

La protection des données personnelles de la théorie juridique à la pratique informatique

Pauline Martin¹, Valentin Montmirail²

¹CDEP, Université d'Artois, Douai, France

²CRIL, Université d'Artois, Lens, France

Douai - 06 Mars 2017

Protection des données personnelles

- ▶ Règlementation spéciale en France;
- ▶ Règlementation au niveau de l'Union Européenne.

La loi informatique et libertés

- ▶ Adoptée en 1978 [Com78];
- ▶ Modifiée par la loi du 6 août 2004.

La législation correspondante

- ▶ Modifiée à l'échelle européenne le 27 avril 2016;
- ▶ Modifiée au niveau national le 7 octobre 2016.

Garantie par des textes plus généraux

- ▶ Article 12 DUDH [Nat48];
- ▶ Article 8 Conv. EDH [Con10];
- ▶ Loi n° 70-643 du 17 juillet 1970 [Lé70];
- ▶ 1995 : reconnaissance du droit à la vie privée.

Consacré par le Conseil constitutionnel

- ▶ Autorités de protection des données : CNIL;
- ▶ Création du groupe de l'article 29;
- ▶ CJUE + Conseil d'Etat + Conseil Constitutionnel.

Théorie Juridique

Tout est mis en oeuvre pour protéger les individus.

Pratique Informatique

- ▶ La mise en place de ces règles est-elle possible ?
- ▶ Le niveau de protection est-il optimal ?

Loi informatique et liberté du 6 janvier 1978 modifiée

“ **Toute information** relative à une **personne physique identifiée** ou qui peut être **identifiée directement ou indirectement**, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ” [Com78]

Echelle européenne : Plusieurs étapes

- ▶ Directive 95/46/CE du 24 octobre 1995 [Com95]
- ▶ CJUE : 19 octobre 2016
- ▶ RGPD [Par16]
 - ▶ Article 4 Paragraphe 1
 - ▶ Considérant 26

La loi française ne reprend pas les éléments permettant de caractériser l'identité mais renvoie aux moyens en vue de permettre son identification.

Information : Notion très vague

- ▶ Peu importe la forme : photo, adresse, âge, géolocalisation
- ▶ Peu importe le message qu'elle véhicule
- ▶ Peu importe qu'elle soit subjective ou objective
- ▶ Peu importe la technologie utilisée

Se rapportant à une personne physique

- ▶ Exclut les personnes morales
- ▶ Exclut les personnes décédées
- ▶ **Tout être humain**

De manière directe...

Propres à l'identité physique, physiologique, psychique, économique, culturelle ou sociale. Directive 95/46/CE [Com95].

...ou indirecte

- ▶ n° de Sécurité Sociale;
- ▶ Régime matrimonial;
- ▶ Coordonnées bancaires;
- ▶ Informations fiscales;
- ▶ Emplacement géographique;
- ▶

Paradoxe des données personnelles

- ▶ Données personnelles pour identifier : protégées.
- ▶ En pratique : pas besoin d'identifier pour proposer des services.

Nouvelle logique d'identification

Ne passe plus nécessairement par l'identité d'une personne.

