Cabinet Infhotep

Protection des données personnelles

Le compte à rebours a commencé

Edition 2016

« Placer l'Homme au cœur de l'organisation »

Cabinet Infhotep
6, rue d'Antin
75002 Paris
France
Tel : +33 (0) 155 353 636
Fax : +33 (0) 155 353 640
www.infhotep.com
contact@infhotep.com

A propos du cabinet Infhotep

Créé en 2005 par un noyau dur d'associés, le cabinet Infhotep est un cabinet de conseil en stratégie et en organisation.

La singularité du cabinet Infhotep est d'accompagner la transformation des entreprises sur l'ensemble de leur chaine de valeur en s'appuyant sur trois grands domaines de compétences : *le business consulting, le conseil en système d'information et le conseil en management de projet.*

Le cabinet Infhotep apporte à ses clients une vision et une assistance globale qui se déclinent sur l'élaboration, la définition, le pilotage et la déclinaison opérationnelle de la stratégie. Les consultants du cabinet Infhotep aident leurs clients à définir et conduire au quotidien la transformation de l'entreprise en s'attaquant aux problématiques métier, d'organisation, d'optimisation de processus et de système d'information, de gestion de projets et de conduite du changement.

Ainsi, le cabinet Infhotep se concentre et capitalise autour des fonctions et activités qui conditionnent la performance de l'organisation de ses clients : marketing, commercial, supply-chain, achats, production, informatique, ressources humaines…

Doté de consultants expérimentés issus du monde de l'entreprise et du conseil, le cabinet Infhotep a pour objectif de permettre à ses clients d'atteindre leurs résultats dans une approche efficace, rationnelle et pragmatique.

Le positionnement et la force de frappe du cabinet Infhotep reposent sur un modèle de gestion des ressources humaines et sur des valeurs fortes telles que l'excellence, l'indépendance, la pédagogie, l'humanisme et le pragmatisme. Avec cette volonté affichée de proposer une équipe unie par une forte culture d'entreprise et des valeurs partagées, le cabinet Infhotep garantit à ses clients un travail réalisé avec éthique, déontologie, confiance, confidentialité et engagement.

Le cabinet Infhotep est organisé en partnership.

Au-delà des compétences et de l'expérience de ses consultants, le savoir-faire et la force du cabinet reposent sur les missions effectuées pour des clients, tels que :

Références secteur privé : Bolloré, Nexity, Weldom, Icade, ICDC, le Gartner Group, Bourse Direct, le PMU, Malakoff Médéric, Eiffage, Logica Training, Reuters, BPB Placoplâtres, Samas Groupe, Inter Mutuelles Assistance, Wurth, Figaroclassifieds, Sofinco, AstraZeneca, LVMH…

Références secteur public et enseignement : Ministère de l'Ecologie, le Cnous, le Cre RATP, Conseils Régionaux de Picardie et Midi-Pyrénées, Conseils Généraux du Val d'Oise et de la Haute-Garonne, FSI, Ville d'Antibes, Ville de Saint Denis, Ville de La Rochelle, Universités de Tours, Orléans, Paris XI, UPJV...

> **Rendre opérationnelles les ambitions des cadres dirigeants**
>
> *Les associés du cabinet du Infhotep*

A propos des auteurs

Alessandro Fiorentino est consultant au sein de la pratique Système d'information du cabinet, en charge de l'activité Informatique et Libertés au sein de la pratique SI du cabinet Infhotep. Il commencé sa carrière en tant qu'analyste-programmeur. Il a par la suite assumé la fonction d'architecte des systèmes d'information au sein d'un grand groupe de courtiers en gestion de patrimoine. Titulaire d'un Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Supérieur d'Electronique de Paris (ISEP), il a soutenu une thèse professionnelle relative à la mise en œuvre du Privacy by Design. Ambassadeur du Privacy by Design depuis mai 2013, il accompagne les entreprises dans le développement de projets intégrant les principes de protection de la vie privée dès la conception.

Antoine Anglade est directeur en charge de la pratique Ressources Humaines du cabinet. Antoine a rejoint le cabinet Infhotep après avoir occupé pendant sept ans des fonctions opérationnelles dans les directions des ressources humaines (Radio France, Alain Ducasse Entreprise…). Il réalise et dirige des missions ayant trait aux pratiques et à l'innovation RH. Il conseille des directeurs RH et leurs équipes de grands et moyens comptes. Antoine Anglade est diplômé du Master Conseil en organisation et conduite du changement de l'Institut International du Management (CNAM).

Marc-Eric Trioullier conseille depuis dix-sept ans les grands comptes du secteur privé et public dans l'évolution de leur système d'information sur les aspects techniques, fonctionnels et organisationnels. Responsable de la pratique Systèmes d'Information au sein du Cabinet Infhotep, il coordonne également l'ensemble de l'offre sécurité au sein du cabinet et anime le séminaire du cabinet sur le plan de continuité d'activité. Marc-Eric est co-auteur de l'ouvrage : « Sécurité des architectures Web » paru chez Dunod (ISBN : 2100073540). Marc-Eric Trioullier est titulaire d'un Master de Méthodes Informatiques Appliquées à la Gestion des Entreprises et d'un DESS Ingénierie Réseau et Système.

Aude de Montgolfier travaille depuis 15 ans dans le domaine du management des informations et des stratégies d'organisation et de fonctionnement documentaires. Elle possède une réelle expertise tant dans le domaine privé que dans le domaine public, à travers des missions précédemment réalisées ou en cours de réalisation. Au sein du cabinet Infhotep, elle porte l'offre sur la gouvernance du patrimoine informationnel.

