurs énoncés dans ledit avis restent d'actualité, les développements technologiques et autres dans le domaine des ISP et de la protection des données, y compris les changements législatifs proposés dans les deux domaines, justifient les efforts qui sont actuellement déployés pour actualiser et compléter l'avis de 2003.

---

[5] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (JO L 281 du 23.11.1995, p. 31).

[6] LAPSI est un réseau thématique européen concernant les «aspects juridiques des informations du secteur public», financé par la Commission européenne, voir http://www.lapsi-project.eu/ (en anglais). La recommandation politique est disponible (en anglais) à l'adresse http://www.lapsi-project.eu/lapsifiles/lapsi_privacy_policy.pdf.

[7] Voir le considérant 7.

[8] Voir avis 7/2003 du groupe de travail «article 29» sur la réutilisation des informations émanant du secteur public et la protection des données à caractère personnel - Trouver le juste milieu - adopté le 12 décembre 2003 (WP 83). Voir également deux avis antérieurs connexes: l'avis 3/1999 concernant l'information émanant du secteur public et la protection des données à caractère personnel, adopté le 3 mai 1999 (WP20), et l'avis 5/2001 concernant un rapport spécial du Médiateur européen, adopté le 17 mai 2001.

En outre, l'avis peut également tenir compte à présent d'autres efforts récents et en cours visant à fournir d'autres orientations, en particulier:

- l'avis du Contrôleur européen de la protection des données (CEPD) du 18 avril 2012 sur le paquet de mesures de la Commission européenne relatif à l'ouverture des données[9];
- l'avis 3/2013 du groupe de travail «article 29» sur la limitation de la finalité[10];
- les travaux en cours au sein du sous-groupe «technologie» du groupe de travail «article 29» sur les techniques d'anonymisation[11];
- les travaux dans certains États membres sur l'anonymisation et l'évaluation des risques;[12] et
- la jurisprudence et les pratiques existantes en matière d'équilibre entre la réutilisation et la protection des données à caractère personnel dans certains États membres[13].

III. Éléments centraux et structure de l'avis

L'avis 7/2003 se concentre sur le principe de limitation de la finalité[14], mais aborde également d'autres questions comme les bases juridiques de la divulgation publique et de la réutilisation des ISP, la protection spéciale des données sensibles, le transfert vers des pays tiers, la qualité des données et les droits des personnes concernées. Ces observations restent d'actualité. Compte tenu des travaux antérieurs, le présent avis ne fait qu'actualiser et compléter les conclusions de l'avis 7/2003, le cas échéant, à la lumière des nouveaux développements législatifs et technologiques.

La section IV contribue à préciser que l'obligation de réutilisation en vertu de la directive ISP modifiée est sans préjudice des obligations relatives à la protection des données. Elle souligne aussi l'importance de la «protection des données dès la conception et par défaut» et des «évaluations d'impact sur la protection des données» pour contribuer à garantir que les craintes en matière de protection des données soient dissipées avant que les données à caractère personnel ne soient rendues disponibles à des fins de réutilisation.

La section V donne des orientations, à l'aide d'exemples, concernant les catégories de données à caractère personnel qui peuvent relever du champ d'application de la directive ISP.

La section VI se concentre sur les situations qui surviennent le plus souvent dans le cadre des initiatives de réutilisation des ISP: lorsque des données statistiques agrégées, issues de données à caractère personnel, sont rendues disponibles sous forme agrégée et anonyme. C'est notamment le cas des données statistiques agrégées sur les taux de criminalité, les dépenses publiques ou la réussite scolaire des enfants dans différentes régions géographiques ou différents établissements scolaires. C'est le scénario le plus fréquent de réutilisation d'ISP contenant des données à caractère personnel, et une grande partie du présent avis lui est consacrée. La principale préoccupation en

---

[9] Avis du CEPD du 18 avril 2012 sur le paquet de mesures de la Commission européenne relatif à l'ouverture des données, qui comprend une proposition de directive modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public (ISP), une communication sur l'ouverture des données et la décision 2011/833/UE de la Commission sur la réutilisation des documents de la Commission. Disponible à l'adresse suivante: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-18_Open_data_FR.pdf.

[10] Avis 3/2013 du groupe de travail «article 29» sur la limitation de la finalité, adopté le 2 avril 2013 (WP 203).

[11] Un avis sur ce sujet devrait être adopté au cours du deuxième semestre de 2013.

[12] Voir, par exemple, le code de pratique sur l'anonymisation (*Anonymisation: Managing data protection risk code of practice*) publié par le bureau du commissaire à l'information au Royaume-Uni en novembre 2012 et les directives relatives à l'analyse des risques publiées par l'autorités française chargée de la protection des données en juin 2012.

[13] Voir, par exemple, la recommandation politique du LAPSI de septembre 2012 (pp. 4-14).

[14] Voir article 6, paragraphe 1, point b), de la directive 95/46/CE.

matière de protection des données est ici de garantir une réelle agrégation et anonymisation et de réduire au minimum le risque de ré-identification des données à caractère personnel à partir des ensembles de données agrégées.

La section VII aborde - avec moins de détails - les situations où les données à caractère personnel sont accessibles au public et, partant, où elles peuvent éventuellement être rendues disponibles à des fins de réutilisation. S'il ne s'agit pas, à l'heure actuelle, du scénario typique des initiatives de réutilisation des ISP, il est important de tenir compte du fait que les organismes du secteur public mettent de plus en plus de données à caractère personnel à la disposition du public, souvent sur l'internet. Il s'agit souvent de données à caractère personnel directement identifiables telles que, par exemple, des informations cadastrales sur le propriétaire d'un bien immobilier donné, des déclarations d'intérêts ou de salaires de certains fonctionnaires, des dépenses de députés. La question qui se pose ici est de savoir dans quelle mesure, à quelles fins, dans quelles conditions et avec quelles garanties ces données peuvent être rendues disponibles à des fins de réutilisation. Il est important de déterminer clairement si ces données entrent dans le champ d'application de la directive ISP.

Dans ce contexte, il convient de souligner que toute information relative à une personne physique identifiée ou identifiable, qu'elle soit accessible au public ou non, constitue une donnée à caractère personnel. Partant, l'accès aux données à caractère personnel qui ont été rendues publiques et leur réutilisation (par exemple, par une publication sur l'internet) restent soumis à la législation applicable en matière de protection des données.

D'autres scénarios spécifiques, comme les données de recherche et les archives historiques - qui tombent à présent sous le coup de la directive ISP -, seront brièvement abordés dans les sections VIII et IX.

La section X traite de la question de l'octroi de licences pour les ISP et de la nécessité d'intégrer, le cas échéant, une clause relative à la protection des données dans ces licences.

Enfin, la section XI propose une série de conclusions et recommandations.

IV. Toutes les données à caractère personnel «accessibles au public» ne devraient pas être rendues disponibles à des fins de réutilisation

4.1. L'obligation de réutilisation en vertu de la directive ISP est sans préjudice des exigences en matière de protection des données

Lorsqu'elle a été adoptée en 2003, la directive ISP n'imposait pas aux organismes du secteur public l'obligation d'autoriser la réutilisation des ISP. La décision d'autoriser ou non la réutilisation est laissée à l'appréciation des États membres ou de l'organisme du secteur public concerné (sous réserve du cadre réglementaire national sur la transparence et l'accès). L'avis 7/2003 a été adopté à la lumière de cette «non-obligation». Aux termes de la section 2, point cc), de l'avis 7/2003, «il est important de souligner que la directive «Réutilisation» ne peut être invoquée en tant qu'obligation juridique devant être remplie, dans la mesure où la directive ne crée aucune obligation de divulguer des informations à caractère personnel».

Avec la modification ISP, l'analyse devient plus complexe, mais la conclusion finale reste identique.

L'article 3, paragraphe 1, de la directive ISP modifiée prévoit que «sous réserve du paragraphe 2, les États membres veillent à ce que les documents auxquels s'applique la présente directive en vertu de

l'article 1er puissent être réutilisés à des fins commerciales ou non commerciales, conformément aux conditions définies aux chapitres III et IV». Si la réutilisation ne peut être refusée pour les raisons énoncées à l'article 1er (raisons découlant des règles nationales en matière d'accès et en particulier également pour des motifs de protection des données à caractère personnel), la réutilisation doit être autorisée.

Parallèlement, le considérant 21 de la directive ISP signale que «la présente directive devrait être mise en œuvre et appliquée dans le respect total des principes relatifs à la protection des données à caractère personnel». En outre, l'article 1er, paragraphe 4, prévoit que la directive ISP «laisse intact et n'affecte en rien le niveau de protection des personnes physiques à l'égard du traitement des données à caractère personnel».

Ces dispositions, prises et lues ensemble, signifient que le «principe de réutilisation» n'est pas automatique lorsque le droit à la protection des données à caractère personnel est en jeu, et qu'il ne l'emporte pas sur les dispositions applicables de la législation sur la protection des données. Lorsque les documents détenus par des organismes du secteur public contiennent des données à caractère personnel, leur réutilisation relève de la directive 95/46/CE et reste soumise à la législation applicable en matière de protection des données.

En conséquence, lorsque la réutilisation porte sur des données à caractère personnel, l'organisme du secteur public ne peut pas systématiquement invoquer la nécessité de respecter la directive ISP comme base juridique pour rendre les données disponibles à des fins de réutilisation[15].

4.2. Importance de l'évaluation d'impact sur la protection des données avant l'ouverture des données à la réutilisation

Vu les risques potentiels que comporte la réutilisation des ISP - et en particulier le fait que lorsque les données à caractère personnel ont été rendues accessibles à des fins de réutilisation, il est très difficile de contrôler de manière efficace l'utilisation de ces données -, le groupe de travail «article 29» souligne la nécessité d'adhérer aux principes de «protection des données dès la conception et par défaut» et de veiller à ce que les préoccupations en matière de protection des données soient prises en compte dès que possible. En particulier, le groupe de travail «article 29» recommande vivement que l'organisme du secteur public évalue minutieusement l'impact sur la protection des données avant de rendre disponibles les données à caractère personnel à des fins de réutilisation. Les États membres devraient également envisager de rendre cette évaluation d'impact obligatoire dans leur droit national ou de la promouvoir en tant que meilleure pratique. Quoi qu'il en soit, même si cela n'est pas expressément prévu dans le droit national, avant de divulguer des informations et de décider de les rendre accessibles à ces fins, les organismes du secteur public devraient procéder à un examen minutieux afin d'établir si les données à caractère personnel peuvent être rendues disponibles à des fins de réutilisation. Et, si c'est le cas, ces organismes devraient également déterminer à quelles conditions et avec quelles garanties spécifiques en matière de protection des données la réutilisation est acceptable.

L'évaluation devrait, entre autres, établir une base juridique pour la divulgation (et une base juridique potentielle pour la réutilisation), évaluer les principes de limitation de la finalité, de proportionnalité et de minimisation des données, et examiner la protection spéciale que requièrent

[15] Le groupe de travail «article 29» tient également à indiquer clairement que, du point de vue du réutilisateur, la directive ISP ne fournit pas en soi de base légale pour le traitement (pour les bases légales, voir l'avis 7/2003 et la section 7.5 ci-après).

les données sensibles. Lors de cette évaluation, l'impact potentiel sur les personnes concernées devrait être soigneusement examiné.