Cas concret : Un site personnel

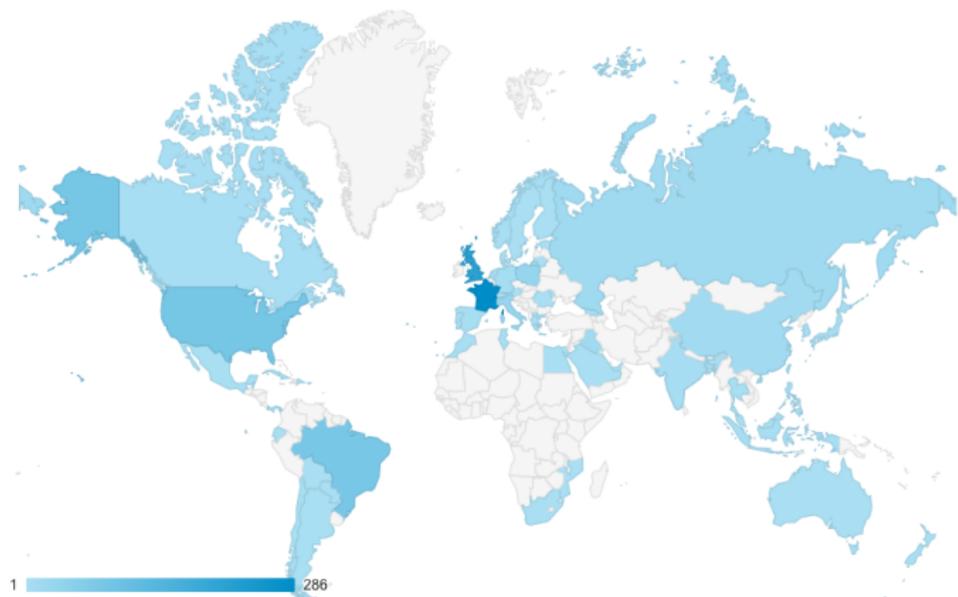


Figure : Google Analytics <http://valentin-montmirail.com>

Cas concret : Un site personnel

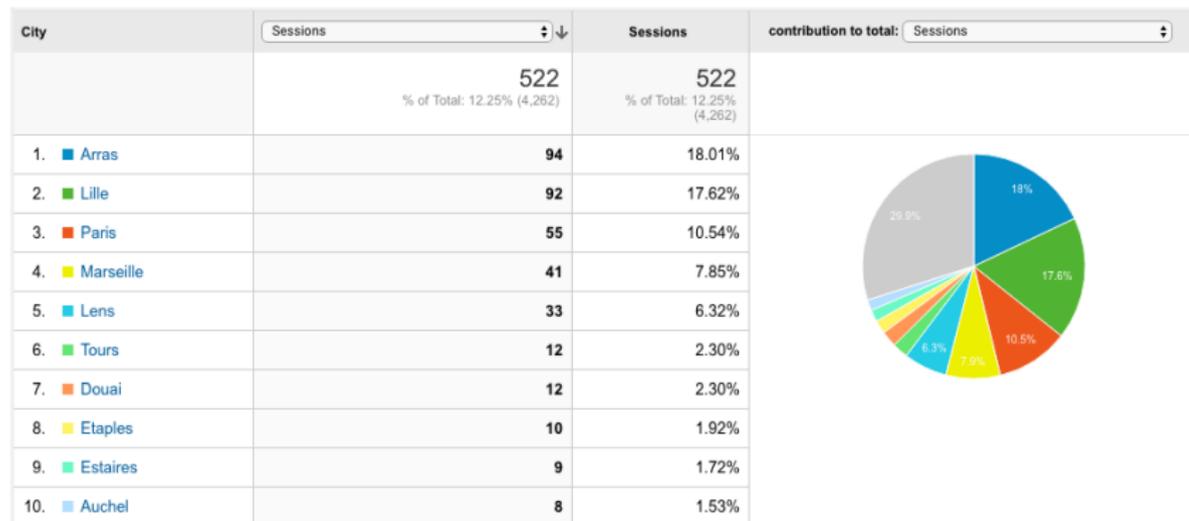


Figure : Google Analytics <http://valentin-montmirail.com>

Cas concret : Un site personnel

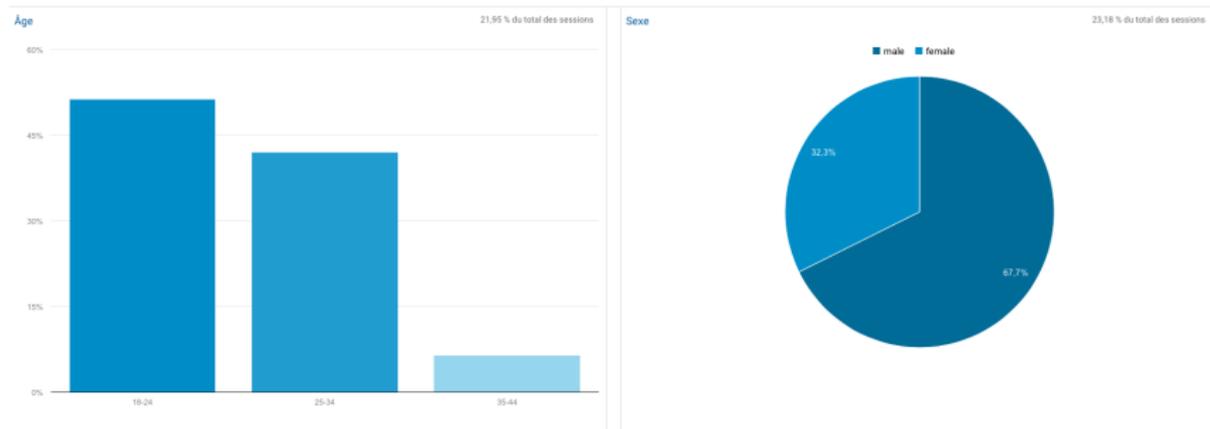


Figure : Google Analytics <http://valentin-montmirail.com>

Cas concret : Un site personnel

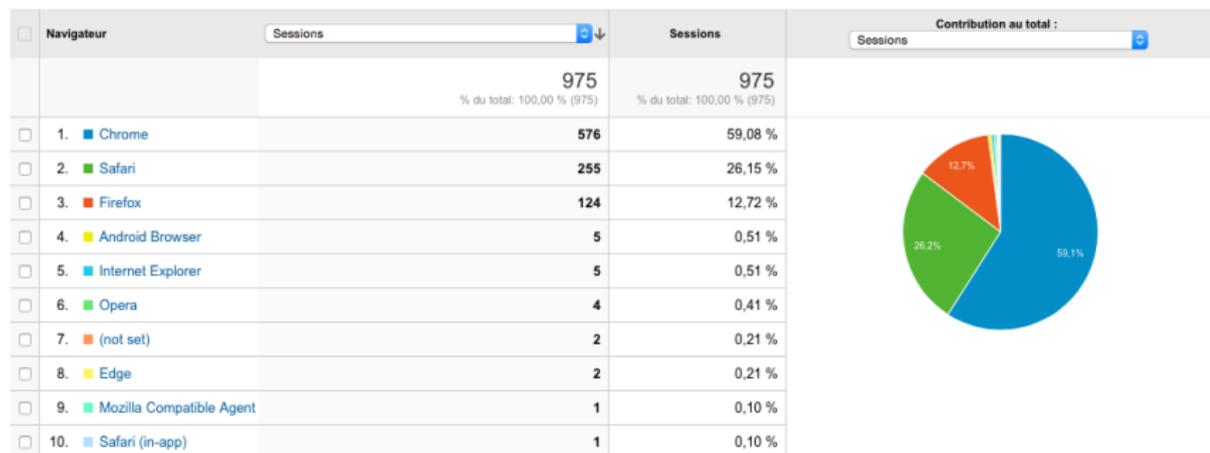


Figure : Google Analytics <http://valentin-montmirail.com>

En pratique

- ▶ Les données peuvent être revendues au plus offrant.

