DE NOUVELLES DISPOSITIONS POUR PROTÉGER LES DONNÉES PERSONNELLES

Florence Raynal, avec la collaboration de Fabienne Amiard et Delphine Carnel

A.D.B.S. | « Documentaliste-Sciences de l'Information »

2014/3 Vol. 51 | pages 23 à 25

ISSN 0012-4508

Article disponible en ligne à l'adresse :

https://www.cairn.info/revue-documentaliste-sciences-de-l-information-2014-3-page-23.htm

De nouvelles dispositions pour protéger les données personnelles

[Données] L'Europe est sur le point d'adopter plusieurs textes européens sur la protection des données personnelles. Quelles implications auraient-ils pour les citoyens et pour les entreprises ? Doit-on s'attendre à de nouvelles obligations en matière de droit à l'oubli ?

En 2012, la Commission européenne a proposé une réforme des règles adoptées par l'Union européenne (UE) en 1995 en matière de protection des données personnelles. Cette proposition comprend un règlement définissant un cadre général de l'UE pour la protection des données et une directive relative à la protection des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ainsi que d'activités judiciaires connexes.

Une adaptation à de nouveaux défis

Ces textes répondent à quatre enjeux.

• **Un enjeu technologique.** Le cadre normatif existant doit être adapté à un nouveau contexte. Les nouvelles technologies et leurs applications, entrées dans le quotidien des citoyens et développées par des opérateurs mondiaux, ne connaissent plus de frontières physiques. Le futur cadre réglementaire doit assurer une protection efficace du citoyen, tout en étant flexible pour répondre aux évolutions futures.

• **Un enjeu politique.** Les révélations sur les programmes de surveillance massive de la NSA ont provoqué une onde de choc. Il en résulte une tension politique de l'UE avec les États-Unis sur l'utilisation des données des citoyens européens recueillies par les géants américains de l'Internet au moment où s'engagent les négociations pour un traité de libre-échange transatlantique et une prise de conscience de l'importance de la protection des données par les citoyens et consommateurs.

• **Un enjeu économique.** L'économie numérique revêt une importance croissante pour les acteurs économiques et les États. Les données personnelles sont décrites comme son « carburant » et un intense lobbying des entreprises fait valoir que le législateur ne doit pas entraver le potentiel de l'économie numérique, voire la reprise économique. Les entreprises mesurent aussi l'importance stratégique, en terme de compétitivité, d'une approche responsable des données personnelles.

• **Un enjeu international.** La proposition de règlement européen se situe dans un contexte international mouvant, avec plusieurs réformes concomitantes dans différentes régions du monde. Le Conseil de l'Europe procède à la révision de la Convention n° 108 sur la protection des données, l'OCDE vient d'actualiser ses lignes directrices en la matière et l'APEC (Coopération économique pour l'Asie-Pacifique) développe son propre cadre en matière de transferts internationaux de données. Cette réforme est emblématique pour l'Europe qui doit montrer qu'elle est capable de s'adapter aux nouvelles réalités du numérique tout en préservant un haut niveau de protection pour l'individu et d'innover en construisant un modèle de gouvernance équilibré, crédible et légitime à la fois pour le citoyen, les entreprises et les interlocuteurs mondiaux.

Un impact pour les entreprises

Le projet de règlement européen devrait se traduire par :

- une simplification des formalités préalables : disparition du système de déclaration normale ou simplifiée ainsi que des autorisations préalables pour chaque transfert de données ;
- la création de nouveaux droits pour le citoyen, ce qui suppose une implication des entreprises pour une concrétisation effective et efficace de ces droits (droit à l'oubli, droit à la portabilité[1], profilage régulé) ;
- l'introduction de nouvelles mesures d'*accountabillity*[2] impliquant des moyens pour mettre en œuvre des principes et une obligation de démonstration de leur respect (par exemple, analyse de l'impact des traitements à risque, désignation d'un correspondant Informatique et libertés, conduite d'audits, intégration de la protection de la vie privée dès la conception du traitement, tenue d'une documentation, élaboration de codes de bonne conduite, etc.).

Ces dispositions impliqueront un partenariat avec les autorités de contrôle telles que la Cnil pour le développement de solutions adaptées à la réalité des entreprises et garantissant un niveau élevé de protection des citoyens. ////

1. Portabilité : possibilité pour la personne concernée d'obtenir une copie de ses données dans un format structuré couramment utilisé et permettant leur réutilisation.

2. *Accountability* : principe qui recouvre à la fois la mise en place de moyens pour mettre en œuvre les principes et une obligation de les respecter.