Cette évaluation devrait contribuer à déterminer, le cas échéant, les données à caractère personnel qui peuvent être rendues disponibles à des fins de réutilisation, et avec quelles garanties[16]. Il convient de souligner que la proposition de règlement sur la protection des données[17] encourage et, dans certains cas, requiert des évaluations d'impact sur la protection des données comme outil clé pour garantir que les responsables du traitement rendent des comptes [18].

Dans la mesure du possible, l'analyse préalable à la décision de réutilisation devrait se baser sur un débat éclairé et sur la représentation des différents acteurs, notamment: le responsable du traitement qui souhaite divulguer les données; les personnes qui demandent les données et peuvent donc contextualiser la discussion; les représentants des personnes dont les données à caractère personnel sont en jeu (par exemple, les organisations de protection des consommateurs, les organisations de défense des droits des patients, les syndicats d'enseignants). Lorsque le résultat de cette analyse n'est pas clair, l'autorité compétente chargée de la protection des données et les autorités nationales chargées de la liberté d'information peuvent proposer des orientations.

Les États membres devraient également envisager d'établir et d'aider des réseaux de connaissances/centres d'excellence, facilitant ainsi le partage de bonnes pratiques concernant l'anonymisation et l'ouverture des données. Cela peut revêtir une importance particulière pour les organismes du secteur public de moindre envergure, qui peuvent ne pas avoir l'expertise nécessaire pour réaliser l'anonymisation, pour évaluer l'impact sur la protection des données et pour calculer et tester les risques de ré-identification[19].

Enfin, une évaluation d'impact est vivement recommandée avant la mise en place d'une nouvelle législation qui demande la divulgation au public de données à caractère personnel.

---

[16] Si l'étude conduit à une décision de ne pas mettre à disposition à des fins de réutilisation les données à caractère personnel en tant que telles, mais plutôt de rendre disponibles des ensembles de données rendues anonymes issus de données à caractère personnel, il convient de procéder à une évaluation des risques de ré-identification. Voir la section VI sur l'anonymisation et l'évaluation des risques de ré-identification.

[17] Le 25 janvier 2012, la Commission a adopté un paquet en vue de la réforme du cadre européen de protection des données. Le paquet englobe (i) une «communication» (COM(2012) 9 final), (ii) une «proposition de règlement sur la protection des données» (COM(2012) 11 final), et (iii) une «proposition de directive relative à la protection des données» (COM(2012) 10 final).

[18] Pour d'autres orientations sur la manière de réaliser une évaluation d'impact sur la protection des données, voir, par exemple, le site web du projet PIAF (un cadre d'évaluation des facteurs liés à la vie privée pour la protection des données et les droits à la protection de la vie privée) à l'adresse suivante: http://www.piafproject.eu/index.html (en anglais). Le PIAF est un projet cofinancé par la Commission européenne qui vise à encourager l'UE et ses États membres à adopter une politique progressive d'évaluation des facteurs liés à la vie privée comme moyen de répondre aux besoins et défis liés à la vie privée et au traitement des données à caractère personnel. Des orientations sont également disponibles dans certains États membres. Voir, par exemple, le manuel d'évaluation des facteurs liés à la vie privée publié par le commissaire britannique à l'information (disponible, en anglais, à l'adresse suivante: http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment), les directives relatives à l'analyse des risques publiées par les autorités françaises chargées de la protection des données (citées à la note de bas de page 12), et les orientations fournies par le commissaire slovène à l'information, en particulier sur les «Évaluations des facteurs liés à la vie privée dans les projets d'administration en ligne» (disponible à l'adresse suivante: https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIASmernice__ENG_Lektorirano_10._6._2011.pdf (en anglais).

[19] Par exemple, au Royaume-Uni, un consortium dirigé par l'université de Manchester, en collaboration avec l'université de Southampton, l'Office national des statistiques et le nouvel institut public sur l'ouverture des données (*Open Data Institute* - ODI), gère le réseau britannique sur l'anonymisation (UKAN) afin de permettre le partage de bonnes pratiques en la matière entre les secteurs public et privé. Le réseau a un site web (http://www.ukanon.net), présente des études de cas, et organise des stages et séminaires.

V. Champ d'application de la directive ISP: exceptions pour des motifs de protection des données à caractère personnel

La présente section donne des orientations sur le champ d'application de la directive ISP et, en particulier, sur les exceptions pour des motifs de protection des données.

5.1. Applicabilité du cadre général de protection des données à la réutilisation des ISP

Le considérant 21 de la directive ISP signale que «la présente directive devrait être mise en œuvre et appliquée dans le respect total des principes relatifs à la protection des données à caractère personnel». En outre, l'article 1er, paragraphe 4, prévoit que la directive ISP «laisse intact et n'affecte en rien le niveau de protection des personnes physiques à l'égard du traitement des données à caractère personnel».

5.2. Exceptions pour des motifs de protection de données à caractère personnel

La directive ISP prévoit que «la présente directive ne s'applique pas: […] aux documents qui, conformément aux règles d'accès en vigueur dans les États membres, ne sont pas accessibles…»[20].

En outre, la directive ISP, telle que modifiée, prévoit également des exceptions pour des motifs de protection des données. L'article 1er, paragraphe 2, point c quater), aborde les trois situations suivantes, qui sont toutes exclues du champ d'application de la directive ISP:

- documents dont l'accès est exclu en application de règles d'accès pour des motifs de protection des données à caractère personnel;
- documents dont l'accès est limité en application de règles d'accès pour des motifs de protection des données à caractère personnel, et
- parties de documents accessibles en vertu desdites règles qui contiennent des données à caractère personnel dont la réutilisation a été définie par la loi comme étant incompatible avec la législation concernant la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

5.3. Observations générales

Le groupe de travail «article 29» souligne qu'indépendamment du «principe de réutilisation» formulé dans la modification ISP, la réutilisation à des fins commerciales ou non commerciales en vertu de la directive ISP n'est pas toujours appropriée lorsque les ISP qui seront réutilisées contiennent des données à caractère personnel. Les décisions concernant la réutilisation de données à caractère personnel en vertu de la directive ISP devront être prises au cas par cas. Il faut également mettre en place des mesures juridiques, techniques et organisationnelles supplémentaires pour protéger les personnes concernées.

La réutilisation de données à caractère personnel accessibles au public est et devrait être limitée par:

- les dispositions générales de la législation applicable en matière de protection des données,
- (le cas échéant) des restrictions juridiques supplémentaires spécifiques, et
- des garanties techniques et organisationnelles mises en place pour protéger les données à caractère personnel.

[20] Voir directive ISP, article 1er, paragraphe 2, point c).

5.4. Documents dont l'accès est exclu

Cette disposition exclut du champ d'application de la directive ISP tous les documents dont l'accès est exclu, en application de règles d'accès de l'État membre, pour des motifs de protection des données à caractère personnel.

Contrairement aux législations sur la protection des données, qui sont harmonisées en grande partie sur la base de la directive 95/46/CE, les législations sur l'accès à l'information varient fortement d'un État membre à l'autre. Les règles d'accès demandent en général un test de comparaison qui évalue les intérêts protégés par les règles relatives à la protection des données et de la vie privée par rapport aux avantages d'une éventuelle ouverture et transparence. Vu les différences existantes, le résultat de l'exercice de comparaison varie d'un État membre à l'autre. Par exemple, dans certains États membres, les autorités fiscales peuvent publier certaines parties des déclarations de l'impôt sur les revenus de contribuables (publication soumise à des mesures juridiques, techniques et organisationnelles en vue de réduire au minimum les risques de mauvais usage), tandis que, dans d'autres, ces informations sont considérées comme relevant d'une exception et conservent, en général, un caractère privé.

Ceci dit, la législation nationale doit respecter l'article 8 de la Convention européenne des droits de l'homme (CEDH) et les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne («Charte de l'UE»). Cela implique, comme l'a déclaré la Cour de justice de l'UE dans ses arrêts *Österreichischer Rundfunk* et *Schecke*[21], qu'il faut établir que la divulgation est nécessaire et proportionnée au but légitime recherché.

Quoi qu'il en soit, lorsque l'accès aux données à caractère personnel contenues dans un document est exclu en vertu du droit de l'État membre concerné (y compris lorsque la législation nationale sur la transparence et l'ouverture ne prévoit pas l'accessibilité générale aux données à caractère personnel en question), lesdites données seront également exclues du champ d'application de la directive ISP.

Pour garantir une transparence et une sécurité juridique aux personnes concernées, la bonne pratique, chaque fois que c'est possible, consiste à adopter une approche proactive et à définir à l'avance les données à caractère personnel qui peuvent être rendues publiques. Les personnes concernées peuvent alors être informées, au moment de la collecte des données, de l'éventualité qu'une partie des données à caractère personnel qu'elles fournissent, ou qui feront l'objet d'un traitement ultérieur au cours de la procédure administrative, soient rendues publiques conformément à la législation sur la liberté d'information.

5.5. Documents dont l'accès est limité

Cette disposition exclut du champ d'application de la directive ISP tous les documents dont l'accès est limité, en application de règles d'accès de l'État membre, pour des motifs de protection des données à caractère personnel. Une fois encore, les règles d'accès peuvent varier d'un État membre à l'autre en ce qui concerne les données qui peuvent faire l'objet d'un accès limité et les types de restrictions applicables. C'est le cas, par exemple:

[21] Voir arrêt de la Cour de Justice du 20 mai 2003, Rundfunk, dans les affaires jointes C-465/00, C-138/01 et C-139/01, et du 9 novembre 2010, Volker und Markus Schecke, dans les affaires jointes C-92/09 et C-93/09.

- des collections d'archives nationales contenant des données à caractère personnel qui sont accessibles uniquement sous réserve de conditions d'accès spécifiques et de garanties supplémentaires (voir section IX ci-après);
- des collections de données de recherche contenant des données à caractère personnel qui sont accessibles uniquement sous réserve de conditions d'accès spécifiques et de garanties supplémentaires (voir section VIII ci-après);
- de certaines informations contenues dans des registres publics, les dossiers de tribunaux ou d'autres documents administratifs contenant des données à caractère personnel qui ne peuvent être accessibles qu'à des personnes ou organisations qui montrent un intérêt légitime, ou uniquement sous réserve d'autres conditions d'accès spécifiques et de garanties supplémentaires.

5.6. Parties de documents <u>accessibles</u> mais dont la réutilisation est illégale

Cette disposition exclut du champ d'application de la directive ISP les

- parties de documents
- accessibles en vertu des règles d'accès nationales
- qui contiennent des données à caractère personnel dont la réutilisation a été définie par la loi comme étant incompatible avec la législation sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Cette disposition confirme que, même lorsque certains documents contenant des données à caractère personnel sont entièrement accessibles, leur réutilisation peut toutefois être limitée pour des motifs de protection des données.

Le groupe de travail «article 29» insiste sur le fait que cette disposition de la directive ISP devrait être interprétée conformément à l'article 1er, paragraphe 4, de ladite directive, selon lequel la directive ISP «laisse intact et n'affecte en rien le niveau de protection des personnes physiques à l'égard du traitement des données à caractère personnel».

Le groupe de travail «article 29» saluerait comme une bonne pratique l'adoption de dispositions spécifiques dans le droit national qui préciseraient clairement (i) les données qui sont rendues publiques, (ii) à quelles fins et (iii), le cas échéant, dans quelle mesure et dans quelles conditions leur réutilisation est autorisée. Toutefois, lorsque de telles dispositions spécifiques n'existent pas, cela ne signifie pas que les données à caractère personnel accessibles au public peuvent toujours être réutilisées en vertu de la directive ISP.