En théorie

- ▶ Ces données méritent une forme de protection...
- ▶ ...même si les éléments d'identification sont absents.

Définition : Données à caractère personnel

- ▶ Toute information qui permet l'identification de manière directe ou indirecte;
- ▶ Pas seulement d'une information permettant l'identification d'une personne;
- ▶ Pas nécessaire d'être identifié pour être confronté aux problématiques relatives aux données personnelles;

Il serait opportun de prendre en considération ce changement de paradigme et ne plus se contenter de cette conception des données à caractère personnel...

Données anonymisées

- ▶ Pas de définition dans le règlement;
- ▶ Opposées aux données à caractère personnel dans le considérant 26.

La donnée anonyme est celle qui ne peut pas être rattachée à une personne **identifiée ou identifiable**.

Données anonymisées

La protection relative aux DP n'est pas applicable !

Données pseudonymisées

- ▶ Notion nouvelle intégrée dans le RGPD [Par16];
- ▶ Définition à l'article 4, paragraphe 5 [Cor16].

Données pseudonymisées

Consiste à **dissimuler l'identité d'un individu** sans pour autant la faire disparaître.

- ▶ Conservation séparée des clés de réidentification;
- ▶ Mesures techniques tendant à empêcher la réidentification.

Données pseudonymisées

- ▶ Mesure de protection des données qui n'altère pas la nature de la donnée à caractère personnel.
- ▶ La donnée pseudonymisée est une donnée à caractère personnel indirectement identifiante.

La pseudonymisation est différente de l'anonymisation.

La RGPD [[Par16](#)] est applicable aux données pseudonymisées.

Données anonymisées

En pratique : les données sont hachées.

Données pseudonymisées

En pratique : les données sont chiffrées.

Traitement de données à caractère personnel

Article 2 alinéa 3 Loi n° 78-17 modifiée [Com17] : Toute opération ou tout ensemble d'opérations portant sur de telles données, **quel que soit le procédé utilisé**.

La loi fournit une **liste non exhaustive d'opérations** constitutives de traitement de données personnelles :

- ▶ collecte,
- ▶ enregistrement,
- ▶ organisation,
- ▶ conservation,
- ▶ adaptation,
- ▶ ...

En informatique: Traitement de données

- ▶ une série de processus,
- ▶ pour extraire de l'information,
- ▶ produire des connaissances à partir de données brutes,
- ▶ le tout, de manière automatisé.

Qui est le responsable du traitement ?

Plusieurs personnes à prendre en considération.

- ▶ Sur qui pèsent les exigences prévues par la réglementation;
- ▶ Qui encourt les sanctions en cas de violation de ces dispositions.

Définition Européenne

Personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens de traitement de données à caractère personnel. [Com95]

Responsable ?

- ▶ Quelle est l'organisme qui se charge du traitement des données ?
- ▶ Qui détermine la finalité et les moyens du traitement ?
- ▶ Pourquoi ce traitement a-t-il lieu ? Qui l'a entrepris ?

Le contexte est fondamental.

Critère principal : jouer un rôle dans la détermination des finalités.

Comment identifier le responsable du traitement ?

Vérifier si le responsable du traitement agit seul ou non

- ▶ Condition la plus difficile à vérifier;
- ▶ **les situations varient** l'une de l'autre;
- ▶ **grand nombre d'acteurs** à différents niveaux.

RGPD [Par16] : Les responsables conjoints du traitement **définissent par voie d'accord** leurs **obligations respectives**.

Coopération \neq Coresponsabilité.

Responsabilité solidaire : tout le monde responsable sur un même pied d'égalité.

Sous-traitant

- ▶ Toute personne traitant des DP pour le compte du responsable de traitement [Lé04];
- ▶ Article 2-e de la directive européenne;
- ▶ Personne physique, morale, service ou tout autre organisme;
- ▶ Doit être une **entité juridique** ≠ **du responsable de traitement**;
- ▶ **Exécuter les instructions** du responsable du traitement;
- ▶ **Définir le champ d'intervention du sous-traitant.**

RGPD [Par16] : Sous-traitant peut être **requalifié responsable de traitement**.

Responsable du traitement

Tout traitement des informations personnelles communiquées à Amazon.fr est effectué sous la responsabilité, premièrement, d'Amazon Europe Core SARL, d'Amazon EU SARL, Amazon Services Europe SARL et Amazon Media EU SARL, les quatre entités situées au 5 rue Plaetis, L -2338 Luxembourg, les responsables du traitement, et deuxièmement, d'Amazon.fr SAS, le sous-traitant, situé au 67 Boulevard du Général Leclerc - 92110 Clichy.

Le bouclier de protection des données UE-Etats-Unis

Amazon.com, Inc. participe au cadre du bouclier de protection des données UE-Etats-Unis. Cliquez [ici](#) pour en savoir plus.

Destinataire du traitement

- ▶ Qui est le destinataire du traitement ?
- ▶ Personne habilitée à recevoir communication de ces données [Com78];

Determiner une liste de destinataire

- ▶ Au moment de l'élaboration du traitement;
- ▶ Dans la période précédant le début du lancement opérationnel du traitement.

But : Pour définir le périmètre du traitement des DP.

Principe de transparence

- ▶ Les données sont collectées et traitées de manière licite et loyale [Com78];
- ▶ Charte européenne des droits fondamentaux, art. 8;
- ▶ Conseil Constitutionnel : droit au respect à la vie privée;
- ▶ Article 5 RGPD : traitement de manière licite, loyale et transparente.