Pour échanger sur des points qui sont détaillés dans notre étude :

« Protection des données personnelles : le compte à rebours a commencé »

N'hésitez pas à nous contacter :

contact@infhotep.com

Nous tenons à remercier l'ensemble des consultants du cabinet Infhotep pour leurs retours d'expériences aussi divers qu'enrichissants. Plus particulièrement, nous remercions Christian des Lauriers et David Bessot pour leurs remarques et relectures avisées.

Sommaire de l'étude

Infhotep

«L'Europe des données est à un tournant majeur qui la conduira dans les années à venir à assumer un rôle décisif dans le monde numérique.

L'adoption du Règlement sur la protection des données personnelles représente une étape majeure dans la reconquête d'une souveraineté numérique européenne précédemment érodée.

Cet héritage européen incarné dans le Règlement épouse les besoins de l'univers numérique dans lequel nous vivons aujourd'hui. »

Isabelle Falque-Pierrotin
Présidente du G29 (le groupe des Commissions nationales de l'information et des libertés européennes)
Présidente de la Commission Nationale Informatique et Libertés (CNIL)
Et Conseiller d'Etat
HuffingtonPost, publié le 15 juin 2016

Introduction

Notre société a connu depuis quelques décennies de grands changements, la révolution numérique a bouleversé un grand nombre de business modèles.

Les principaux grands groupes du monde mettent en œuvre de plus en plus de technologies automatisées, ceci pour baisser les prix et être concurrentiels dans une économie globalisée. La conséquence de ces nouvelles technologies est une augmentation non négligeable du volume des collectes et des échanges de données.

L'omniprésence de l'informatique provoquée par ces évolutions technologiques permanentes a propulsé au cœur du débat la question de la protection des données à caractère personnel.

Le règlement général sur la protection des données du 27 avril 2016, adopté par le Conseil et le Parlement européen, est l'aboutissement du projet de règlement publié le 25 janvier 2012 par la Commission européenne.

Le règlement a pour objectif le renforcement des droits des citoyens et la modernisation du cadre juridique existant, permettant à l'Europe de faire face à l'essor du numérique et à la mondialisation.

Ce règlement sera applicable à partir du 25 mai 2018 dans tous les pays membres de l'Union européenne abrogeant le Directive 95/46/CE. Pour les entreprises, le compte à rebours a commencé. Néanmoins, un grand nombre d'entreprises françaises ignorent toujours l'existence de cette nouvelle réglementation et son impact pour le système d'Information. Selon l'étude de Trend micro publiée début 2016, 31% des DSI ignorent son existence. Un dirigeant sur dix pense que cette réforme ne s'applique pas à son organisation. Pourtant, ce nouveau cadre juridique devrait impacter les processus des entreprises telles que les ressources humaines, la formation, la fonction commerciale et marketing, tant le spectre de captation des données personnelles est large.

Une prise de conscience à la hauteur de l'importance que représente le sujet de la protection des données personnelles parait aujourd'hui inévitable. Il conviendra d'être en mesure de faire face au nouveau cadre juridique européen introduit par le règlement avant la date d'application.

La directive européenne de 1995 reposait en grande partie sur une logique déclarative par le biais des différentes formalités préalables comme les déclarations, les actes d'engagement ou les demandes d'autorisations. Le règlement général sur la protection des données quant à lui, repose sur une philosophie de conformité dont la responsabilité incombe au « responsable de traitement », sous le contrôle et avec l'accompagnement de l'autorité administrative. Chaque CNIL endossera le rôle de régulateur pour les traitements pour lesquels les citoyens de chaque pays membres sont concernés.

Cette étude vise à vous présenter les résultats de nos travaux de veille et d'analyse en détaillant le contenu de la règlementation. Elle aborde également dans quelle mesure cette règlementation s'applique à votre organisme. Enfin, elle introduit nos premiers conseils à destination de nos partenaires privés et publics afin de se préparer à leur mise en conformité pour 2018.

En synthèse

Applicable à partir du 25 mai 2018, dans tous les pays membres de l'Union européenne, le règlement fait du Correspondant Informatique et Libertés une pierre angulaire de la problématique.

Ce dernier devra accompagner l'entreprise qui l'a désigné à appréhender de nouveaux principes comme :

- la protection des données dès la conception connue également comme le concept de Privacy by Design,
- le droit à la portabilité,
- le droit à l'oubli,
- le principe d'accountability,
- l'obligation de notifier toute violation de données à caractère personnel aux autorités de contrôle mais également aux personnes concernées par ladite violation,
- les Privacy Impact Assessments traduits par la CNIL en "études d'impacts sur la vie privée".

Les prestataires et les éditeurs de logiciel ne seront pas épargnés. En effet, le règlement introduit un principe de coresponsabilité de la sécurité des données de leurs clients.

Nous verrons que la problématique de la protection des données personnelles est omniprésente dans la plupart des entreprises au sein des différents services.

Pour l'organisme, en plus de satisfaire ses besoins en conformité, sa mise en conformité avec le nouveau cadre juridique européen lui permettra d'exclure les éventuels coûts liés aux conséquences financières entrainées par de potentielles atteintes à la vie privée.

Les sanctions encourues en cas de non-respect du règlement général sur la protection des données sont considérablement aggravées. Elles pourront s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaire mondial annuel si cette seconde valeur est supérieure.