En revanche, dans ces cas, la législation sur la protection des données (appliquée parallèlement à d'autres législations du domaine, comme celle sur l'accès aux documents) détermine si les données à caractère personnel peuvent être rendues disponibles à des fins de réutilisation dans ce cas particulier et, dans l'affirmative, avec quelles garanties supplémentaires. Si l'évaluation est positive, la réutilisation est autorisée, sous réserve de garanties spécifiques en matière de protection des données et de toutes les autres conditions énoncées dans la directive ISP (pour autant qu'elles ne portent pas atteinte à la législation sur la protection des données). Si ce n'est pas le cas, la réutilisation ne tombera pas sous le coup de la directive ISP.

Les exemples suivants peuvent illustrer les cas où s'applique cette exception à l'application de la directive ISP. Dans le premier exemple, les restrictions à la réutilisation sont clairement spécifiées dans la législation.

- Le droit fiscal d'un État membre peut prévoir que les déclarations d'impôt sur les revenus de tous les résidents du pays sont accessibles au public afin d'être examinées par tout autre résident sur demande, dans les locaux des autorités fiscales, sans nécessité de montrer un intérêt légitime. Le droit précise aussi clairement que les données ne peuvent faire l'objet d'un traitement ultérieur, par exemple qu'elles ne peuvent être publiées sur l'internet, combinées à d'autres données, ni faire l'objet d'une édition ultérieure. Une ONG demande l'accès et le droit de réutiliser la base de données de déclarations fiscales afin de les publier sur son site web. Dans ce cas, les données fiscales ne relèvent pas du champ d'application de la directive ISP et l'organisme du secteur public n'a pas l'obligation de rendre disponible l'ensemble de données à des fins de réutilisation en vertu de la directive ISP.

Dans de nombreux autres cas, cependant, les restrictions légales sont susceptibles d'être exprimées moins clairement et d'être moins catégoriques en termes de réutilisation. Typiquement, divers registres civils, commerciaux et de population, ainsi que d'autres bases de données permettent au public de consulter des données à caractère personnel, de plus en plus sous forme numérique via l'internet. L'accessibilité est souvent soumise à des garanties spécifiques, y compris des restrictions techniques concernant les capacités de recherche et le téléchargement massif. Les utilisateurs peuvent également se voir demander leur consentement aux modalités d'accès.

- Le droit fiscal d'un État membre peut prévoir que le nom des résidents qui ont des arriérés fiscaux au-delà d'un certain seuil pendant une longue période soit publié sur un site web spécial, pendant une période limitée, sous réserve de garanties techniques supplémentaires, notamment de restrictions en ce qui concerne le téléchargement en masse et les capacités de recherche. L'objectif de cette publication est d'encourager le paiement en temps opportun des impôts sur le revenu et de servir de sanction supplémentaire (en termes de réputation) pour ceux qui ne le font pas. Un consortium bancaire demande l'accès à ces données à des fins de réutilisation dans son système d'évaluation du crédit.

- Des lois spécifiques dans le secteur des soins de santé d'un État membre peuvent permettre, sous réserve de garanties, aux patients de vérifier, sur un site web spécial, si un médecin ou un autre professionnel particulier est frappé d'une interdiction d'exercer. Des garanties techniques s'appliquent, notamment des restrictions en ce qui concerne le téléchargement en masse et les capacités de recherche. Une organisation de défense des droits des patients souhaite avoir accès à ces informations à des fins de réutilisation en vue de créer un site web multilingue et plus convivial pour accéder aux mêmes données.

- Des lois spécifiques d'un État membre peuvent exiger la publication des noms des donateurs finançant des partis politiques au-delà d'un certain montant. Les informations qui peuvent révéler les opinions politiques des donateurs sont rendues publiques via un site web spécial. Des garanties techniques s'appliquent, notamment des restrictions en ce qui concerne le téléchargement en masse et les capacités de recherche. Un groupe d'activistes demande l'accès aux données en masse à des fins de réutilisation en vertu de la directive ISP afin de créer un nouveau site web avec des caractéristiques supplémentaires et des capacités de recherche améliorées.

- Le nom et l'adresse du propriétaire d'un bien immobilier sont accessibles au public via le registre cadastral d'un État membre, mais la navigation dans la base de données est limitée de sorte à ne permettre que la recherche d'un certain bien immobilier et non d'une certaine personne. Le téléchargement massif est également limité. Une entreprise commerciale

demande l'accès aux données en masse à des fins de réutilisation en vue de créer un site web plus convivial et à un prix plus compétitif.

- Les registres commerciaux d'un État membre permettent au public d'accéder à un large éventail de données à caractère personnel, notamment le nom, l'adresse et le spécimen de la signature des directeurs, ainsi que des informations concernant les propriétaires de certains types de sociétés. Les capacités de recherche font l'objet de certaines restrictions et le nombre d'éléments qui peuvent être téléchargés est limité. Les informations sont disponibles via un site web spécial, sous réserve du paiement d'une redevance. Une société commerciale demande l'accès à des données en masse à des fins de réutilisation en vue de créer un site web qui combine des informations provenant de plusieurs types de registres et d'offrir des informations améliorées à un prix plus compétitif.

Quoi qu'il en soit, l'organisme du secteur public concerné doit évaluer minutieusement l'impact sur la protection des données afin de décider des données qui peuvent être rendues disponibles à des fins de réutilisation en vertu de la directive ISP et, si c'est le cas, si la législation sur la protection des données requiert des conditions et des garanties spécifiques. Le «principe de réutilisation» n'est pas automatique et ne peut déroger aux dispositions applicables de la législation sur la protection des données.

Cette évaluation minutieuse est d'autant plus importante qu'en vertu de la directive ISP, l'organisme du secteur public ne doit en principe pas tenir compte de l'identité particulière du réutilisateur qui demande l'accès. Selon l'article 10 (Non-discrimination), «toute condition applicable en matière de réutilisation des documents est non discriminatoire pour des catégories comparables de réutilisation». En outre, aux termes de l'article 11 (Interdiction des accords d'exclusivité), «la réutilisation des documents est ouverte à tous les acteurs potentiels du marché […]. Les contrats ou autres accords conclus entre les organismes du secteur public détenteurs des documents et les tiers n'accordent pas de droits d'exclusivité».

Partant, lorsqu'ils décident d'autoriser ou non la réutilisation, les organismes du secteur public doivent prendre en considération la compatibilité de l'autorisation de la réutilisation dans le cadre d'une licence ouverte vis-à-vis non seulement du demandeur, mais également de toute personne qui demande des données. Cela requiert un niveau élevé de confiance quant au fait qu'aucun réutilisateur potentiel ne pourra faire mauvais usage des données à caractère personnel rendues disponibles.

La directive ISP n'exclut pas que les conditions applicables puissent autoriser le traitement à des fins spécifiques uniquement. L'organisme du secteur public doit alors décider si la réutilisation, par tout «acteur potentiel du marché», à ces fins, est compatible avec les finalités qu'il a spécifiées. La réutilisation potentielle des informations sur le paiement des impôts par des institutions financières, par exemple, à des fins d'évaluation du crédit, est pertinente étant donné qu'elles sont encore un réutilisateur potentiel, à l'aune du critère «toute personne». Partant, pour répondre aux préoccupations en matière de protection des données, en particulier pour garantir le respect du principe de limitation de la finalité, l'organisme du secteur public (ou le législateur) doit être habilité à limiter, le cas échéant, les finalités de la réutilisation.

VI. Réutilisation d'ensembles de données agrégées et rendues anonymes issues de données à caractère personnel

6.1. Quels sont les avantages de l'agrégation et de l'anonymisation pour la réutilisation des ISP?

À ce jour, les initiatives de réutilisation des ISP qu'ont lancées les organismes du secteur public, par le biais de «portails de données ouvertes» ou d'autres plateformes, ont généralement cherché à rendre disponibles à des fins de réutilisation des données agrégées et rendues anonymes, plutôt que des données à caractère personnel en tant que telles. Cette approche est en effet plus sûre et devrait être encouragée.

Les lois sur la protection des données ne permettent généralement pas aux organismes du secteur public de divulguer des données à caractère personnel collectées pour une autre finalité, généralement administrative[22]. Ainsi, dans ces cas, leur réutilisation dans le cadre d'initiatives de réutilisation d'ISP est également impossible. Les statistiques issues de données à caractère personnel, plutôt que les données à caractère personnel elles-mêmes, sont et devraient - en principe - être rendues disponibles à des fins de réutilisation. Il s'agit de la solution la plus efficace pour réduire au minimum les risques de divulgation involontaire de données à caractère personnel. Ces ensembles de données agrégées et rendues anonymes ne devraient pas permettre la ré-identification des personnes et, partant, ne devraient pas contenir de données à caractère personnel.

Décider du niveau d'agrégation approprié et des techniques spécifiques d'anonymisation à utiliser est une tâche ambitieuse. Si l'agrégation et l'anonymisation ne sont pas correctement réalisées, il se peut que la ré-identification à partir de ces ensembles de données soit malgré tout possible. En conséquence, la législation sur la protection des données a un grand rôle à jouer pour contribuer à déterminer le seuil à partir duquel il est «sûr» de divulguer des données agrégées et rendues anonymes dans le cadre d'une initiative d'ISP.

La directive 95/46/CE établit un seuil élevé pour l'anonymisation

Aux fins du présent document, le terme «anonymisation» renvoie aux données qui ne peuvent plus être considérées comme des données à caractère personnel au sens de l'article 2, point a), de la directive 95/46/CE. L'article 2, point a), définit les «données à caractère personnel» comme «toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale»[23].

Le considérant 26 de la directive 95/46/CE est également pertinent et prévoit en outre que «pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne».

Il faut souligner qu'un seuil élevé est ainsi fixé, qui sera examiné plus loin dans le présent avis. Si les données ne peuvent être rendues anonymes jusqu'à ce seuil, la loi sur la protection des données continue à s'appliquer. Cela signifie, entre autres, que si le seuil n'est pas atteint, la divulgation publique des informations (et toute utilisation ultérieure) doit être «compatible» avec la finalité pour

[22] Évidemment, le cas échéant, la législation sur la liberté d'information peut exiger la divulgation de données à caractère personnel, et l'intérêt pour la transparence et la disponibilité des informations dans certains cas peut primer les préoccupations en termes de protection des données et de la vie privée. Cette question évolue et pourrait conduire à des changements à l'avenir.

[23] Dans sa déclaration du 27 février 2013 sur les «discussions actuelles relatives au paquet de réformes sur la protection des données», le groupe de travail «article 29» a souligné qu'une «personne physique peut être considérée comme identifiable lorsqu'elle peut, dans un groupe de personnes, être distinguée des autres et, partant traitée différemment. Cela signifie que la notion d'identifiabilité englobe la distinction». La déclaration précise également que les «numéros d'identification, données de localisation, adresses IP, identifiants en ligne ou autres facteurs spécifiques concernant une personne physique devraient être considérés comme des données à caractère personnel».

laquelle les données sont collectées en vertu de l'article 6, paragraphe 1, point b), de la directive 95/46/CE. En outre, le traitement doit également avoir une base juridique appropriée, en vertu de l'article 7, points a) à f), de la directive 95/46/CE (par exemple, consentement ou nécessité de respecter la loi). Par contre, si les données ont été rendues anonymes au sens de l'article 2, point a), et du considérant 26 de la directive 95/46/CE, les règles relatives à la protection des données ne s'appliqueront plus et les réutilisateurs pourront réutiliser les données sans ces contraintes.