Respect de l'obligation d'information

Obligation d'information : c'est l'essentiel de l'obligation de loyauté et de licéité.

En pratique pour respecter ces obligations ?

Exemple : <https://www.amazon.fr/>

- ▶ Adresse IP et cookies : données personnelles ?

Exemple : <https://www.amazon.fr/>

- ▶ Adresse IP et cookies : données personnelles ?



Confidentialité- France

Notre réseau a détecté que vous êtes localisé en France.

... accorde de l'importance à la vie privée de nos utilisateurs.

Les lois françaises exigent que nous obtenions votre permission avant d'envoyer des cookies à votre navigateur Web.

Notre site dépend de ces cookies pour fonctionner correctement.

S'il vous plaît cliquez sur le bouton: «Accepter les cookies» pour continuer à naviguer sur notre site.

Accepter les Cookies

La réglementation ne semble pas imposer de forme particulière à l'obligation d'information.

Article 12, 1° du RGPD [Par16]

- ▶ Large : laisse un maximum de possibilités au responsable du traitement.
- ▶ L'essentiel est que l'information soit donnée.

Article 12, 1° du RGPD [Par16]

- ▶ Le responsable du traitement prend des mesures appropriées.
- ▶ Fournir information d'une façon concise, transparente, compréhensible...

CNIL + G29 : traitement effectué à l'insu des personnes intéressées = déloyal

Jurisprudence

Si l'information du traitement est **postérieure au traitement des données** → déloyale et illicite.

En pratique pour respecter ces obligations ?



amazon.fr
Toutes nos boutiques ▾

Parcourir les boutiques -

Chez vous Ventes Flash Chèques-cadeaux Vendre Aide

Bonjour. Identifiez-vous
Votre compte ▾

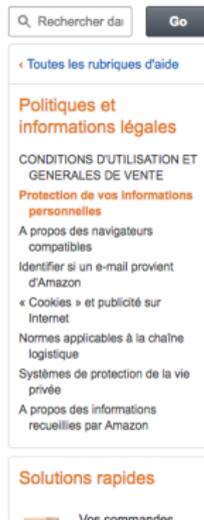
Testez
Premium ▾

Vos
Listes ▾

Panier

Les séries Amazon Original avec Amazon Premium
Essayez Amazon Premium

Aide et Service Client



Rechercher dans

Go

← Toutes les rubriques d'aide

Politiques et informations légales

CONDITIONS D'UTILISATION ET GENERALES DE VENDE

Protection de vos informations personnelles

A propos des navigateurs compatibles

Identifier si un e-mail provient d'Amazon

« Cookies » et publicité sur Internet

Normes applicables à la chaîne logistique

Systèmes de protection de la vie privée

A propos des informations recueillies par Amazon

Solutions rapides

Vos commandes

[Sécurité et confidentialité](#) > [Politiques et informations légales](#)

Protection de vos informations personnelles

Dernière mise à jour le 30 septembre 2016. Pour consulter la version précédente, cliquez [ici](#).

Nous savons que vous êtes attentifs à l'utilisation et au partage de vos informations personnelles et vous remercions de votre confiance pour les traiter scrupuleusement, avec précaution, et à bon escient.

En visitant le site Amazon.fr, vous acceptez qu'Amazon.fr collecte, traite et utilise les informations personnelles visées comme indiqué ci-après.

- Responsable du traitement
- Quelles sont les informations des clients collectées par Amazon.fr ?
- Qu'en est-il des « cookies » ?
- Amazon.fr partage-t-elle les informations qu'elle reçoit ?
- Mes informations personnelles sont-elles protégées ?
- Qu'en est-il des Annonceurs Tiers et des Liens vers d'autres Sites Internet ?
- A quelles informations puis-je avoir accès ?
- Quels choix me sont proposés ?
- Les enfants sont-ils autorisés à utiliser Amazon.fr ?
- Notices et révisions
- Exemples d'informations collectées
- Le bouclier de protection des données UE-Etats-Unis
- Sociétés du Groupe Amazon

Autres pages liées à la protection de votre compte.

- [Réinitialiser votre mot de passe](#)

Droit d'opposition

- ▶ Une personne peut s'opposer au traitement de ses données personnelles;
- ▶ Pour que la personne puisse exercer ce droit, elle doit être informée du traitement des données.

Ne doit pas faire obstacle à l'exercice du droit d'opposition

- ▶ CNIL;
- ▶ Le Conseil d'Etat a indiqué que
 - ▶ Au moment de **l'enregistrement des données**
 - ▶ Au plus tard lors de **la première communication de ces données à des tiers**

Objectif de transparence

- ▶ Veiller aux conditions de recueil du consentement préalable;
- ▶ Ne doit pas être confondu avec le droit d'opposition;
 - ▶ Consentement
 - ▶ Droit d'opposition
- ▶ Le consentement doit être **libre** et **éclairé**;
- ▶ Commission Européenne;
- ▶ G29.

Article 10 de la directive 95/46/CE [Com95]

- ▶ **L'identité du responsable du traitement** et, le cas échéant, de son représentant;
- ▶ **Les finalités du traitement** auquel les données sont destinées;
- ▶ Les **destinataires ou les catégories de destinataires** des données;
- ▶ Le fait de **savoir si la réponse aux questions est obligatoire ou facultative**;
- ▶ L'existence d'un **droit d'accès aux données** la concernant;
- ▶ L'existence d'un **droit de rectification de ces données**.