3. Les sanctions Google, par exemple : en France 150 000 €, en Espagne 900 000 €.

//// Un renforcement du pouvoir de sanction de la Cnil et de ses homologues

Une harmonisation des pouvoirs de sanction des autorités de protection est nécessaire en raison de l'existence d'importantes disparités[3] et de la nouvelle responsabilisation des responsables de traitements/sous-traitants en matière d'*accountability* et de simplification des formalités préalables. Les sanctions pécuniaires, plus importantes, pourront atteindre 2 % du chiffre d'affaires annuel mondial de l'entreprise[4]. Il faut disposer pour ceci d'un outil qui permette aux citoyens d'évaluer l'importance de la violation commise et la valeur financière de leurs données. Cet outil doit être un outil de dissuasion et non de régulation quotidienne de la protection des données.

4. Pour la Commission LIBE du Parlement européen, elles pourraient se monter jusqu'à 100 millions d'euros et 5 % du chiffre d'affaires mondial.

Des aspects à régler

Le danger d'un régime particulier pour les données pseudonymes

Des pseudonymes numériques permettent à des entreprises de singulariser des individus, sans connaître leur identité civile, en recourant à d'autres identifiants (login, code lié au téléphone, à l'ordinateur ou à une carte à puce, empreinte digitale, etc.). En rassemblant ainsi des informations sur les habitudes de consommation, les déplacements, l'emploi, le niveau de vie, etc. des personnes, les traitements visent à distinguer les individus pour leur communiquer une information personnalisée, leur offrir un prix différencié, leur ouvrir (ou non) l'accès à certains services, etc. Il y a donc une possibilité de discrimination.

Cette sous-catégorie de données personnelles, au motif que leur traitement présenterait moins de risques, serait soumise à un régime de protection allégée. Or, pour le G29[5], la pseudonymisation, utile pour renforcer la protection des données, ne change pas la nature des données - qui restent personnelles - une réidentification par le responsable de traitement ou une tierce partie restant possible.

5. La Cnil fait partie du groupe de travail Article 29 de la directive européenne sur la protection des données personnelles qui regroupe les autorités de contrôle de chaque pays de l'UE et deux représentants des institutions européennes chargées de ces questions. http://www.cnil.fr/linstitution/international/g29

6. Avis du 16/04/2014 concernant les principaux éléments du guichet unique et du mécanisme de cohérence pour les entreprises et les individus.

7. www.cnil.fr/institution/actualite/article/article/archives-et-protection-des-donnes-personnelles-partenariat-entre-la-cnil-et-le-siaf/

8. Autorisation unique AU-029 du 12 avril 2012, www.cnil.fr/documentation/deliberations/deliberation/delib/265

Le guichet unique

Si les entreprises implantées dans plusieurs États membres doivent disposer d'un interlocuteur unique pour les traitements de données mis en œuvre dans ces pays, cette nécessité ne doit pas remettre en cause la protection des droits des citoyens. Or, le modèle proposé aujourd'hui par la Commission européenne ne garantit pas un droit à un recours effectif.

Dans la proposition, la détermination de l'autorité compétente sera fondée sur le critère de l'établissement principal, et cette autorité aura une compétence exclusive pour prendre toute décision relative au traitement et à son responsable au nom des 27 autres États. En d'autres termes, si une entreprise installée en Europe effectue des traitements dans plusieurs États membres, l'autorité compétente sera celle du pays où l'entreprise a installé son établissement principal, même si l'un de ces établissements est installé sur un autre territoire, quel que soit le public ciblé.

Cette proposition, qui favorisera la délocalisation dans les États où les autorités de contrôle ont moins de moyens pour exercer leur mission, soulève des difficultés pratiques et juridiques, notamment pour le citoyen qui devra exercer son recours devant le juge de l'autorité compétente (qui ne sera pas forcément celle de sa résidence).

Pour le G29[6], les autorités de protection doivent être compétentes lorsque leurs citoyens sont affectés par un traitement mis en œuvre sur leur territoire ou lorsqu'une entreprise y est établie. Cette entreprise doit bénéficier d'un guichet unique lorsqu'elle dispose de plusieurs établissements en UE ou que les citoyens de plusieurs États membres sont affectés par le traitement mis en œuvre par cette entreprise. Ce guichet unique doit jouer le rôle d'un coordinateur, d'un pilote auprès des autres autorités concernées par le traitement et ne prendra des décisions qu'avec leur accord. Ces décisions, mises en œuvre par chaque autorité sur son territoire national, pourront alors faire l'objet de recours par l'individu sur son territoire de résidence devant les juridictions dont relève son autorité de protection. La solution du G29 propose un schéma juste et équilibré, trait d'union entre le besoin exprimé par les multinationales de bénéficier d'un interlocuteur unique au sein de l'UE et la nécessaire proximité réclamée par le citoyen lui permettant d'exercer ses droits sur son territoire auprès de son autorité naturelle.