Une fois encore, il faut souligner qu'aux fins du présent avis, le terme «données rendues anonymes» renvoie aux données qui ne sont plus considérées comme des données à caractère personnel. Les données rendues anonymes devraient, en particulier, être distinguées des données qui ont été manipulées en utilisant différentes techniques pour réduire les risques de ré-identification des personnes concernées, mais qui n'ont pas atteint le seuil requis par l'article 2, point a), et le considérant 26 de la directive 95/46/CE[24]. Dans de nombreux scénarios, ces techniques ne sont appropriées que pour une divulgation limitée à des fins de réutilisation par des tiers contrôlés mais pas pour une totale divulgation publique et une réutilisation sous licence libre.

Il convient également de souligner que lorsque les données sont divulguées publiquement à des fins de réutilisation, les personnes qui peuvent y accéder ne font l'objet d'aucun contrôle. La probabilité qu'une «autre personne» dispose des moyens - et les utilise - pour ré-identifier des personnes, va augmenter très nettement. En conséquence, et indépendamment de l'interprétation du considérant 26 dans d'autres contextes, en ce qui concerne la mise à disposition de données à des fins de réutilisation en vertu de la directive ISP, le groupe de travail «article 29» tient à ce qu'il soit tout à fait clair qu'il faut veiller avec le plus grand soin à ce que les ensembles de données qui seront divulgués ne contiennent pas de données qui peuvent être ré-identifiées par des moyens susceptibles d'être raisonnablement utilisés par toute personne, y compris les réutilisateurs potentiels, mais également des tiers qui peuvent avoir intérêt à obtenir les données, par exemple les services répressifs.

Autres orientations concernant l'anonymisation et le concept de données à caractère personnel

Pour d'autres orientations sur l'anonymisation et le concept de données à caractère personnel, voir l'avis 4/2007 du groupe de travail «article 29» sur le concept de données à caractère personnel, adopté le 20 juin 2007 (WP 136). Le groupe de travail «article 29» pourra fournir d'autres orientations sur les techniques d'anonymisation dans un document séparé au cours du deuxième semestre 2013.

6.2. Quels sont les défis et les limites de l'anonymisation pour la réutilisation des ISP?

Les progrès de la technologie informatique moderne et la disponibilité omniprésente des informations rendent l'anonymisation de plus en plus difficile. La ré-identification des personnes est une menace de plus en plus présente et fréquente[25]. Dans la pratique, il existe une très grande zone

[24] La déclaration du 27 février 2013 souligne que «lorsqu'il est possible de ré-identifier une personne ou d'identifier (indirectement) une personne par d'autres moyens, les règles de protection des données continuent à s'appliquer».

[25] Voir, par exemple, «Transparent Government, Not transparent Citizens», un rapport préparé pour les services du gouvernement britannique par Kieron O'Hara de l'université de Southampton en 2011, dans lequel l'auteur alerte sur la capacité à identifier des personnes à partir de données rendues anonymes, en utilisant, entre autres, «l'identification en puzzle», et indique qu'il n'y a pas de solutions techniques complètes au problème de «dé-anonymisation» (disponible, en anglais, à l'adresse suivante: http://www.cabinetoffice.gov.uk/sites/default/files/resources/transparency-and-privacy-review-annex-b.pdf). Voir également *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* par Paul Ohm de la

d'ombre: un responsable du traitement qui divulgue des données peut estimer qu'un ensemble de données se présente sous une forme anonymisée, alors qu'un tiers peut encore identifier du moins une partie des personnes à partir des données, par exemple en utilisant d'autres informations accessibles au public, ou d'autres informations dont il dispose.

L'un des principaux facteurs de risque est le volume croissant de données en ligne et hors ligne, qu'elles soient accessibles au public ou qu'elles soient détenues par des organisations commerciales, et qui peuvent ensuite être utilisées pour établir le profil de personnes à des fins de publicité comportementale et pour un éventail croissant d'autres finalités. Lorsqu'on les considère sous l'angle des «énormes volumes de données» dont disposent déjà ces organisations, les ISP issues de données à caractère personnel et rendues disponibles à des fins de réutilisation pourraient augmenter la probabilité que les personnes puissent être identifiées ou que leurs profils puissent être enrichis, souvent à leur insu.

6.3. Qui devrait procéder à l'agrégation et à l'anonymisation, et quand?

Le responsable du traitement ou un tiers de confiance agissant pour le compte d'un ou plusieurs responsable(s) du traitement (et qui a également les aptitudes spécialisées nécessaires) devrait procéder à l'agrégation et à l'anonymisation le plus tôt possible. L'anonymisation ne peut être laissée à l'appréciation du réutilisateur, par exemple comme une condition d'octroi d'une licence. En outre, il convient de veiller à ce que l'éventuelle organisation tierce qui procède à l'agrégation et à l'anonymisation n'ait pas de conflit d'intérêts et assume clairement la responsabilité quant au fait que les données à caractère personnel seront uniquement utilisées pour procéder à l'anonymisation et que toutes les garanties nécessaires à cet effet seront mises en place. Le tiers doit également être en mesure de garantir l'effacement des données à caractère personnel dont sont issus les ensembles de données agrégées et rendues anonymes dès que ces données ne seront plus nécessaires à cette fin.

6.4. Évaluer les risques de ré-identification

Si les données ne peuvent être rendues anonymes au sens de l'article 2, point a), et du considérant 26 de la directive 95/46/CE, la législation sur la protection des données continue à s'appliquer.

Les responsables du traitement devraient déterminer si une personne peut être raisonnablement identifiée à partir de l'ensemble de données «rendues anonymes» qui sera mis à disposition à des fins de réutilisation et à partir d'autres données, autrement dit, si une organisation ou un particulier peut identifier une personne à partir des données en cours de divulgation - seules ou combinées à d'autres informations disponibles.

Comme expliqué à la section 6.1, le présent avis ne vise pas à fournir des orientations exhaustives et définitives sur la manière d'évaluer les risques de ré-identification. Il ne cherche pas non plus à fournir de définition concluante des termes «anonymisation» ou «données rendues anonymes». Toutefois, il rappelle que le lecteur peut trouver d'autres orientations dans des documents existants (y compris ceux mentionnés à la section 6.1) et que le sous-groupe «technologie» du groupe de travail «article 29» travaille actuellement sur les techniques d'anonymisation, comme le mentionnent les sections 6.1 et 2.2.

---

faculté de droit de l'université du Colorado, 57 UCLA Law Review 1701 (2010), disponible en ligne à l'adresse suivante: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (en anglais).

Cela dit, et sans viser l'exhaustivité, le groupe de travail «article 29» tient à souligner certains des facteurs/concepts utiles à prendre en compte lors de l'évaluation des risques de ré-identification, y compris, en particulier:

- les autres données disponibles, pour le grand public ou pour d'autres personnes ou organisations; le lien possible entre les données qui seront publiées et d'autres ensembles de données;
- la probabilité d'une tentative de ré-identification (certains types de données seront plus attrayants que d'autres aux yeux des intrus potentiels); et
- la probabilité que la ré-identification, si elle est tentée, soit couronnée de succès, compte tenu de l'efficacité des techniques d'anonymisation proposées[26].

Quelles «autres» informations existent?

Lorsque l'on détermine si une personne peut être indirectement identifiée, il faut voir si l'identification est possible en utilisant les données en question (dans le cas qui nous occupe, l'ensemble de données «rendues anonymes»), et des données et *autres informations* qui se trouvent en la possession de l'organisation ou du particulier qui tente la ré-identification, ou peuvent/sont susceptibles de tomber entre ses mains.

Les «autres informations» nécessaires à la ré-identification pourraient être des informations accessibles à certaines entreprises ou à d'autres organisations, y compris les services répressifs ou d'autres organismes du secteur public, à certaines personnes ou à tout le monde car elles ont été publiées sur l'internet, par exemple. Un exemple évident est le cas où des données accessibles au public - comme les listes électorales, les annuaires téléphoniques ou d'autres données facilement obtenues par une recherche sur le web - peuvent être combinées aux données «rendues anonymes» (de manière inadéquate), permettant l'identification d'une personne (par exemple, en utilisant sa date de naissance et son code postal).

Les risques de ré-identification peuvent augmenter lorsqu'une personne ou un groupe de personnes en sait déjà beaucoup sur une autre personne, par exemple un membre de la famille, un collègue, un contact sur un site de réseautage social, un médecin, un enseignement, un agent des forces de l'ordre ou un autre professionnel.

Toutefois, il importe de déterminer non seulement si la personne qui a des connaissances préalables peut identifier la personne concernée, mais également si elle apprendra quelque chose de nouveau à partir des informations obtenues par le biais de la ré-identification. Les deux exemples ci-après illustrent l'importance de cette distinction.

Exemple 1: statistiques sur la rougeole. Dans un cas, les données statistiques rendues anonymes peuvent révéler que dans la ville A, en 2012, x personnes ont contracté la rougeole. Aucune autre information n'est fournie et les informations données ne sont pas ventilées. Un médecin qui a contribué aux statistiques en fournissant des informations sur ses propres patients aux autorités sanitaires compétentes conserve, dans son bureau, des dossiers plus complets sur ces patients, soumis au secret médical. Le médecin pourrait facilement ré-identifier plusieurs patients à partir de l'ensemble de données statistiques. De même, une mère qui sait que son enfant a contracté la rougeole cette année-là pourrait facilement ré-identifier son enfant dans l'ensemble de données.

[26] Concernant les techniques d'anonymisation, voir le prochain avis du groupe de travail «article 29» à ce sujet.

Toutefois, ni la mère ni le médecin n'apprendrait rien d'autre que ce qu'elle ou il savait déjà avant la publication de l'ensemble de données rendues anonymes.

Exemple 2: toxicomanie et alcoolisme, abus sexuels et résultats scolaires. Cet exemple contraste avec le suivant. Une étude est réalisée concernant les corrélations entre la toxicomanie et l'alcoolisme des parents, les abus sexuels sur les enfants et les résultats scolaires. Les données de recherche prétendument «rendues anonymes» sont publiées avec de bonnes intentions mais sans que l'on ait minutieusement évalué les risques de ré-identification.

Les statistiques révèlent, notamment, qu'en ce qui concerne l'école A, où sont inscrits 500 élèves au total en 2012, 20 % d'entre eux (100 élèves) vivent dans un foyer où au moins un des parents est alcoolique ou toxicomane. Parmi ces derniers, dans 8 % des cas (8 élèves), l'enfant a été victime d'abus sexuels. Le rapport précise également qu'aucun autre élève n'a été victime d'abus sexuels dans l'école A.

Les chiffres révèlent également que dans 96 % des cas (96 élèves), les enfants dont les parents sont alcooliques ou toxicomanes éprouvent plus de difficultés à l'école (ils ont de «mauvais résultats», selon une norme académique pertinente). Toutefois, dans cette école particulière, seuls 50 % des victimes d'abus sexuels (4 élèves) éprouvent de grandes difficultés à faire leurs devoirs.