Article 32 de la loi informatique et libertés [Com78]

- ▶ La personne concernée par les DP est informée;
- ▶ De l'identité du responsable du traitement;
- ▶ **Les finalités du traitement;**
- ▶ **Du caractère obligatoire ou facultatif des réponses;**
- ▶ Des conséquences éventuelles, à son égard, d'un défaut de réponse;
- ▶ Des **destinataires ou catégories de destinataires des données;**
- ▶ Directives relatives au sort de ses DP après sa mort;
- ▶ **Durée de conservation des catégories de données traitées.**

Finalité du traitement

- ▶ Le responsable du traitement doit préalablement déterminer **les finalités**;
- ▶ Article 5, 1, b) du RGPD [[Par16](#)];
- ▶ Les données sont collectées pour des finalités **déterminées, explicites et légitimes**;
- ▶ G29 a donné une méthodologie pour déterminer la finalité;

La détermination de la finalité

- ▶ Principe de transparence;
- ▶ Garantir une prévisibilité;
- ▶ Mieux contrôler l'utilisation des DP.

Finalité du traitement

- ▶ Une évaluation précise en amont;
- ▶ Ne doit pas être décrite dans des termes trop large;
- ▶ Distinguer les différentes finalités;
- ▶ La finalité doit être légitime;
- ▶ L'information donnée doit être claire et précise;
- ▶ G29 : Elle doit être exprimée dans des termes intelligibles pour tous;
- ▶ Doit être préalable au traitement;
- ▶ Support écrit préférable

Amazon.fr partage-t-elle les informations qu'elle reçoit ?

Les informations relatives à nos clients représentent une part importante de notre activité et notre métier n'est pas d'en faire le commerce. Nous partageons ces informations uniquement dans les cas suivants et pour les finalités décrites dans cette politique de confidentialité, avec Amazon.com, Inc. et les filiales qu'Amazon.com, Inc. contrôle et qui sont, soit soumises à cette politique de confidentialité, soit appliquent des règles au moins aussi protectrices que celles décrites dans cette politique de confidentialité.

- **Partenaires affiliés que nous ne contrôlons pas**

Nous travaillons en étroite collaboration avec nos partenaires. Dans certains cas, tels que pour nos vendeurs « Marketplace », ces partenaires peuvent exploiter leurs propres boutiques ou vous vendre directement leurs biens ou services via le site Amazon.fr. Dans d'autres cas, nous exploitons des boutiques, fournissons des services ou commercialisons des lignes de produits, conjointement ou pour le compte de ces partenaires. Pour consulter quelques exemples d'offres co-brandées ou d'offres conjointes, veuillez cliquer [ici](#). Vous pouvez savoir quand un tiers est impliqué dans vos transactions et quand nous partageons avec ce tiers les informations relatives à ces transactions.

- **Prestataires de services tiers**

Nous avons recours à d'autres sociétés ou personnes indépendantes lesquelles fournissent certains services pour notre compte. En voici quelques exemples : le traitement des commandes, la livraison des produits, l'envoi du courrier postal ou électronique, la suppression d'information redondante de nos listes clients, la gestion de nos fichiers clients, l'analyse de nos bases de données, la fourniture d'une assistance marketing, la fourniture de résultats de recherche et de liens (y compris des liens et listings payants), le traitement des paiements par carte bancaire et la fourniture du service clients. Ces prestataires ont accès aux informations personnelles nécessaires à l'exécution de leurs prestations mais ne sont pas autorisés à les utiliser à d'autres fins. De plus, ils sont tenus de traiter ces informations personnelles en conformité avec la présente politique de confidentialité et en application des lois applicables à la protection des données personnelles.

- **Offres promotionnelles**

Proportionnalité de la mise en oeuvre

- ▶ Article 6, 3° de la loi Informatique et Liberté [Com78]
- ▶ Article 5, 1-c) du RGPD [Par16]

Innovation de la loi du 6 août 2004 [Lé04] qui reprend l'exigence de la directive du 24 octobre 1995 [Com95].

Sanctions

Pas de sanctions pénales.

Anulation par le juge administratif ou sanction administrative.

Proportionnalité au regard de la finalité

- ▶ Implique un examen au cas par cas;
- ▶ Contrôle de la CNIL;
- ▶ Contrôle du CE;
- ▶ Contrôle du juge judiciaire;
- ▶ Contrôle de la CJCE.

Contrôle attentif par toutes les juridictions de l'application de principe de proportionnalité.

Caractère indispensable des données traitées

Sanctions systématiques les cas dans lesquels le responsable de traitement ne prouve pas de façon certaine que les moyens auxquels il a recours pour le mettre en œuvre sont **absolument indispensables** et **ne se limitent pas seulement à être utile ou à simplifier la gestion du traitement.**

CE : Traitement OSCAR

Les DP telles que la photo et les empreintes digitales des enfants âgés de + de 12 ans au titre desquelles le bénéficiaire a reçu une aide étaient pertinentes et adéquates, au regard de l'objet du traitement OSCAR;

CE : Solution inverse

Est **excessive** la collecte par le ministère de l'éducation nationale d'informations relatives au sexe et à la nationalité des conjoints de ses agents → aucune utilité.

RGPD [Par16]

Les DP sont adéquates, pertinentes et surtout **limitées au minimum nécessaire au regard des finalités pour lesquelles elles sont traitées.**

Nécessité de mise à jour

Article 6, 4° loi du 6 août 2004 [Lé04].

- ▶ Seules peuvent être collectées des données exactes et complètes;
- ▶ Obligation de mettre à jour ces données.

Responsable du traitement doit prendre **les mesures appropriées** pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient **effacées ou rectifiées**.