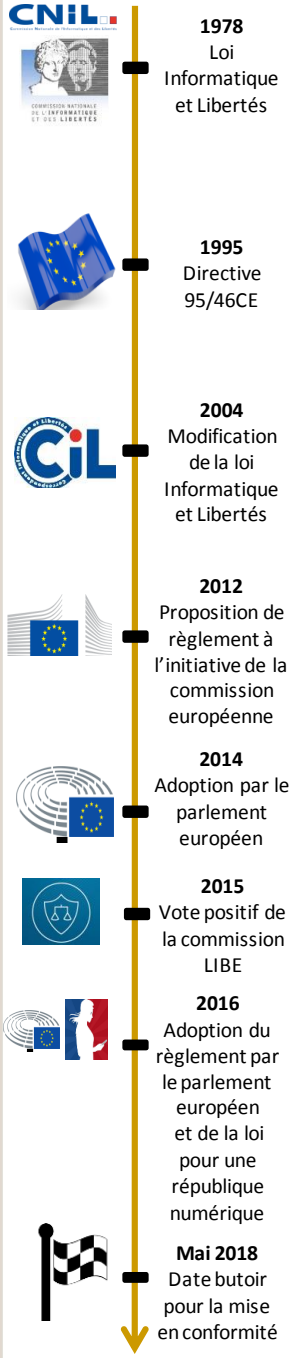
Ce nouveau règlement devrait être considéré par chaque entreprise comme une opportunité d'optimiser sa sécurité juridique. Il ne doit pas se traduire comme une contrainte réglementaire de plus, mais comme un cadre permettant d'affronter la transformation numérique en respectant le droit à la vie privée des clients.

Présenté jusqu'à maintenant comme un avantage concurrentiel, la protection des données personnelles sera sans aucun doute un facteur de confiance des utilisateurs ou des clients, un élément majeur dans la relation client dont les entreprises ne pourront plus se dispenser dans le futur.

Il est maintenant urgent, pour chaque entreprise, d'effectuer un bilan de sa situation déclarative et de compléter sa politique de protection des données à caractère personnel. De manière globale, il s'agit d'anticiper le nouveau cadre juridique introduit par le règlement et de se placer en position d' « adequacy » (l'adéquation de la « privacy »).

La mission du cabinet Infhotep est d'accompagner cette mutation en s'assurant qu'elle permette une réelle valeur ajoutée pour l'entreprise ou l'organisation.

Cadre juridique Informatique et Libertés



Abrogeant la directive 95/46/CE, le règlement général de protection des données ne devra pas être transposé dans les lois nationales des pays membres. Il sera contraignant dès sa date d'application, et en cohérence avec la hiérarchie des textes, il prévaudra sur les lois nationales.

Les entreprises n'ayant pas encore conscience des changements annoncés, nous vous proposons une rétrospective du cadre juridique pour mieux vous aider à appréhender cette nouvelle réforme.

Genèse de la loi du 6 janvier 1978 et naissance de la CNIL

Tout a commencé le 21 mars 1974, Philippe Boucher publia à la une du journal Le Monde, le célèbre article : "Safari ou la chasse aux Français". Cet article alertait sur un projet gouvernemental connu sous le nom de SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus). Préparé par les équipes de Raymond Marcellin, ce projet visait à créer un identifiant unique par le biais du Numéro d'Inscription au Répertoire (NIR) pour chaque citoyen et un croisement de tous les fichiers exploités par l'Etat.

L'article de Philippe Boucher soulignait les potentielles et prévisibles dérives de certaines utilisations de l'informatique, notamment un fichage général de la population.

L'émoi provoqué par ces révélations sur l'opinion publique a conduit le gouvernement à créer une commission afin qu'elle propose des mesures garantissant que le développement de l'informatique ne porte pas atteinte aux libertés individuelles des citoyens.

C'est en 1976 que Jean Lecanuet déposa le projet de loi qui débouchera, en 1978, sur la loi dite "Informatique et Libertés" et sur la création de la Commission Nationale Informatique et Libertés.

Chargée de veiller à l'application de la loi et notamment à ce que l'informatique ne porte atteinte ni à l'identité humaine, ni à la vie privée, ni aux libertés individuelles et publiques, la CNIL est la première Autorité Administrative Indépendante qui fut créé en France.

Le droit à la vie privée et les textes fondateurs

La protection de la vie privée a été affirmée pour la première fois en 1948 par la Déclaration universelle des droits de l'homme des Nations unies à l'article 12.

Article 12
« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Ratifiée par tous les États-membres de l'UE, la Convention européenne des droits de l'homme inscrit en 1950 le droit à la vie privée à l'article 8.

Article 8 al.1
« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance » article 8 al.1 de La CEDH.

La Charte des droits fondamentaux de l'Union européenne découle de la convention européenne des droits de l'homme.

En France, l'article 9 du Code civil y fait également référence depuis la loi du 17 juillet 1970 : *« chacun a droit au respect de sa vie privée ».*

Dans le monde de la protection des données, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est l'un des textes fondateurs.

Le 28 janvier 1981, le Conseil de l'Europe, regroupant 47 États-membres, promulgua la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Appelée également « la convention 108 », elle incita la plupart des États-membres à mettre en place une législation nationale visant à protéger les données personnelles. C'est d'ailleurs en référence à cette date fondatrice, que le « DATA PRIVACY DAY » se passe le 28 janvier de chaque année depuis 1981.

De même, au niveau européen, l'un des textes fondateurs est la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995. Cette directive, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, vise à harmoniser la protection des données personnelles et faciliter leurs échanges à travers les frontières.