À l'école, chacun sait que X, un garçon brillant qui travaille dur, vit dans un milieu familial difficile, et que sa mère est alcoolique. Il est souvent tyrannisé par certains camarades de classe. Ces mêmes camarades apprennent maintenant, grâce aux statistiques relayées dans le journal de l'école, que X doit entrer dans les 50 % des enfants victimes d'abus sexuels qui n'ont pas de problème à l'école (ceux qui ont «de bons résultats»). Ainsi, ils ont appris de nouvelles informations (dans ce cas, très sensibles) à partir de l'ensemble de données rendues anonymes de manière inefficace.

Le risque que des informations soient combinées pour produire des données à caractère personnel augmente à mesure que la puissance de calcul et les techniques de corrélation de données se développent, et à mesure que des informations potentiellement «corrélables» deviennent publiques. En effet, la puissance de calcul double chaque année et le stockage de données, du fait également de la disponibilité de services d'informatique en nuage, est susceptible de devenir un produit de base. Ainsi, le risque de ré-identification par la corrélation de données est imprévisible car il est toujours impossible de déterminer avec certitude quelles données sont déjà disponibles et lesquelles pourront être divulguées à l'avenir.

En dépit de cette incertitude, les risques de ré-identification peuvent généralement être, du moins dans une certaine mesure, atténués en adhérant au principe de limitation des données, autrement dit, en garantissant que seules les données nécessaires à une finalité donnée sont divulguées.

La probabilité de tentative réussie de ré-identification: le test de l'«intrus motivé»

Le test de l'«intrus motivé» est un nouveau concept, qui doit encore être complètement éprouvé. Il peut être utile pour déterminer:

- si quelqu'un a la motivation pour procéder à la ré-identification, et
- si la ré-identification peut/est susceptible d'être couronnée de succès.

Le test de l'intrus motivé implique essentiellement de déterminer si un «intrus» pourrait procéder à la ré-identification *si* la motivation le poussait à essayer. L'«intrus motivé» est une personne (un particulier ou une organisation) qui souhaite identifier la personne concernée dont les données à

caractère personnel sont à l'origine des données rendues anonymes. Ce test vise à évaluer si l'intrus motivé peut y arriver. L'approche suppose que l'«intrus motivé» est compétent et a accès à des ressources proportionnelles à la motivation qu'il peut avoir pour la ré-identification.

Certains types de données présenteront un plus grand attrait que d'autres aux yeux d'un «intrus motivé». Par exemple, un intrus - de manière générale - pourrait être plus motivé à ré-identifier des données à caractère personnel si ces données:

- ont une valeur commerciale élevée (y compris sur le marché noir ou en dehors de l'Union européenne) et peuvent donc être achetées et vendues pour un profit financier[27];
- peuvent être utilisées pour le renseignement ou à des fins répressives;
- révèlent des informations sur des personnalités publiques susceptibles d'intéresser la presse;
- peuvent être utilisées à des fins politiques ou activistes (par exemple, dans le cadre d'une campagne contre une personne ou une organisation donnée);
- pourraient être utilisées pour des motifs personnels fondés sur de mauvaises intentions (par exemple, harcèlement, intimidation, ou simplement pour embarrasser un tiers);
- pourraient susciter la curiosité (par exemple, le souhait d'un riverain de découvrir qui a été impliqué dans un incident indiqué sur une carte de la criminalité).

S'il est utile de réfléchir aux éventuelles motivations des intrus potentiels, le groupe de travail «article 29» souligne que cette approche présente également des limites considérables:

- l'exercice peut dans une certaine mesure être spéculatif;
- en l'absence de «facteurs motivants» évidents tels que ceux décrits plus haut, l'exercice peut rassurer à tort et suggérer que des données à caractère personnel relativement anodines peuvent être rendues disponibles à des fins de réutilisation sans anonymisation efficace;
- les intrus peuvent faire preuve de sophistication et d'innovation et avoir «une longueur d'avance», trouvant des usages pour les données anonymisées qui ne sont pas évidents pour d'autres personnes;
- eu égard à l'expansion des analyses de «grands volumes de données», il y a un risque croissant qu'une fois anonymisées, des données apparemment anodines puissent, combinées à d'autres informations, poser finalement des risques plus sérieux.

6.5. Test de ré-identification

Dans certaines circonstances, il peut être difficile de déterminer le risque de ré-identification, en particulier lorsqu'un tiers peut utiliser des méthodes statistiques complexes pour mettre en concordance différentes données rendues anonymes. Partant, dans le cadre de l'évaluation générale du risque de ré-identification, la bonne pratique veut que l'on utilise le test de ré-identification - un type de test du «stylo» ou test de «pénétration» - pour détecter toute vulnérabilité à la ré-identification et y faire face. Il consiste à tenter de ré-identifier des personnes à partir des ensembles de données dont la divulgation est prévue.

[27] Cela peut englober, par exemple, des données transactionnelles ou d'autres données comportementales à partir desquelles il est possible de déduire des profils de consommateurs individuels, qui peuvent ensuite être utilisés à des fins publicitaires ou de différenciation des prix; des informations financières ou autres permettant le vol d'identité; des informations sensibles qui peuvent être utilisées pour faire chanter des personnes ou les soumettre à des discriminations; des informations médicales qui peuvent être utilisées par des compagnies d'assurances, par exemple, pour refuser une couverture en raison de la préexistence d'une affection médicale; des informations permettant de tirer des conclusions concernant la solvabilité, qui pourraient être utilisées pour évaluer les risques de crédit; etc.

La première étape du test de ré-identification consiste à examiner les ensembles de données que l'organisme du secteur public a publiés ou a l'intention de publier. La deuxième consiste à tenter de déterminer si d'autres données disponibles - à caractère personnel ou non - pourraient être corrélées aux données pour conduire à la ré-identification. Les «tests de pénétration» ciblés, en particulier, devraient contribuer à évaluer les risques d'identification en puzzle, à savoir le recoupement de différentes informations pour créer une image plus complète d'une personne.

Le test de ré-identification ne devrait évidemment pas être considéré comme une panacée et ne devrait pas donner un faux sentiment de sécurité. Tout d'abord, il pourrait être difficile à réaliser étant donné qu'il requiert souvent une importante expertise technique et des outils adéquats, ainsi qu'une connaissance des autres données disponibles. Ensuite, les responsables du traitement doivent également savoir que le risque de ré-identification peut changer au fil du temps. Par exemple, des techniques et outils d'analyse des données de plus en plus puissants et abordables sont aujourd'hui disponibles, et la corrélation avec d'autres ensembles de données devient de plus en plus facile à mesure que des volumes de plus en plus grands de données sont générés. Partant, les organisations devraient procéder à un examen périodique de leur politique de divulgation des données et des techniques d'anonymisation des données. En outre, les décisions ne devraient jamais se baser uniquement sur les menaces actuelles, mais également sur les menaces futures prévisibles.

Après avoir procédé à l'évaluation du risque de ré-identification visé à la section 6.4 et - le cas échéant - au test de ré-identification, l'organisme du secteur public peut déterminer si l'ensemble de données peut être considéré ou non comme ayant été rendu anonyme, en d'autres termes, s'il ne contient plus de données à caractère personnel au sens de l'article 2, point a), et du considérant 26 de la directive 95/46/CE. Si c'est le cas, l'ensemble de données peut être divulgué sans contraintes en matière de protection des données[28]. Par contre, si un test est couronné de succès, les données concernées ne peuvent pas (ou plus) être disponibles en tant que données rendues anonymes, mais doivent être considérées comme des données à caractère personnel (et, partant, leur divulgation n'est pas possible, ou n'est possible que sous réserve des exigences examinées à la section VII).

6.6. Rappel des ensembles de données compromis

Si la ré-identification de données à partir d'un ensemble de données ouvertes est avérée, l'organisme du secteur public qui fournit l'ensemble de données doit pouvoir interrompre le flux de données ou effacer l'ensemble de données du site web proposant des données ouvertes. Dans ce dernier cas, l'organisme du secteur public doit également informer les réutilisateurs et leur demander d'arrêter le traitement et d'effacer toutes les données provenant de l'ensemble de données compromis. Dans la mesure où il sera difficile d'informer tous les réutilisateurs dans le cadre d'un régime de licence ouvert conforme à la directive ISP, les organismes publics doivent prendre des mesures raisonnablement efficaces pour régler cette question. Si un rappel arrive souvent trop tard pour éviter le dommage, c'est une étape nécessaire pour limiter l'impact négatif sur les personnes concernées.

[28] Voir, toutefois, la section 10.3 (Conditions de licence pour les ensembles de données rendues anonymes) et, en particulier, la nécessité de mettre en place des garanties pour pouvoir continuer à faire en sorte que les personnes physiques ne puissent pas être ré-identifiées.

VII. Ouverture des données à caractère personnel à des fins de réutilisation

7.1. Exemples de données à caractère personnel accessibles au public divulguées par des organismes du secteur public

Si la mise à disposition d'ensembles de données rendues anonymes est le scénario typique des initiatives de réutilisation d'ISP, dans certains cas, les organismes du secteur public peuvent également rendre disponibles des données à caractère personnel à des fins de réutilisation.

La plupart des registres accessibles au public, comme les registres cadastraux ou les registres des entreprises, contiennent de grandes quantités de données à caractère personnel et sont, vu les initiatives d'administration en ligne, de plus en plus accessibles en ligne. Il y a également de nombreux autres exemples où les législateurs de certains États membres ont établi une base juridique pour mettre à disposition des données à caractère personnel sur l'internet ou à la demande. Il peut s'agir, par exemple[29], des données suivantes:

- dépenses, salaires ou déclarations de conflit d'intérêts de certains fonctionnaires, ou bénéficiaires d'aides d'État (par exemple, de subventions agricoles),
- noms des organisations ou particuliers qui font des dons à des partis politiques,
- déclarations fiscales de particuliers[30],
- arrêts et décisions de tribunaux (où les noms des parties et d'autres personnes sont parfois effacés ou remplacés par des initiales pour réduire le risque de ré-identification),
- listes électorales,
- rôles de tribunaux (c'est-à-dire les calendriers quotidiens des audiences relatives aux affaires examinées par un tribunal).

Dans chacun de ces cas, les organismes du secteur public ou les législateurs peuvent déterminer de manière proactive s'ils souhaitent rendre ces données disponibles à des fins de réutilisation (par exemple, pour améliorer des services publics, tels que la fourniture d'accès à des registres cadastraux ou à des registres d'entreprises). Les réutilisateurs potentiels peuvent également contacter les organismes du secteur public pour demander la réutilisation des données. Dans certains autres cas, il se peut également que les réutilisateurs potentiels prennent simplement les données à caractère personnel qui sont déjà disponibles en ligne et les utilisent sans nécessairement contacter l'organisme du secteur public qui a divulgué les informations. Dans les trois cas, les réutilisateurs doivent évidemment respecter la législation sur la protection des données lorsqu'ils traitent des données à caractère personnel.

7.2. Différences entre les règles nationales en matière d'accès

Les obligations légales de rendre accessibles au public certaines données à caractère personnel varient fortement d'un État membre à l'autre du fait des différentes traditions juridiques et culturelles. Certains États membres disposent d'une base juridique pour la mise à disposition de certaines données à caractère personnel, tandis que d'autres, dans la même situation, interdisent la divulgation des mêmes données. La directive ISP reconnaît et indique clairement qu'elle s'appuie

[29] Voir également les exemples donnés à la section V, dans le cadre de la discussion sur le champ d'application de la directive ISP.

[30] Voir, par exemple, l'arrêt de la Cour de justice du 16 décembre 2008 dans l'affaire C-73/07, Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy et Satamedia Oy.

sur les régimes d'accès en vigueur dans les États membres et ne modifie pas les règles nationales en matière d'accès aux documents[31].