Caractère exact et complet des DP traitées

- ▶ CNIL : Obligation de résultat;
- ▶ ≠ Cour de cassation : Obligation de moyens;
- ▶ RGPD : Obligation de moyens;

Sanctions

Si le responsable de traitement ne procède pas à la rectification, à la mise jour, au verrouillage ou à l'effacement des DP :

→ 1 500€ d'amendes + sanctions administratives (\leq 30 000€).

Quels choix me sont proposés ?

Comme mentionné ci-dessus, vous avez toujours la possibilité de ne communiquer aucune information, même si certaines informations sont nécessaires pour effectuer des achats ou pour utiliser des fonctionnalités d'Amazon comme «[Votre profil](#)», [Vos listes d'envies](#), vos [commentaires clients](#) et [Amazon Premium](#).

Conformément aux dispositions en vigueur vous disposez d'un droit d'accès, de modification, de rectification et de suppression des informations vous concernant. Vous pouvez exercer ces droits sur les pages citées dans la section "À quelles informations puis-je avoir accès" Si vous mettez une information à jour, nous conservons généralement une copie de vos informations initiales dans nos dossiers.

Quels choix me sont proposés ?

Comme mentionné ci-dessus, vous avez toujours la possibilité de ne communiquer aucune information, même si certaines informations sont nécessaires pour effectuer des achats ou pour utiliser des fonctionnalités d'Amazon comme «[Votre profil](#)», [Vos listes d'envies](#), vos [commentaires clients](#) et [Amazon Premium](#).

Conformément aux dispositions en vigueur vous disposez d'un droit d'accès, de modification, de rectification et de suppression des informations vous concernant. Vous pouvez exercer ces droits sur les pages citées dans la section "À quelles informations puis-je avoir accès" Si vous mettez une information à jour, nous conservons généralement une copie de vos informations initiales dans nos dossiers.

En pratique

À jour tant que l'utilisateur ne modifie pas.

Obligation de limiter dans le temps

- ▶ Article 28 loi informatique et liberté de 1978 [Com78];
- ▶ Article 5 Convention n° 108 du Conseil de l'Europe;
- ▶ Article 5, 1°, e) RGPD [Par16].

Les données sont conservées sous une forme permettant l'identification des personnes concernées **pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.**

Droit à l'oubli

- ▶ Effacées;
- ▶ Anonymisées sans ré-identification possible;
- ▶ Archivées sous certaines conditions.

Principales garanties de ce qui a été identifié par la doctrine puis par la CNIL de ce qu'on appelle "**le droit à l'oubli**".

Philippe Aigrain, président de la **Quadrature du Net** :

“L'affirmation du droit à l'oubli est vaine. C'est un droit qui restera fictif”.

“Quand on connaît le fonctionnement des bases de données, on sait qu'il est impossible de supprimer une donnée”.

Pierre Lepage

Un tel droit n'existe pas en tant que tel dans la loi du 6 janvier 1978 [Com78]. Cela le distingue des autres droits tels que le droit d'opposition et de suppression qui en constituent les autres modalités avec le droit de retirer son consentement.

Droit à l'effacement

Droit de retirer son consentement a été inclus dans le droit à l'effacement à l'article 17 du RGPD [Par16].

Concrètement, il s'agit d'un **droit à l'effacement** en cas d'absence de suppression automatique.

Droit à l'effacement

- ▶ Personnes concernées peuvent demander à ce que leurs données soient effacées;
- ▶ Article 19 RGPD [Par16] : Maintient l'exigence d'informer chaque destinataire;
- ▶ Risque que les conséquences soient lourdes en pratique;
- ▶ **Portée limitée** car cet article n'a vocation à s'appliquer que s'il ne se révèle pas **impossible ou s'il n'exige pas des efforts disproportionnés**.

Durée limitée et difficultés la durée adéquate de conservation

- ▶ Article 6, 5° Loi informatique et libertés [Com78];
- ▶ Difficulté à déterminer une durée adéquate;
- ▶ Nécessairement tout **au long de la relation entre le responsable du traitement et la personne concernée**;
- ▶ Le point de départ d'une durée de conservation : **la suppression du compte utilisateur.**

La durée doit être proportionnée à la finalité du traitement !

Article 30 I de la loi modifiée du 6 janvier 1978 [Com78]

Obligation de mentionner la durée de conservation de leur traitement

Exceptions

Ne concerne pas systématiquement les traitements intéressant la sûreté de l'Etat, da défense ou la sécurité publique.

- ▶ Dérogations;
- ▶ Finalités historiques, statistiques ou scientifiques;
- ▶ Archives publiques ou privées autres;
- ▶ Journalisme ou expression littéraire et artistique.

Condition supplémentaire aux conditions de licéité

Article 7 de la loi informatique et libertés [Com78].

Le responsable de traitement doit obtenir le consentement de la personne concernée avant de mettre en œuvre le traitement.

RGPD [Par16]

Article 6, 1^o, a) : Le traitement n'est licite que si, et dans la mesure où [. . .] la personne concernée a consenti au traitement de ses DP pour une ou plusieurs finalités spécifiques.

Article 4 , 11° RGPD [Par16]

“Toute manifestation de volonté, libre, spécifique , éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair, que des DP la concernant fassent l’objet d’un traitement”

Même si le traitement de DP a reçu le consentement de l'utilisateur, cela ne justifie pas la collecte de données excessives au regard d'une fin particulière.

Consentement = condition cumulative

Prévues à l'article 5 de la loi informatique et libertés [Com78].