Inspirée des « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel », publié en 1980 par l'OCDE, ce texte est le premier à prendre en compte les évolutions technologiques et les nouveaux enjeux comme le développement exponentiel de l'informatique, l'avènement et la consécration de l'Internet ou encore le développement de la biométrie.

Comme son nom l'indique, la directive vise à harmoniser les normes des différents États-membres en matière de protection des données personnelles, ceci afin de faciliter leur libre-circulation à des fins commerciales notamment.

L'évolution de la loi du 6 janvier 1978

Lorsque l'on fait référence à la loi Informatique et Libertés, la désignation la plus courante est la « Loi n° 78-17 du 6 janvier 1978 modifiée ». Ce terme indique que la loi de 1978 a été modifiée afin de transposer la directive européenne 95/46/CE dans la loi nationale.

Rappel : Une directive européenne n'a pas valeur contraignante, elle doit être transposée dans les lois nationales de chaque pays membres afin que les différents principes introduits soient respectés.

C'est donc depuis le 6 août 2004 que la « Loi n° 78-17 du 6 janvier 1978 modifiée », prend en compte à son tour les évolutions technologiques et les nouveaux enjeux comme le développement exponentiel de l'informatique, l'avènement et la consécration de l'Internet.

Les principales conséquences de cette réforme furent un renforcement des pouvoirs a posteriori de la Commission Nationale Informatique et Libertés et la création de la fonction de Correspondant Informatique et Libertés.

Ci-dessous, vous trouverez les principaux mots-clés liés à la protection des données à caractère personnel ainsi que les principes fondamentaux présents dans l'ensemble des textes fondamentaux.

Les mots-clés « Informatique et Libertés »

Une donnée à caractère personnel

Ce terme est définit dans l'article 2 de la « Loi Informatique et Libertés » :

« Constitue une donnée à caractère personnel 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. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

Un traitement / un fichier

Ce terme est également définit dans l'article 2 de la « Loi Informatique et Libertés » :

« Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

« Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.»

Un responsable de traitement

Ce terme est définit dans l'article 3 de la « Loi Informatique et Libertés » :

« Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens.»

Nous verrons au cours de cette étude qu'un principe de coresponsabilité a été introduit dans le règlement général, notamment pour les éditeurs et les sous-traitants.

Les principes fondamentaux

La loi Informatique et Libertés définit les principes à respecter lors de la collecte, du traitement et de la conservation de données personnelles. Elle garantit également un certain nombre de droits pour les personnes concernées. Le nouveau règlement réaffirme ces principes fondamentaux et en introduit des nouveaux.

Principe 1 : la finalité

Avant toute collecte et utilisation de données personnelles, le responsable de traitement doit précisément annoncer aux personnes concernées ce à quoi elles vont lui servir. Ces objectifs, appelés "finalités", doivent respecter les droits et libertés des individus. Ils limitent la manière dont le responsable pourra utiliser ou réutiliser ces données dans le futur.

- La finalité doit être déterminée, légitime et explicite.
- La finalité doit être respectée.
- La finalité permet de déterminer la pertinence des données personnelles que vous recueillez.
- La finalité permet de fixer la durée de conservation des données du fichier.

Principe 2 : la pertinence

Seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées : c'est le principe de minimisation de la collecte. Le responsable de traitement ne doit donc pas collecter plus de données que ce dont il a vraiment besoin.

Certaines données bénéficient d'une protection particulière :

- Les données « sensibles » (les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle d'une personne) mises en exergue dans l'article 8 de la loi Informatique et Libertés.
- Les données relatives aux infractions, condamnations et mesures de sûreté.
- Le numéro de sécurité sociale (NIR).

Principe 3 : la conservation

Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de les conserver et elles doivent être supprimées. La durée de conservation doit être définie au préalable par le responsable du traitement, en tenant compte des obligations réglementaires de conservation (en particulier la réglementation commerciale, civile ou fiscale). La durée de conservation est variable et dépend de la nature des données et des finalités poursuivies.
Certaines données personnelles peuvent, et dans certains cas doivent, faire l'objet d'un archivage lorsqu'elles présentent un intérêt administratif ou historique.

La doctrine de la CNIL à ce sujet repose sur trois catégories d'archives définies par le code du patrimoine :

- La base active également appelée « archives courantes ».
- Les archives intermédiaires dont l'accès doit être restreint en attendant leur suppression ou leur archivage définitif.
- les archives définitives utilisées pour les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction. Ces archives sont déterminées par le Code du patrimoine et leurs traitements sont dispensés des formalités préalables définies dans la loi Informatique et Libertés. Le code du patrimoine régit également les délais de communicabilité pour ces documents lorsqu'ils présentent des informations à caractère personnel.

Il y a quatre principes liés à l'archivage qu'un responsable de traitement doit respecter :

- Un archivage doit être sélectif.
- Un archivage doit être limité dans le temps (hormis pour les archives historiques).
- Un archivage doit être sécurisé.
- Quel que soit le type d'archive, la consultation des données archivées doit être tracée.

Principe 4 : les droits des personnes

Des données concernant des personnes peuvent être collectées à la condition essentielle qu'elles aient été informées de cette opération. Ces personnes disposent également de certains droits qu'elles peuvent exercer auprès de l'organisme qui détient ces données le concernant : un droit d'accéder à ces données, un droit de les rectifier et enfin un droit de s'opposer à leur utilisation.

Toute personne peut :

- Accéder à l'ensemble des informations la concernant.
- Connaître l'origine des informations la concernant.
- Accéder aux informations sur lesquelles le responsable du fichier s'est fondé pour prendre une décision le concernant.
- En obtenir la copie.