7.3. Nécessité d'évaluer l'impact sur la protection des données et d'avoir des garanties appropriées

En règle générale, il est absolument nécessaire d'adopter une approche prudente lorsque la mise à disposition de données à caractère personnel à des fins de réutilisation est envisagée. Le groupe de travail «article 29» recommande en particulier d'évaluer minutieusement l'impact sur la protection des données avant de publier un ensemble de données (ou avant d'adopter une loi qui exige leur publication), en appréciant également les possibilités de réutilisation et l'impact potentiel de celle-ci. D'une manière générale, il faut éviter d'autoriser l'ouverture de données à caractère personnel à des fins de réutilisation dans le cadre d'une licence ouverte sans soumettre la réutilisation à des restrictions techniques et juridiques.

7.4. Importance d'un régime de licence

Le groupe de travail «article 29» recommande également qu'un régime de licence rigoureux soit mis en place et correctement mis en œuvre afin de garantir que les données à caractère personnel ne seront pas utilisées à des fins incompatibles avec la finalité première - par exemple, pour des messages commerciaux non sollicités ou d'autres finalités que les personnes concernées jugeraient intempestives, inappropriées ou répréhensibles.

7.5. Importance d'une base juridique solide pour la publication et la réutilisation

Le groupe de travail «article 29» rappelle l'importance d'établir une base juridique solide pour la publication de données à caractère personnel, qui tienne compte des règles pertinentes en matière de protection des données, notamment des principes de proportionnalité, de minimisation des données et de limitation de la finalité.

Le groupe de travail «article 29» recommande que toute loi qui demande un accès public à des données énonce clairement les finalités de la divulgation des données à caractère personnel. Si ce n'est pas le cas, ou si seuls des termes généraux et vagues sont employés, la sécurité juridique et la prévisibilité en souffriront. En particulier, pour toute demande de réutilisation, l'organisme du secteur public et les réutilisateurs potentiels éprouveront de grandes difficultés à déterminer la finalité première de la publication et, ensuite, les autres finalités qui seraient compatibles avec cette finalité. Comme cela a été dit précédemment, même si les données à caractère personnel sont publiées sur l'internet, cela n'implique pas qu'elles peuvent faire l'objet d'un traitement ultérieur pour toute autre finalité.

Toute réutilisation ultérieure doit, dans ces cas, reposer sur une base juridique appropriée (par exemple, un consentement ou une obligation légale) en vertu de l'article 7, points a) à f), de la directive 95/46/CE, et elle doit respecter tous les autres principes de protection des données.

7.6. Limitation de la finalité

Il est compliqué d'appliquer efficacement le principe de limitation de la finalité en cas de réutilisation d'ISP. D'une part, l'idée même et la force motrice de l'innovation qui sous-tendent le concept de «données ouvertes» et de réutilisation d'ISP sont que les informations devraient être

[31] Cela dit, comme expliqué dans la section 5.4, la législation nationale doit être conforme à l'article 8 de la CEDH et aux articles 7 et 8 de la Charte de l'UE, tels qu'interprétés par la jurisprudence pertinente.

disponibles à des fins de réutilisation pour des nouveaux produits et services innovants et, partant, pour des finalités qui ne sont pas préalablement définies et ne peuvent donc être clairement prévues. La directive ISP requiert également que la licence n'impose pas de restrictions excessives en matière de réutilisation.

D'autre part, la limitation de la finalité est un principe clé de la protection des données et elle requiert que les données à caractère personnel qui ont été collectées pour une finalité spécifique ne soient pas utilisées ultérieurement pour une autre finalité, incompatible[32]. Ce principe s'applique également aux données à caractère personnel accessibles au public. Le simple fait qu'elles soient accessibles au public pour une finalité spécifique ne signifie pas qu'elles soient susceptibles d'être réutilisées pour toute autre finalité.

Par exemple, les dépenses de hauts fonctionnaires sont publiées sur l'internet pour garantir la transparence, l'autorisation d'une réutilisation de ces données pour d'autres finalités par tout membre du public peut se révéler non compatible.

Comme expliqué plus en détail dans l'avis 3/2013 sur la limitation de la finalité (voir section 3.2.2 et annexe 1), il faut prendre en considération plusieurs facteurs pour déterminer si le traitement ultérieur des données à caractère personnel est incompatible avec les finalités pour lesquelles ces données ont été collectées. Il faut tenir compte en particulier des éléments suivants:

(a) la relation entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur;
(b) le contexte dans lequel les données à caractère personnel ont été collectées et les attentes raisonnables des personnes concernées à propos de leur utilisation ultérieure;
(c) la nature des données à caractère personnel et l'impact du traitement ultérieur sur les personnes concernées;
(d) les garanties appliquées par le responsable du traitement pour assurer un traitement équitable et éviter tout impact excessif sur les personnes concernées.

Ces facteurs clés doivent être pris en considération pour décider de divulguer ou non des données à caractère personnel, ainsi que dans chaque cas de réutilisation de ces données. Quelques exemples sont fournis ci-après:

- Un organisme du secteur public publie, dans un répertoire, les coordonnées de ses fonctionnaires, notamment leur nom, leur titre, leur adresse et leur numéro de téléphone professionnels. Ce répertoire vise clairement - quoique non expressément - à aider le public à identifier la personne à contacter pour effectuer une démarche ou régler d'autres questions officielles. Un réutilisateur souhaite «récupérer» le contenu dudit répertoire, l'associer aux adresses et numéros de téléphone privés des fonctionnaires (lorsqu'ils sont accessibles au public, par exemple, dans un annuaire téléphonique), et publier les adresses et numéros de téléphone privés et professionnels sur une carte interactive pour montrer où les fonctionnaires vivent et travaillent. Cette combinaison et cette réutilisation de données doivent être considérées comme incompatibles avec la finalité première. Un fonctionnaire, dont les coordonnées professionnelles sont divulguées pour que le public puisse le contacter, ne s'attend raisonnablement pas à ce que ces informations soient ensuite corrélées avec d'autres données qu'il a rendues publiques pour une autre finalité non liée à son travail.

[32] Ce n'est que dans des cas exceptionnels - sous réserve des garanties strictes prévues à l'article 13 de la directive 95/46/CE - que les données peuvent être utilisées d'une manière incompatible avec les finalités définies lors de la collecte. Voir la section III, point 3, de l'avis 3/2013 sur la limitation de la finalité.

- En vertu du droit national, dans certains États membres, les faire-part de mariage sont publics et peuvent être consultés par tous. Cette publication vise à notifier la volonté du couple fiancé de se marier et à permettre aux personnes intéressées de s'y opposer. Le fait que les données à caractère personnel contenues dans la publication des faire-part de mariage soient mises à la disposition de tous ne permet toutefois pas à des tiers d'utiliser ces informations pour envoyer des messages commerciaux au couple. Cette autre utilisation serait inadéquate, puisque la finalité de la divulgation des faire-part de mariage est de permettre la présentation d'éventuelles objections au mariage, comme le prévoit la loi.

7.7. Finalités commerciales et non commerciales

L'avis 7/2003 souligne que les activités commerciales sont une des principales motivations de la réutilisation des ISP, contrairement à l'accès à l'information, là où les législations relatives à la liberté de l'information ont pour but de garantir la transparence, l'ouverture et l'obligation de rendre des comptes aux citoyens.

L'avis 7/2003 souligne également que les «citoyens utilisent, normalement, lesdites informations à des fins personnelles et non commerciales». Cette déclaration doit être actualisée à la lumière de l'expérience acquise entre-temps en matière de réutilisation des ISP. L'expérience engrangée avec les initiatives de données ouvertes a révélé que la réutilisation des ISP peut également contribuer fortement à renforcer la transparence et la responsabilité et conduire à une meilleure utilisation des services publics. La distinction entre la réutilisation à des fins commerciales ou non commerciales ne devrait pas être décisive quand on examine la compatibilité de l'utilisation ultérieure des données à caractère personnel. L'évaluation de ladite compatibilité ne devrait pas se fonder avant tout sur le fait que le modèle économique d'un réutilisateur potentiel se base ou non sur le profit.

Il faut soigneusement évaluer si les finalités et les modalités d'un traitement ultérieur des données sont compatibles avec les finalités premières, au regard des critères examinés à la section 7.6. Dans le cas de la réutilisation des ISP, cela conduira inévitablement à l'examen d'un éventail de scénarios de traitement, et non d'un seul.

7.8. Proportionnalité et autres préoccupations

La proportionnalité est un autre principe clé énoncé dans la directive 95/46/CE[33]. Il existe de nombreuses méthodes et modalités différentes pour rendre des données à caractère personnel accessibles au public. Certaines d'entre elles peuvent être plus intrusives que d'autres et présenter des risques plus importants. Partant, certaines peuvent être jugées appropriées, et d'autres non.

Comme pour la finalité, des préoccupations existent quant au contrôle du traitement ultérieur des données et à la garantie du respect d'autres principes définis dans la législation sur la protection des données, notamment la proportionnalité. Lorsque les données sont rendues publiques, en particulier sur l'internet, il est très difficile de limiter efficacement leur utilisation et de garantir le respect de la législation sur la protection des données.

[33] Voir article 6, paragraphe 1, point c), de la directive 95/46/CE.

Certains des défis que pose le respect de la législation sur la protection des données sont:

- comment garantir l'actualisation et l'exactitude des données qui sont déconnectées de la source première;
- comment garantir que l'utilisation des données à caractère personnel reste limitée aux fonctionnalités prévues pour la finalité première de la publication;
- comment garantir l'effacement en temps opportun des données si la publication de données à caractère personnel était uniquement prévue pour une durée limitée[34];
- comment garantir l'exercice des droits des personnes à l'égard des données à caractère personnel rendues disponibles à des fins de réutilisation (y compris le droit de demander la correction, l'actualisation ou l'effacement).

7.9. Restrictions juridiques et/ou techniques à la réutilisation

Parfois, la législation ou la conception technique des systèmes limite des opérations de traitement spécifiques ou établit d'autres garanties qui limitent l'utilisation des registres publics (par exemple, elles limitent la possibilité de télécharger l'intégralité du registre ou restreignent les recherches sur la base du nom et du prénom d'une personne). Dans ce cas, la réutilisation devrait en principe être autorisée uniquement sous réserve du respect ces conditions et limitations spécifiques.

Dans ce contexte, il importe d'examiner soigneusement les mesures - y compris juridiques et techniques - qui pourraient être mises en place pour contribuer à garantir qu'une réponse sera apportée aux préoccupations concernant la protection des données, y compris celles énoncées dans la section 7.8. Il importe en particulier d'examiner la manière dont les réutilisateurs accéderont aux données - par exemple, par une fonction de téléchargement en masse ou une interface personnalisée proposant des capacités d'accès limitées dans certaines conditions. À ce sujet, il est crucial de savoir quelles mesures de sécurité supplémentaires seront mises en place, comme un système de vérification «captcha[35]» pour empêcher un accès automatique et réduire au minimum le risque de récupération de l'intégralité d'une base de données. L'utilisation de mesures techniques spécifiques pourrait contribuer à réduire le mauvais usage des données à caractère personnel et les impacts négatifs sur les personnes concernées qui pourraient découler d'un accès illimité et inconditionnel des réutilisateurs à l'intégralité de l'ensemble de données.