- ▶ Condition de la licéité du traitement (\neq droit d'opposition);
- ▶ Retrait du consentement :
 - ▶ Portée limitée : beaucoup de dérogations;
 - ▶ Pas de définition précise donnée par les textes;
 - ▶ Seulement des conditions de validité : La CNIL s'y réfère;
- ▶ Explicite et indubitable;
- ▶ Forme du consentement :
 - ▶ Ecrit privilégié;
 - ▶ Déclaration orale;
 - ▶ Comportement : on peut raisonnablement déduire un accord.

Consentement : sans contrainte

Consentement doit être donné **sans contrainte** : expression du libre choix de la personne concernée.

Le recueil du consentement

pas de risques de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes si la personne ne donne pas son consentement.

Le recueil du consentement

- ▶ Il ne doit porter que sur le traitement envisagé;
- ▶ Ne peut pas être général et ne peut pas s'appliquer à un ensemble illimité d'activités de traitement;

La CNIL a sanctionné un éditeur qui étendait le bénéfice du consentement préalable de ses lecteurs à d'autres publications de la société ainsi que des biens et services de tiers.

Le recueil du consentement

Le consentement doit être **intelligible** et mentionner de façon **claire et précise l'étendue** et les conséquences du traitement des données.

Le contexte dans lequel le consentement s'applique est **limité**.

Le consentement est donné pour un **traitement déterminé** et ne peut pas être étendu.

Article 10 directive 95/46/CE [Com95] et
Article 32 loi informatique et libertés [Com78] :

- ▶ La personne concernée par les DP est informée;
- ▶ De l'identité du responsable du traitement;
- ▶ **Les finalités du traitement;**
- ▶ **Du caractère obligatoire ou facultatif des réponses;**
- ▶ Des conséquences éventuelles, à son égard, d'un défaut de réponse;
- ▶ Des **destinataires ou catégories de destinataires des données;**
- ▶ Directives relatives au sort de ses DP après sa mort;
- ▶ **Durée de conservation des catégories de données traitées.**

G29, 2 types d'exigences supplémentaires :

- ▶ Qualité des informations : texte **clair**, sans jargon, **compréhensible et visible**;
- ▶ Informations doivent être accessibles;
- ▶ Il ne suffit pas qu'elles soient disponibles quelque part.

Preuve du recueil du consentement

- ▶ Le responsable de traitement a la **charge de la preuve**;
- ▶ Directive 95/46/CE [Com95] exige que la personne ait donné son consentement **de manière indubitable**;
- ▶ G29 : il ne doit y avoir **aucun doute, aucune ambiguïté sur l'intention de l'intéressé**

Concrètement : pas d'information explicite sur la preuve

Commission Européenne

Le consentement spécifique exigé ne peut résulter que du consentement exprès de l'utilisateur, donné en toute connaissance de cause et après une information adéquate sur l'usage qui sera fait des données personnelles.

5 Dérogations : Directive 95/46/CE [Com95]

- ▶ Respect d'une obligation légale : Article 7, 1° loi informatique et libertés [Com78];
- ▶ Sauvegarde de la vie de la personne concernée : Article 7, 2° Loi n°78-17 modifiée [Com17];
- ▶ Exécution d'une mission de service public : Article 7, 3° Loi n°78-17 modifiée [Com17];
- ▶ Dans le cadre contractuel : Article 7, 4° Loi n°78-17 [Com17];
- ▶ En raison de l'intérêt légitime poursuivi : Article 7, 5° Loi n°78-17 [Com17].

Interrogations quant à l'utilité...

- ▶ Il existe de nombreuses dérogations;
- ▶ Il semble être placé par l'article 6 du RGPD [Par16] au même rang que celles-ci dérogations;
- ▶ les dérogations sont tellement nombreuses que l'on a l'impression que le recueil du consentement est exceptionnel.

Article 8 Loi du 6/01/1978 [Com78]

“Il est interdit de collecter ou de traiter des données faisant apparaître directement ou indirectement les origines raciales ou ethniques, les opinions philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci”.

Article 9 RGPD [Par16]

Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, [...], ainsi que le traitement des données génétiques, aux fins d'identifier une personne physique de manière unique, des données concernant la santé [...] d'une personne physique sont **interdits**.

Interdictions

Il existe certaines interdictions de traitement en raison de **la nature des données traitées**.

- ▶ Origines raciales ou ethniques;
- ▶ Opinions politiques philosophiques ou religieuses;
- ▶ Appartenance syndicale;
- ▶ Santé;
- ▶ Vie sexuelle;

Possibilité de dérogations à l'interdiction du traitement si la finalité du traitement l'exige. Dérogations **d'interprétation stricte**.

Dérogations

- ▶ Consentement exprès de la personne concernée : Art.8, II, 1° loi 78-17 [Com17];
- ▶ Santé : 3 types de traitement nécessaires concernés :
 - ▶ La sauvegarde de la vie humaine;
 - ▶ La recherche;
 - ▶ Aux fins de la médecine préventive, [...].
- ▶ Associations ou organismes à but non lucratif;
- ▶ Données rendues publiques par la personne concernée;
- ▶ Exercice ou défense d'un droit en justice;
- ▶ Statistiques (soumis à une autorisation de la CNIL);
- ▶ Données anonymisées;
- ▶ Traitements autorisés et justifiés par l'intérêt public.

Droit à la portabilité des données

* Article 20 RGPD [Par16] sur le droit à la portabilité des données.

- ▶ Droit de recevoir les données à caractère personnel les concernant;
- ▶ Dans un format structuré;
- ▶ Lisible par une machine;
- ▶ Droit de transmettre ces données à un autre responsable du traitement;

* Article 34 RGPD [Par16] sur le droit d'être informée de la violation de ses données personnelles

Les flux transfrontières

Pays tiers : hors UE puisque le RGPD est applicable dans tous les pays au sein de l'UE.