- Exiger que ses données soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées.

Le droit d'accès peut s'exercer :

- Par écrit : courrier postal, accompagné d'une copie d'une pièce d'identité. Idéalement, en recommandé avec accusé de réception.
- Sur place : avec présentation d'une pièce d'identité. Il est possible de se faire accompagner par la personne de son choix.

Le responsable de traitement dispose d'un délai de réponse maximal de 2 mois à compter de la date de réception de la demande.

Principe 5 : la sécurité les données

Le responsable de traitement doit prendre toutes les mesures nécessaires pour garantir la sécurité des données qu'il a collectées mais aussi leur confidentialité, c'est-à-dire s'assurer que seules les personnes autorisées y accèdent. Ces mesures pourront être déterminées en fonction des risques pesant sur ce fichier (sensibilité des données, objectif du traitement…).

Plusieurs principes permettent d'optimiser la sécurité des données :

- Chaque utilisateur doit être authentifié.
- Les habilitations doivent être prédéterminées selon un cadre fixé en amont.
- Tous les utilisateurs doivent être sensibilisés.
- Les postes de travail et les périphériques mobiles doivent être sécurisés.
- Les données doivent être sauvegardées.
- La maintenance effectuée par des intervenants et de la sous-traitance doit être encadrée.
- Les accès doivent être tracés et les incidents enregistrés.
- Les locaux protégés.
- Le réseau informatique interne sécurisé.
- Les serveurs et les applications sécurisés, ainsi que les échanges avec d'autres organismes.

Adoption du règlement européen

L'adoption du règlement général sur la protection des données du 27 avril 2016 par le Conseil et le Parlement européen, est l'aboutissement du projet de règlement publié le 25 janvier 2012 par la Commission européenne.

Le règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a été publié au Journal Officiel le 4 mai 2016 et sera applicable à partir du 25 mai 2018 dans tous les pays membres de l'Union européenne.

Il a pour conséquence principale l'abrogation de la directive 95/46/CE du Parlement européen et du Conseil. Cette directive impliquait que les États membres la transposent au sein de leurs propres législations. Elle visait à harmoniser le cadre juridique européen.

Néanmoins, les différentes interprétations des pays membres ont provoqué certaines disparités lors des transpositions dans les législations nationales. Les pouvoirs de sanction des autorités nationales de contrôle n'étaient pas assez importants pour imposer aux grands acteurs du web (tels que les GAFA) de respecter le cadre juridique qui avait été défini.

Le règlement général sur la protection des données poursuit donc l'objectif d'harmonisation des législations européennes. Les institutions européennes ont optés pour la formalisation d'un règlement qui sera directement applicable dans chaque état membre sans qu'aucune

transposition ne soit nécessaire. Ainsi, la nouvelle règlementation est donc pan-européenne et remplacera le patchwork des lois nationales sur la protection des données. Pendant ces deux ans de transition, les entreprises devront se mettre en conformité.

Outre l'harmonisation législative, le règlement général sur la protection des données vise à instaurer une concurrence plus loyale par le biais de l'extension du champ d'application du règlement. En effet, la réglementation s'applique maintenant à toute entreprise, administration européenne et toute entité qui vise ou commercialise des biens ou des services au sein de l'UE, ou qui stocke et utilise des données personnelles de personnes résidant au sein de l'UE. Ainsi, une entreprise établie aux États-Unis ou en Russie qui commercialise ses produits directement à des résidents de l'Union européenne par l'intermédiaire du web, sans avoir de représentation sur le territoire de l'Union européenne, sera soumise aux exigences du règlement. Ce principe aura donc un fort impact sur des entreprises qui observent le comportement de personnes situées au sein de l'UE, tels que Google, Amazon, Facebook, Apple, etc.

Un principe de guichet unique présent dans le règlement permet à une personne concernée par une problématique liée au non-respect de la protection de ses données personnelles d'effectuer ses démarches directement auprès de son autorité administrative. Cette autorité nationale sera en charge d'instruire la demande quelle que soit l'origine du service utilisé.

Cette réforme globale doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique.

Ce nouveau règlement devrait être considéré par chaque entreprise comme une opportunité d'optimiser sa sécurité juridique. Il ne doit pas se traduire comme une contrainte réglementaire de plus, mais comme un cadre permettant d'affronter la transformation numérique en respectant le droit à la vie privée des clients. Présenté jusqu'à maintenant par beaucoup comme un avantage concurrentiel, la protection des données personnelles sera sans aucun doute un facteur de confiance dont les entreprises ne pourront plus se dispenser.

Il est maintenant urgent pour chaque entreprise d'effectuer un bilan de sa situation déclarative et de compléter sa politique de protection des données à caractère personnel. De manière globale, il s'agit d'anticiper l'entrée en vigueur de ce nouveau règlement européen qui prévoit la désignation obligatoire d'un délégué à la protection des données pour tous les organismes privés qui gèrent des données personnelles concernant 5000 personnes et l'ensemble des organismes publics.

Le Correspondant Informatique et Libertés est mort, vive le Data Protection Officier

Le Correspondant Informatique et Libertés

La fonction de Correspondant Informatique et Libertés (CIL) a été introduite en 2004 à l'occasion de la refonte de la loi Informatique et Libertés du 6 janvier 1978 par un amendement parlementaire déposé par Monsieur le Président Alex TÜRK.