Fait important, dans de nombreux cas, il peut être nécessaire de garantir que les réutilisateurs ne pourront réaliser des recherches ciblées qu'au moyen de technologies visant à prévenir les téléchargements massifs de fichiers de données, comme les interfaces de programmation d'applications («API»). Cela peut contribuer à garantir la proportionnalité de l'utilisation et réduire les risques de mauvais usages de bases de données intégrales. En outre, ces interfaces personnalisées peuvent contribuer à garantir que les données seront toujours actualisées et qu'elles ne seront plus disponibles via l'API lorsque l'organisme du secteur public concerné en aura décidé ainsi. D'autre part, elles peuvent limiter les modalités selon lesquelles un réutilisateur peut réutiliser les données.

---

[34] Voir, par exemple, l'arrêt de la Cour de justice dans l'affaire Volker und Markus Schecke GbR contre Land Hessen (affaires jointes C-92/09 et C-93/09), point 31: «il serait impossible de retirer les données d'Internet après l'expiration de la période de deux ans prévue à l'article 3, paragraphe 3, du règlement n° 259/2008».

[35] Un «captcha» (forme de test de Turing permettant de différencier de manière automatisée un utilisateur humain d'un ordinateur) est un test de système de défi-réponse conçu pour différencier un utilisateur humain de programmes automatisés. Un captcha différencie un humain d'un ordinateur en fixant une certaine tâche facile à réaliser pour la plupart des humains mais plus difficile pour les programmes informatiques actuels.

7.10. Exactitude, actualisation et effacement

Une autre question spécifique consiste à savoir à ce qui se passe si des données à caractère personnel sont publiées ou rendues accessibles au public d'une autre manière pour une période limitée. L'article 6, paragraphe 1, point e), de la directive 95/46/CE prévoit que les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement. Le considérant 18 de la directive ISP précise également que «si l'autorité compétente décide de ne plus mettre à disposition certains documents en vue de leur réutilisation ou de ne plus les mettre à jour, elle devrait rendre sa décision publique dans les meilleurs délais, si possible sous forme électronique».

Il est toutefois difficile, voire impossible parfois, de garantir que les données soient effacées ou éliminées lorsqu'elles ont été publiées et rendues disponibles à des fins de réutilisation.

À cet égard, il peut y avoir une solution - certes incomplète - si les données ne sont pas rendues disponibles sous une forme téléchargeable, uniquement via une API personnalisée et sous réserve de certaines restrictions et mesures de sécurité, comme indiqué plus haut.

VIII. Données de recherche

Il est important ici d'établir une distinction entre, d'une part, la publication de données rendues anonymes (voir section VI) et, de l'autre, l'accès limité. Le programme d'ouverture de données se base clairement sur l'accessibilité publique des données. Toutefois, bon nombre de recherches (la recherche scientifique, à des fins commerciales ou non commerciales, mais également d'autres types de recherches) s'accompagnent de la divulgation de données au sein d'une communauté fermée. Dans cette communauté, un nombre limité de chercheurs ou d'institutions a accès aux données, il est possible de limiter la divulgation ou l'utilisation ultérieure des données, et la sécurité de ces dernières peut être garantie.

Un accès limité est particulièrement important pour la manipulation de données à caractère personnel (souvent sous forme pseudonymisée[36]) issues de données sensibles et lorsqu'il y a un risque élevé de ré-identification. Il peut subsister des risques liés à la divulgation à accès limité, mais ils sont moins importants et peuvent être atténués lorsque les données sont divulguées au sein d'une communauté fermée travaillant avec des règles établies.

Un problème que rencontrent souvent ceux qui utilisent des données à des fins de recherche est que, d'une part, ils veulent que les données soient riches, granulaires et suffisamment utilisables pour les finalités qu'ils poursuivent et que, d'autre part, ils veulent s'assurer que la ré-identification soit impossible. D'un côté, les données pseudonymisées au niveau personnel (par exemple, simplement codées) peuvent être très précieuses pour les chercheurs du fait de leur granularité personnelle et parce que les dossiers pseudonymisés de différentes sources peuvent être rapprochés relativement aisément. Toutefois, cela signifie également qu'il y a un risque élevé de ré-identification: la possibilité de lier plusieurs ensembles de données (pseudonymisés ou non) à la même personne peut être un précurseur de l'identification ou peut permettre une identification directe.

[36] Voir de nouveau l'avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007 (WP 136), en particulier aux pages 13-23 (abordant les «données pseudonymisées», les «données codées» et les «données anonymes», pp. 19-23). La question des informations «concernant» une personne physique est examinée aux pages 10-13. Il convient également de noter, comme le mentionne le présent avis à la page 3, que le groupe de travail «article 29» travaille actuellement à l'élaboration d'autres orientations sur les techniques d'anonymisation.

En conséquence, il faut une évaluation minutieuse et des précautions supplémentaires avant de publier des ensembles de données pseudonymisées ou de les rendre disponibles à des fins de réutilisation. En général, plus les données sont détaillées, personnelles et corrélables, plus l'accès aux données devrait être limité et contrôlé. Plus les données sont agrégées et moins elles sont corrélables, plus il est probable qu'elles puissent être publiées et rendues disponibles à des fins de réutilisation sans risques notables.

Il s'agit d'une question complexe et en constante évolution, et il serait inopportun de refuser catégoriquement la publication et la réutilisation de tous les ensembles de données qui ne satisfont pas au seuil élevé d'«anonymisation» décrit à la section VI. Ceci dit, si une analyse au cas par cas et une évaluation minutieuse sont toujours souhaitables, en règle générale, le groupe de travail «article 29» estime que la divulgation dans les conditions prévues par la directive ISP d'ensembles de données personnels, ou d'autres ensembles de données qui présentent un risque notable de ré-identification, sera souvent inappropriée.

En outre, il importe de souligner que si certains de ces ensembles de données doivent néanmoins être publiés et rendus disponibles, après une évaluation minutieuse des risques et des avantages, la divulgation et toute réutilisation ultérieure doivent être effectuées dans le total respect de la législation sur la protection des données (voir section VII). Il en est ainsi parce que ces données, en dépit de certaines mesures (parfois très importantes) prises pour réduire les risques de ré-identification, continuent à être considérées comme des données à caractère personnel.

IX. Archives historiques

Les archives historiques et les musées présentent également des caractéristiques spécifiques qui requièrent des garanties spécifiques. Dans de nombreux cas, en fonction de facteurs tels que l'ancienneté et le caractère sensible des données et le contexte de la collecte, d'autres options - comme le fait de permettre un accès limité uniquement sous réserve d'une obligation de confidentialité - peuvent être plus appropriées que la numérisation et la publication sans restrictions sur l'internet des données à des fins de réutilisation.

En ce qui concerne les archives, il importe également de souligner que si la nature sensible des données diminue généralement au fil du temps, la divulgation inappropriée de vieux dossiers archivés durant des décennies pourrait encore avoir un effet très néfaste sur la personne physique directement concernée, mais également sur d'autres, comme des membres de la famille ou des descendants. Cela vaut en particulier pour des données hautement sensibles. Par exemple, la divulgation d'un casier judiciaire peut continuer à stigmatiser une personne physique et à gêner sa réinsertion. En outre, les informations concernant une personne décédée qui aurait été un agent secret ou collaborateur d'un régime d'oppression, un pédophile, un criminel, une personne souffrant d'une maladie mentale donnant lieu à une stigmatisation ou d'une maladie héréditaire, peuvent également toutes avoir un impact négatif sur la famille (par exemple, le conjoint survivant, les enfants ou d'autres descendants) de la personne décédée. Les échantillons d'ADN de personnes décédées, qui sont parfois conservés dans les archives d'hôpitaux publics, pourraient également devoir être protégés pour des raisons similaires. Partant, ces informations, même si elles concernent des personnes décédées, peuvent devoir être protégées par la législation sur la protection des données et/ou d'autres lois protégeant les droits fondamentaux, selon le cas.

Les États membres disposent souvent de lois spécifiques régissant l'accès aux archives nationales, aux archives de périodes historiques récentes présentant un intérêt particulier (comme les archives témoignant de la collaboration avec des régimes d'oppression), et aux dossiers conservés par les

tribunaux[37]. Ces lois requièrent souvent des mesures de sécurité appropriées et des restrictions d'accès, ainsi que d'autres garanties visant à soupeser les intérêts en jeu et à garantir l'accessibilité de certaines données à caractère personnel pour des recherches historiques, des enquêtes de journalisme et à des fins de transparence, tout en garantissant que les divulgations, le cas échéant, soient limitées de manière à ne pas porter préjudice à la vie privée et familiale, ni à la dignité, des personnes concernées.

Concernant la «limitation de la finalité», il convient de signaler que les archives historiques conservent généralement des informations à des fins de recherches historiques. Ces finalités diffèrent de celles pour lesquelles les données ont été initialement collectées. Les documents qui termineront dans les collections d'archives ont été créés à l'origine à des fins administratives spécifiques par les différents organismes du secteur public. En général, après un certain temps, lorsque le document n'est plus nécessaire pour la finalité administrative première, un processus de sélection est appliqué et les documents qui sont considérés comme ayant une valeur «historique» sont transférés aux archives historiques. La question qui se pose ici est de savoir pour quelles finalités les données à caractère personnel stockées dans les archives devraient être rendues disponibles à des fins de réutilisation. Dans ce contexte, il est important de procéder à une évaluation minutieuse, qui tienne compte de la valeur potentielle de la mise à disposition des documents d'archive à des fins de réutilisation, mais également de l'impact potentiel sur les droits, les libertés et la dignité des personnes concernées.

Dans l'ensemble, on peut conclure que si la numérisation de certains dossiers contenant des données à caractère personnel et leur mise à disposition à des fins de réutilisation peuvent être appropriées dans certaines situations, et que certaines données peuvent également être divulguées sous une forme rendue anonyme, dans d'autres cas, il est essentiel de restreindre la divulgation et la réutilisation des données à caractère personnel, et d'adopter des mesures de sécurité adéquates pour protéger ces données. Une évaluation minutieuse de l'impact sur la protection des données devrait garantir qu'aucune collection d'archives en soit rendue disponible à des fins de réutilisation avant que soit exclu tout impact négatif potentiel sur les personnes concernées ou que les éventuels risques aient été réduits à un minimum acceptable. Le secteur des archives pourrait également envisager de rédiger des codes de conduite ou de modifier les codes existants afin d'expliquer les bonnes pratiques.

X. Licence de réutilisation de données à caractère personnel

10.1. Dispositions pertinentes de la directive ISP

Le considérant 15 de la directive ISP prévoit que «assurer la clarté et l'accessibilité publique des conditions de réutilisation des documents du secteur public est une condition préalable du développement d'un marché de l'information à l'échelle de la Communauté. Il importe, dès lors, de porter clairement à la connaissance des réutilisateurs potentiels l'ensemble des conditions applicables en matière de réutilisation de documents. Les États membres devraient encourager la création de répertoires des documents disponibles, accessibles en ligne s'il y a lieu, de manière à promouvoir et à faciliter les demandes de réutilisation».

[37] D'autres exemples sont, notamment, les archives des registres d'état civil qui contiennent, dans certains États membres, des informations concernant, entre autres, la cause du décès, le changement de sexe, le nom du partenaire (dont on peut déduire l'orientation sexuelle) ou une éventuelle adoption. L'accès à ces archives est également soumis à des conditions spécifiques.