RGPD 27 avril 2016 [Par16] : Le droit applicable est déterminé en fonction du lieu d'implantation de l'établissement principal du responsable de traitement.

- ▶ Peu importe la nationalité où le lieu de résidence des personnes concernées;
- ▶ Peu importe la localisation physique des DP;
- ▶ Tout traitement de DP doit être effectué conformément au RGPD.

Exemple concret

un-site.fr qui serait hébergé aux USA par un français qui réaliserait un traitement sur les données des visiteurs (à des fins statistiques).

- ▶ Est-ce que le propriétaire du site est soumis à la loi Européenne ?
- ▶ Sachant que, toutes les récoltes de données ainsi que leurs traitements sont donc effectués sur le sol américain ?

Oui, le RGPD [Par16] est applicable car on prend en considération l'établissement du responsable de traitement et non celui des DP.

Article 44 RGPD [Par16]

Principe général applicable aux transferts.

- ▶ Possibilité de transfert de données vers un pays tiers que si la législation de ce pays permet les mêmes garanties qu'au sein de l'UE.
- ▶ USA : décision d'adéquation préalable au transfert donnée par la commission européenne (article 45 RGPD)

L'action de groupe

L'action de groupe en matière de protection des données personnelles fait désormais partie du paysage légal français depuis la publication au Journal officiel du 19 novembre 2016 de la loi de modernisation de la justice du XXI^e siècle n° 2016-1547 du 18 novembre 2016 [Lé16].

Conditions de l'action de groupe

- ▶ Plusieurs personnes physiques;
- ▶ Placées dans une situation similaire;
- ▶ Subissant un dommage ayant une cause commune;
- ▶ Cette cause commune étant :
 - ▶ Un manquement aux dispositions de la LIL;
 - ▶ De même nature;
 - ▶ Par un responsable du TD ou par un sous-traitant.

L'action de groupe peut être exercée aussi bien devant la juridiction civile que devant la juridiction administrative.

Cette action ne peut tendre qu'à la cessation du manquement, tel que l'arrêt d'un traitement illicite.

Limitations

Le texte limite qui peut exercer une action de groupe. Il s'agit des :

- ▶ Associations régulièrement déclarées depuis cinq ans au moins;
- ▶ Associations de défense des consommateurs représentatives au niveau national;
- ▶ Organisations syndicales de salariés ou de fonctionnaires représentative au sens des articles L. 2122-1, L. 2122-5 ou L. 2122-9 du Code du travail ou du III de l'article 8 bis de la loi n° 83-634 du 13 juillet 1983.

Le champ d'application de cette nouvelle action de groupe semble limité, du fait notamment de l'absence de réparation possible pour les personnes concernées.

Le RGPD [Par16] en mai 2018

Il permettra aux personnes concernées de mandater des organismes, organisations ou associations afin d'introduire une réclamation en leur nom devant l'autorité de contrôle et d'obtenir réparation sous certaines conditions.

Ces dispositions s'inscrivent dans une même tendance de renforcement des droits des personnes en matière de protection des données.

La Loi informatique et libertés (article 34)

Impose aux responsables de traitement de “prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données”.

PIA (EIVP) repose sur 2 piliers

- ▶ Les principes et droits fondamentaux, “non négociables”;
- ▶ La gestion des risques sur la vie privée des personnes concernées.

Mettre en place ces 2 piliers : 4 étapes

- ▶ Étude du contexte;
- ▶ Étude des mesures;
- ▶ Étude des risques;
- ▶ Validation.

L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Les bons côtés

- ▶ La loi protège très bien les données personnelles;
- ▶ La loi est respectée en pratique;
- ▶ Beaucoup d'instances vers qui se tourner en cas de problème.

Les bons côtés

- ▶ La loi protège très bien les données personnelles;
- ▶ La loi est respectée en pratique;
- ▶ Beaucoup d'instances vers qui se tourner en cas de problème.

Les mauvais côtés

- ▶ Beaucoup de loop-holes;
- ▶ Des droits qui semblent impossible en pratique;
- ▶ Des cas extrêmement complexes car Internet est mondiale.

La protection des données personnelles de la théorie juridique à la pratique informatique

Pauline Martin¹, Valentin Montmirail²

¹CDEP, Université d'Artois, Douai, France

²CRIL, Université d'Artois, Lens, France

Douai - 06 Mars 2017

-  Commission Nationale de l'Informatique et des Libertés.
La loi Informatique et Libertés, 1978.
-  Commission Européenne.
Directive 95/46/CE du Parlement européen et du Conseil,
1995.
-  Commission Nationale de l'Informatique et des Libertés.
Loi 78-17 du 6 janvier 1978 modifiée, 2017.
-  Convention européenne des droits de l'homme.
Article 8 de la Conv. EDH, 2010.
-  Correspondant-Informatique Libertés.
Définitions du Règlement européen pour la protection des
données à caractère personnel, 2016.

-  Légifrance Gouvernement Français.
Loi n° 70-643 du 17 juillet 1970, 1970.
-  Légifrance Gouvernement Français.
Loi n° 2004-801 du 6 Août 2004, 2004.
-  Légifrance Gouvernement Français.
Loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle, 2016.
-  Nations Unies.
Article 12 de la Déclaration Universelle des Droits de l'Homme, 1948.
-  Parlement Européen et du Conseil.
Règlement Général sur la Protection des Données, 2016.