« Cette innovation constitue un tournant majeur dans l'application de la loi : l'accent est mis sur la pédagogie et le conseil en amont. En effet, désigner un correspondant à la protection des données permet certes de bénéficier d'un allègement des formalités déclaratives mais c'est surtout s'assurer que l'informatique de l'organisation se développera sans danger pour les droits des usagers, des clients et des salariés. C'est aussi, pour les responsables de fichiers, le moyen de se garantir de nombreux risques vis-à-vis de l'application du droit en vigueur ». Alex Türk

C'est l'alinéa III de l'article 22 de la loi qui donne naissance à ce nouveau métier. L'objectif est de proposer aux responsables de traitement[1] un moyen efficace pour assurer le respect de la réglementation « Informatique et Libertés ».

Le statut du Correspondant Informatique et Libertés (CIL), son rôle, ses missions et les conditions d'exercice de sa fonction seront précisés par le décret du 20 octobre 2005 dans les articles 42 à 55.

Le CIL bénéficie d'un statut spécifique d'indépendance. Il est directement rattaché au responsable des traitements et possède une liberté organisationnelle et décisionnelle. Il ne doit recevoir aucune instruction pour l'exercice de sa mission et arrête seul les décisions s'y rapportant.

A l'abri des conflits d'intérêts, il ne peut être le responsable du traitement ou un délégataire des pouvoirs propres à ce dernier ou encore un représentant du personnel.

Le CIL bénéficie également d'une certaine protection vis-à-vis des sanctions. Il ne peut être déchargé de ses fonctions sans que la CNIL en connaisse les raisons.

Les missions du CIL

Le Correspondant Informatique et Libertés est chargé de tenir la liste des traitements mis en œuvre au sein de l'organisme et d'assurer son accessibilité.

Il doit veiller, en toute indépendance, au respect par le responsable des traitements des obligations qui lui incombent.

Il est en charge de diffuser la « culture Informatique et Libertés » au sein de son organisme, où il doit également être force de conseil et de recommandations.

Le CIL est tenu d'établir un bilan annuel d'activité qu'il doit présenter à son responsable de traitement.

Ce bilan annuel recense l'ensemble des activités qu'il a été amené à effectuer comme les missions d'audits internes, des études d'impact sur la vie privée, l'élaboration de codes de conduite ou encore des actions pédagogiques.

[1] L'article 3 de la loi Informatique et Libertés définit le responsable de traitement comme la personne qui détermine les moyens et la finalité des traitements.

Le Data Protection Officer

Comme nous le précisions précédemment, le règlement européen fait du Correspondant Informatique et Libertés une pierre angulaire de la problématique. Appelé à présent Data Protection Officer (DPO), ce dernier devra appréhender de nouveaux principes afin d'accompagner l'entreprise qui l'a désigné comme la protection des données dès la conception (Privacy by Design), le droit à la portabilité, le droit à l'oubli, le principe d'accountability, l'obligation de notifier toute violation de données à caractère personnel aux autorités de contrôle mais également aux personnes concernées par ladite violation et les Privacy Impact Assessments traduit par la CNIL en "études d'impacts sur la vie privée". En effet une véritable expertise sera désormais nécessaire.

La désignation des Data Protection Officer a donné lieu à de longues discussions dans le cadre du trilogue, en amont de l'adoption du règlement général sur la protection des données. A la lecture du nouveau règlement, il est précisé que « les responsables de traitement et les sous-traitants devront désigner un DPO s'ils appartiennent au secteur public, si leur activité les amène à réaliser du profiling à grande échelle ou si leur activité les amène à traiter (toujours à grande échelle) des données dites « sensibles » ou relatives à des condamnations ». Selon l'Association Française de Correspondant à la protection des Données à caractère Personnel (AFCDP), peu d'organismes échapperont à ces critères.
Il est précisé, comme c'est le cas aujourd'hui, qu'un groupe peut faire le choix de désigner un DPO mutualisé sur plusieurs établissements ou encore opter pour un DPO externe.

En 2016, on compte 4.300 Correspondants Informatique et Libertés désignés par 16.376 responsables de traitement, privés ou publics. Auront-ils tous les compétences nécessaires pour appréhender les évolutions de la fonction ? Face à ce bouleversement, l'AFCDP, qui regroupe les professionnels de la conformité Informatique et Libertés et de la protection des données personnelles, a demandé que soit ménagée une « clause du grand-père » qui permettrait aux CIL qui le souhaitent, et qui répondent aux nouvelles exigences, d'être confirmés dans leur fonction en tant que DPO. Ceci pour capitaliser sur les travaux déjà réalisés et pour assurer la diffusion la plus large possible de l'esprit de la loi.

Voici la réponse apportée par Monsieur Edouard Geffray, Secrétaire général de la CNIL, à l'ensemble des CIL présents lors de son intervention[1] à la conférence organisée le 27 janvier 2016 par l'AFCDP à la Maison de la Chimie à Paris : « *Vous êtes plus de 4.000. Nous avons tout intérêt à ce que la plupart d'entre vous soient confirmés en tant que DPO. Mais les deux fonctions ne cohabiteront pas. A la mi-2018, plus de CIL, mais des DPO. Les modalités de ce « basculement » ne sont pas encore connues, nous allons y travailler. Mais cela nécessitera sans doute un acte formel de la part du responsable de traitement.* »

[1] « Nous avons tout intérêt à ce que la plupart d'entre vous soient confirmés en tant que DPO » - Edouard Geffray, Secrétaire général de la CNIL http://www.afcdp.net/Nous-avons-tout-interet-a-ce-que

Les nouveaux principes introduits dans le Règlement Général sur la Protection des Données

Comme nous le précisions précédemment, de nouveaux principes ont été introduits au sein du règlement général sur la protection des données dont les principaux sont présentés ci-dessous :

Le principe d'accountability

Le règlement général sur la protection des données dans son article 5, introduit le principe d'accountability. Il impose aux entreprises d'être en mesure de justifier l'ensemble des dispositifs de contrôle et d'encadrement mis en place pour assurer la conformité Informatique et Libertés au sein de l'organisme.