Le considérant 26 de la modification ISP prévoit par ailleurs que «en ce qui concerne une éventuelle réutilisation du document, les organismes du secteur public peuvent, s'il y a lieu, imposer des conditions par le biais d'une licence…» et que les «États membres devraient encourager l'utilisation de formats ouverts, lisibles par machine».

En outre, l'article 8, paragraphe 1, prévoit que «les organismes du secteur public peuvent autoriser la réutilisation sans conditions ou peuvent imposer des conditions, le cas échéant par le biais d'une licence. Ces conditions ne limitent pas indûment les possibilités de réutilisation et ne sont pas utilisées pour restreindre la concurrence».

10.2. Licence et protection des données

Les licences sont un élément essentiel des règles en matière d'ISP. Elles peuvent également affecter la manière dont les données à caractère personnel sont traitées et devraient figurer parmi les garanties appliquées lorsque des données à caractère personnel (ou des données rendues anonymes issues de données à caractère personnel) sont mises à disposition à des fins de réutilisation. Les licences ne portent pas atteinte à l'obligation de respecter la législation sur la protection des données, mais l'intégration, dans les conditions de la licence, d'une clause relative à la protection des données contribuerait à garantir le respect de cette législation en ajoutant une dimension de «force exécutoire». Une telle clause contribuerait également à sensibiliser les réutilisateurs en leur rappelant les obligations qui leur incombent en tant que responsables du traitement.

Concernant le contenu des licences, il est utile d'établir une distinction entre deux scénarios différents.

10.3. Conditions de licence pour les ensembles de données rendues anonymes

Tout d'abord, concernant les données rendues anonymes (autrement dit, les ensembles de données qui ne contiennent plus de données à caractère personnel), les conditions de la licence devraient:

- rappeler que les ensembles de données ont été anonymisés;
- interdire aux détenteurs d'une licence de ré-identifier toute personne physique[38];
- interdire aux détenteurs d'une licence d'utiliser les données pour prendre des mesures ou des décisions concernant les personnes concernées; et
- contenir également une obligation faite aux détenteurs d'une licence d'avertir le donneur de licence s'ils découvrent que des personnes peuvent ou ont été ré-identifiées.

Comme alternative aux conditions de licence, un message d'avertissement pourrait être porté à l'attention des réutilisateurs, d'une manière visible, sur le portail de données ouvertes. Toutefois, l'adoption de conditions de licence devrait être encouragée car celles-ci présentent l'avantage supplémentaire d'avoir une force exécutoire contractuelle.

Rappel des ensembles de données compromis

Tous les autres utilisateurs du web, y compris les personnes concernées elles-mêmes, doivent pouvoir avertir le donneur de licence qu'une ré-identification a eu ou peut avoir lieu. Lorsque le donneur de licence découvre un risque accru de ré-identification, la licence devrait prévoir une

[38] Des exceptions limitées peuvent s'appliquer, par exemple, dans les cas légitimes de test de ré-identification. Même dans ces cas, toutefois, les résultats des tests devraient être portés à l'attention du responsable du traitement et de l'organisme du secteur public concerné, et les données ré-identifiées ne devraient pas être publiées ni être diffusées à plus grande échelle.

procédure lui permettant de «rappeler» l'ensemble de données «compromis». En d'autres termes, la clause de protection de données devrait conférer au donneur de licence le droit de suspendre ou de mettre fin à l'accessibilité de données (par exemple, le droit de couper l'API ou d'éliminer le fichier de la plateforme). Le donneur de licence devrait déployer tous les efforts possibles, dans les limites du raisonnable, pour demander à tous les réutilisateurs d'effacer tout ou partie des ensembles de données qui ont été compromis (données qui sont devenues ré-identifiables). Cette procédure de rappel devrait notamment consister à placer des avis en évidence sur les sites web, comme les portails de données ouvertes et les forums/listes d'adresses électroniques/médias sociaux utilisés par les groupes ou personnes qui sont susceptibles de réutiliser les données. L'enregistrement obligatoire est peut-être le moyen le plus efficace de rappeler les ensembles de données, mais il ne devrait pas être encouragé s'il implique la collecte d'autres données à caractère personnel des réutilisateurs, ou s'il a pour effet général de décourager l'utilisation des sites web d'ISP et autres services.

10.4. Conditions de licence pour les données à caractère personnel

Lorsque des données à caractère personnel font l'objet d'une licence, il faut définir les limites de l'utilisation de ces données. Ici, la principale préoccupation consiste à garantir que toute réutilisation sera limitée à ce qui est «compatible avec les finalités pour lesquelles les données ont été initialement collectées»[39]. À cet effet, les conditions de licence doivent au moins établir clairement les finalités pour lesquelles les données ont été initialement publiées et indiquer ce qui serait considéré, ou non, comme une utilisation compatible des données à caractère personnel.

Il convient de signaler, toutefois, que cela ne devrait pas «limiter indûment les possibilités de réutilisation» (article 8, paragraphe 1, de la modification ISP). Par conséquent, les conditions génériques des licences ouvertes types seront souvent inappropriées et il faudra élaborer des licences spécifiques pour certaines données à caractère personnel, ou utiliser des modèles qui pourront être adaptés.

À l'heure actuelle, certaines licences ouvertes types (comme la licence publique ouverte en vigueur au Royaume-Uni) excluent les données à caractère personnel, qui ne font l'objet d'aucune licence.

10.5. Une sanction rigoureuse devrait suivre en cas de ré-identification ou d'utilisation inadéquate

Lorsque les données ont été publiées dans le cadre d'une licence - comme une licence publique ouverte -, il peut être difficile d'éviter qu'elles soient réutilisées à des fins inadéquates, qu'elles soient divulguées ou d'assurer leur sécurité. Il est très important dans ce contexte de surveiller la réutilisation et de sanctionner toute infraction, que ce soit sous forme de ré-identification des personnes concernées ou d'utilisation ultérieure à des fins inadéquates par le donneur de licence.

Si le groupe de travail «article 29» rappelle le rôle important que devraient jouer les organismes du secteur public, il souligne également que lorsqu'un réutilisateur collecte des données à caractère personnel par un processus de ré-identification, il est très probable qu'il sera considéré comme responsable d'un traitement illicite de données à caractère personnel et il pourra faire l'objet de mesures répressives prises par les autorités chargées de la protection des données. Parmi ces mesures pourraient notamment figurer de lourdes amendes, en vertu de la proposition de règlement sur la protection des données.

[39] Voir une fois encore l'avis 3/2013 sur la limitation de la finalité.

XI. Conclusions

En conclusion, le groupe de travail «article 29» réitère que la réutilisation des ISP peut présenter des avantages qui conduisent à une plus grande transparence et à un réemploi innovant des informations du secteur public. Toutefois, la plus grande accessibilité aux informations qui en résulte n'est pas sans risques. Il faut suivre une approche équilibrée afin de garantir la protection de la vie privée et des données à caractère personnel des personnes physiques. La législation sur la protection des données doit contribuer à orienter le processus de sélection des données à caractère personnel qui peuvent ou non être rendues disponibles à des fins de réutilisation, ainsi que les mesures à prendre pour protéger les données à caractère personnel.

Indépendamment du «principe de réutilisation» formulé dans la modification ISP, la réutilisation à des fins commerciales ou non commerciales conformément à la directive ISP n'est pas toujours appropriée lorsque les ISP destinées à être réutilisées contiennent des données à caractère personnel. Plutôt que des données à caractère personnel, ce sont souvent des statistiques issues de données à caractère personnel qui sont et devraient être rendues disponibles à des fins de réutilisation.

Cependant, il se peut, dans certains cas, que les données à caractère personnel soient considérées comme disponibles à des fins de réutilisation conformément à la directive ISP, le cas échéant, sous réserve de mesures juridiques, techniques ou organisationnelles supplémentaires visant à protéger les personnes concernées. Dans ces cas, le groupe de travail «article 29» réitère l'importance d'établir une base juridique solide pour rendre les données à caractère personnel accessibles au public, qui tienne compte des règles pertinentes en matière de protection de données, y compris des principes de proportionnalité, de minimisation des données et de limitation de la finalité. Dans ce contexte, il convient également de signaler une fois de plus que toutes les informations concernant une personne physique identifiée ou identifiable, qu'elles soient accessibles au public ou non, constituent des données à caractère personnel. En conséquence, l'accès à et la réutilisation des données à caractère personnel qui ont été rendues publiques restent soumis à la législation applicable en matière de protection des données.

À la lumière de ces considérations, le groupe de travail «article 29» émet les recommandations suivantes:

- le fait que certaines ISP puissent contenir des données à caractère personnel doit être pris en considération au plus tôt lorsque la publication d'ISP est envisagée, selon les principes de «protection des données dès la conception et par défaut»;

- dans cette optique, l'organisme du secteur public concerné (ou le législateur, selon le cas) devrait procéder à une évaluation d'impact sur la protection des données avant de rendre disponibles à des fins de réutilisation des ISP contenant des données à caractère personnel (ou avant d'adopter une législation permettant la publication de données à caractère personnel et les rendant ainsi potentiellement disponibles à des fins de réutilisation); une évaluation d'impact sur la protection des données devrait également être réalisée dans le cas de la mise à disposition à des fins de réutilisation d'ensembles de données rendues anonymes issus de données à caractère personnel;

- lorsque des ensembles de données sont rendus anonymes, il est essentiel d'évaluer le risque de ré-identification, et une bonne pratique consiste à réaliser un test de ré-identification;

- les résultats de l'évaluation pourraient permettre de définir des garanties appropriées pour réduire les risques au minimum, y compris, entre autres, des mesures techniques, juridiques

et organisationnelles - comme des conditions de licence appropriées et des mesures techniques pour éviter le téléchargement massif de données, et des techniques d'anonymisation adéquates; les résultats de l'évaluation peuvent également conduire à une décision de s'abstenir de publier les données et/ou de les rendre disponibles à des fins de réutilisation;

- les conditions de la licence concernant la réutilisation d'ISP devraient inclure une clause de protection des données, chaque fois que des données à caractère personnel sont traitées, y compris dans les cas où des ensembles de données rendus anonymes issus de données à caractère personnel sont rendus disponibles à des fins de réutilisation;

- lorsque l'évaluation d'impact sur la protection des données conclut qu'une licence ouverte ne suffit pas pour éliminer correctement les risques en matière de protection des données, les organismes du secteur public ne devraient pas mettre à disposition les données à caractère personnel en vertu de la directive ISP. (Toutefois, l'organisme du secteur public peut encore user de son pouvoir d'appréciation pour envisager la réutilisation en dehors des conditions et du champ d'application de la directive ISP et peut également exiger des demandeurs qu'ils prouvent que les risques pour la protection des données à caractère personnel sont correctement pris en compte et qu'ils traiteront les données conformément à la législation applicable en matière de protection des données);

- le cas échéant, les organismes du secteur public devraient garantir que les données à caractère personnel sont rendues anonymes et que les conditions de licence interdisent spécifiquement la ré-identification des personnes et la réutilisation des données à caractère personnel pour des finalités qui peuvent porter atteinte aux personnes concernées;

- enfin, les États membres devraient également envisager d'établir des réseaux de connaissances/centres d'excellence et de leur fournir une assistance, ce qui permettrait le partage de bonnes pratiques en matière d'anonymisation et de données ouvertes.

Fait à Bruxelles, le 5 juin 2013

Pour le groupe de travail
Le président
Jacob KOHNSTAMM