Le droit à l'oubli dans le contexte des archives et du datamining

Il est ardu de définir un « juste » équilibre entre le droit à l'oubli, la nécessité de preuve et la liberté d'expression. Les difficultés à fixer des dates de péremption des données et à mettre en place des solutions concrètes d'effacement ou d'archivage des données rendent complexe la recherche de cet équilibre.

En ce sens, la Cnil travaille avec les Archives de France[7] pour articuler les notions de durée de conservation des données de la Loi « Informatique et Libertés » (LIL) et de délais « d'utilité » du Code du patrimoine. Le cycle de vie d'une donnée se compose, en effet, de plusieurs délais de conservation à définir pour chaque type d'utilité de la donnée : un délai d'utilité courante lié aux besoins des missions du service « principal » (dit « service métier ») ; un délai d'utilité administrative lié au respect d'obligations légales, notamment en matière de preuve ; la conservation à titre historique (archivage définitif de certaines données).

S'agissant de la diffusion sur Internet des archives du secteur public telles que le recensement de la population, la Cnil[8] interdit,

pendant un certain temps, de les indexer sur des données personnelles, à partir d'un moteur de recherche externe : jusqu'à 150 ans pour indexer les données « sensibles » de l'article 8 de la LIL (santé, opinion philosophiques, politiques, etc.) ; jusqu'à 120 ans à compter de la date du document archivé pour indexer des données nominatives rendues accessibles au grand public ; exclusion des données de l'article 9 (infraction, condamnation, sûreté).

L'objectif est de garantir la proportionnalité de chaque traitement de données personnelles, y compris la pertinence des données pour construire un outil d'archivage ou de référencement. D'ailleurs, une indexation efficace ne dépend pas que des données personnelles : d'autres mots-clés sont certainement plus opérationnels pour organiser l'accès à un contenu dématérialisé. Toutes les données archivées n'intéressent pas tous les publics. L'enjeu est de construire pour chaque contenu une visibilité « modulée et modulable » au regard des intérêts en présence.

L'arrêt Google Spain du 13 mai 2014 de la Cour de justice de l'Union européenne a conféré au droit à l'oubli une nouvelle dimension. Dans la perspective d'une mise en œuvre uniforme de cet arrêt en Europe, le G29 analyse les bases légales permettant à des personnes d'invoquer un droit au déréférencement auprès des moteurs de recherche ainsi que les modalités précises d'exercice de ce droit à l'effacement et de refus par le moteur de recherche. ■

> **Florence Raynal**
Chef du service des affaires européennes et internationales Cnil
fraynal@cnil.fr

> **avec la collaboration de Fabienne Amiard**
juriste expert à la Cnil
famiard@cnil.fr

> **et Delphine Carnel**
juriste expert à la Cnil
dcarnel@cnil.fr

Un dégel proche pour les œuvres orphelines ?

[lobbying] Une loi transposera prochainement en France une directive européenne qui doit favoriser l'utilisation d'œuvres dont les auteurs ou autres titulaires de droit ne peuvent pas être retrouvés. Quel sera le point d'équilibre entre bibliothèques et ayants droit ?

Donner une nouvelle vie aux livres, articles, photographies, films, rapports, etc. de son fonds documentaire en les numérisant, ne serait-ce que partiellement, quoi de plus légitime ? Or, bien que propriétaire du support, il faut disposer des droits nécessaires pour effectuer cette numérisation et permettre l'accès aux documents numérisés et, à défaut, retrouver les titulaires de droit (éditeurs, producteurs, auteurs ou héritiers, etc.) pour les négocier. Mais si les recherches faites pour identifier et localiser les ayants droit s'avèrent infructueuses, que faire ? Prendre le risque de communiquer ces œuvres au public ou attendre patiemment que les droits patrimoniaux soient échus ?

Une directive européenne frileuse

Toutes ces œuvres dites orphelines ont une valeur culturelle qu'il serait contreproductif de geler. Avec la bibliothèque numérique européenne Europeana en arrière-pensée, la Commission européenne a proposé en mai 2011 un texte qui doit faciliter la ////