Le droit à l'oubli

Une personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant. Le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement ;
- la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2 ;
- les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis ;
- les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1.

Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement prend des mesures raisonnables, y compris d'ordre technique, pour informer les autres responsables du traitement qui traitent ces données que la personne concernée leur a demandé l'effacement de tout lien vers ces données, ou de toute copie ou reproduction de celles-ci.
Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3 ;
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ;
- ou à la constatation, à l'exercice ou à la défense de droits en justice.

Renforcement des conditions du consentement

Dans les cas où le traitement repose sur le consentement, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement doit être présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.

La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.

Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

Une des nouveautés dans l'encadrement du consentement est la prise en compte des conditions applicables au consentement des enfants.

Le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans. Lorsque l'enfant est âgé de moins de 16 ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant.

Les États membres pourront prévoir par la loi un âge inférieur pour ces finalités à condition que cet âge inférieur ne soit pas en-dessous de 13 ans.

Le droit à la portabilité

Le droit à la portabilité dans l'article 20, impose au responsable de traitement d'assurer aux personnes concernées le droit de recevoir les données à caractère personnel les concernant, telles qu'elles les ont fournies. Ces données doivent être transmises dans un format structuré, couramment utilisé et lisible par machine. L'article 20 impose également le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle.

Tant que des structures standardisées n'auront pas été déterminées, ce principe reste difficile à mettre en œuvre. Néanmoins, nous considérons qu'une seconde lecture de ce principe peut se traduire par l'automatisation du droit d'accès. En effet, la mise en place d'une fonctionnalité permettant aux personnes disposant d'un compte en ligne d'obtenir une extraction globale de ses données, serait une première forme de prise en compte du principe qui devra être optimisée lorsque que des formats ou des structures standardisées auront été formalisées par le régulateur.

La protection des données dès la conception

La protection des données dès la conception (Privacy by Design), recommande par le biais de l'article 25 d'intégrer (à toute technologie exploitant des données à caractère personnel) des dispositifs techniques de protection de la vie privée dès sa conception et des mesures organisationnelles permettant d'anticiper en amont des projets informatiques, la problématique de protection des données personnelles.

Ce concept de Privacy by Design n'est pas récent. La protection intégrée de la vie privée (PIVP) ou le respect de la vie privée dès la conception (en anglais «Privacy by Design», PbD) est une idée développée durant les années 1990 par la Commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada), Ann Cavoukian.

Partant du principe que le cadre légal ne serait pas suffisant pour assurer la protection de la sphère privée, elle a proposé d'intégrer le respect de la vie privée directement dans la conception et le fonctionnement des systèmes et réseaux informatiques, mais également dans l'élaboration de pratiques responsables.

Le respect de la vie privée dès la conception, signifie prendre en compte dès le début les exigences en matière de protection de la sphère privée/protection des données et intégrer les outils de protection directement dans le produit, au lieu de les ajouter ultérieurement sous forme de compléments.
Le concept de Privacy by Design repose sur sept principes fondamentaux :

- Prendre des mesures proactives et non réactives, des mesures préventives et non correctives.
- Assurer la protection implicite de la vie privée.
- Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques.
- Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle.
- Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements.
- Assurer la visibilité et la transparence.
- Respecter de la vie privée des utilisateurs.

L'article 25 ne traduit que les deux premiers principes fondamentaux. Le principe de transparence est traduit par le biais de l'article 12.

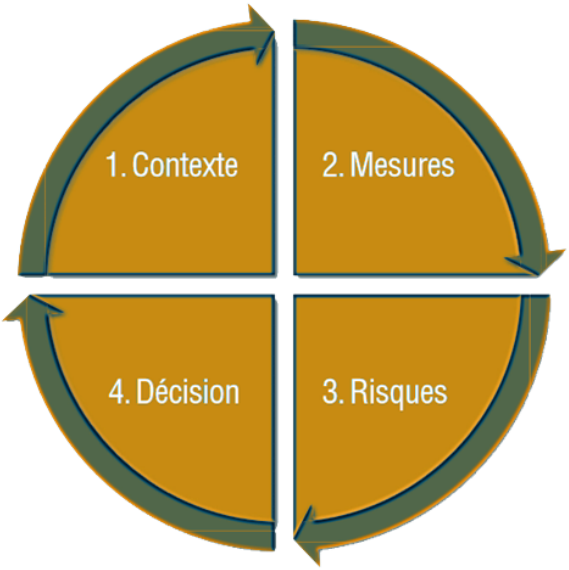
Cette étude vise à vous présenter l'ensemble des fondamentaux liés à la protection des données. Elle apporte une vision globale des nouveaux principes introduits dans le règlement général sur la protection des données. La protection des données dès la conception et la mise en œuvre du concept de Privacy by Design feront l'objet d'un prochain livre blanc « Privacy by Design, une démarche éthique ».

Les Privacy Impact Assessments

Les Privacy Impact Assessments, par le biais de l'article 35 (traduit par la CNIL en "études d'impacts sur la vie privée"), devront être réalisées sur l'ensemble des traitements considérés comme sensibles par le Correspondant Informatique et Libertés, le futur "Data Protection Officer".

Les prestataires et les éditeurs de logiciel ne seront pas épargnés. En effet, le règlement introduit un principe de coresponsabilité. Ils pourront donc être amenés à réaliser directement les études d'impacts nécessaires à la mise en place de leurs solutions et seront, par la même occasion, responsable de la sécurité des données de leurs clients.

La CNIL recommande une démarche en 4 étapes pour rédiger une étude d'impacts sur la vie privée :



- L'étude du contexte permettra de délimiter et de décrire les traitements considérés, leur contexte et leurs enjeux.
- L'étude des mesures a pour objectif d'identifier les mesures existantes ou prévues, d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée.
- L'étude des risques apprécie les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée.
- L'étape de validation permet de décider la manière dont il est prévu de respecter les exigences légales et de traiter les risques. Cette étape peut aboutir à une nouvelle itération des étapes précédentes.

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

La notification aux personnes concernées

La notification obligera les entreprises à déclarer toute violation de données à caractère personnel aux autorités de contrôle par le biais de l'article 33 mais également aux personnes concernées par ladite violation via l'article 34.

L'article 34 du règlement intitulé « Communication à la personne concernée d'une violation de données à caractère personnel », indique que, « lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation à la personne concernée dans les meilleurs délais ».

L'alinéa 3 de ce même article, introduit plusieurs exceptions. Notamment lorsque le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriés appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement.

Cet alinéa place le chiffrement comme un moyen d'exonération privilégiée à l'obligation d'information des personnes concernées par une violation de données.

Pour le Data Protection Officer, il conviendra donc d'appréhender l'ensemble des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données afin de contrôler et de d'effectuer des recommandations adaptées en fonction des cas d'usage.

Des risques accrus en cas de violation ou de non-respect

Comme vu précédemment, le règlement impose une notification de violation de données aux personnes concernées. L'article 33 du règlement impose que les responsables du traitement doivent informer l'autorité administrative de la nature de la violation, des catégories de données et du nombre de personnes concernées ainsi que des mesures prises pour atténuer la gravité de ladite violation. L'article 34 ajoute que les personnes concernées doivent aussi être notifiées de la violation.

Ainsi l'impact d'un manquement dans la gestion et la protection des données personnelles entraine une divulgation publique qui peut désormais se traduire par des litiges, un risque d'image accru et des pénalités financières conséquentes qui peuvent se traduirent par des demandes d'indemnisation ou des sanctions financières. Le règlement général sur la protection des données introduit également par le biais de l'article 82 un droit à réparation des dommages matériels ou moraux suite à une violation du règlement. Toute personne ayant subi un dommage matériel ou moral – du fait d'une violation du règlement – a le droit d'obtenir du responsable du traitement ou du sous-traitant, réparation du préjudice subi. Les citoyens peuvent également se faire représenter par des organismes spécialisés dans la protection des données grâce à l'article 80.

La nouvelle loi pour la république numérique, introduit quant à elle des recours collectifs de type «class actions», en mandatant des associations dédiées pour être indemnisés en cas d'infractions à la loi. Le risque financier d'une violation du règlement s'en trouve donc fortement aggravé.

De plus, les sanctions encourues en cas de non-respect du règlement général, se sont considérablement aggravées. Elles pourront s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaire mondial annuel si cette seconde valeur est supérieure.

Une problématique omniprésente dans les organismes

Les nouvelles technologies ont créé de nouveaux usages. Nos rapports avec les données personnels ont évolués. Les appareils mobiles sont maintenant omniprésents. Les données professionnelles s'affranchissent des mesures de sécurité mises en place par l'entreprise. Les employés s'envoient des documents par e-mail ou par messagerie instantanée. Ils utilisent leurs smartphones et tablettes personnelles pour accéder à leurs données professionnelles et stockent leurs données dans le cloud, un nuage numérique dont ils ne peuvent apprécier ni la localisation réelle, ni le cycle de vie de potentielles redondances.

Les instances européennes conscientes de ces évolutions, ont voulu renforcer et adapter le dispositif législatif à ces changements et à l'explosion de la création et de l'utilisation des données à caractère personnel.

Dans la suite de ce chapitre, nous mettrons en lumière les nouvelles relations des entreprises avec les données à caractère personnel afin d'avoir pleinement conscience que se mettre en conformité est bien un enjeu pour toutes les entreprises aujourd'hui.

Une omniprésence de la donnée personnelle à protéger

« En France on n'a pas de pétrole mais on a des idées… ». Ce slogan vieux de 40 ans n'est plus d'actualité à l'ère du numérique. Comme l'a dit Axelle Lemaire, la Secrétaire d'État auprès du ministre de l'Économie et des Finances, chargée du Numérique et de l'Innovation, « la donnée est devenue le pétrole du XXIème siècle ». A l'aube de l'ère de l'informatique ubiquitaire, nous produisons des données chaque jour dans notre vie.

Troisième ère de l'histoire de l'informatique, succédant à celles des ordinateurs personnels et des mainframes, l'informatique ubiquitaire repose sur une forme de réseau omniprésent. Souvenez-vous, lors de l'ère des mainframes, un grand ordinateur était utilisé collectivement par plusieurs personnes. Par la suite, celle des ordinateurs personnels, un ordinateur était utilisé exclusivement par une seule personne.

Dans l'ère de l'informatique ubiquitaire, l'utilisateur a à sa disposition une multitude de petits appareils comme le smartphone, les objets connectés et bientôt les nanotechnologies. Pour certains de ces appareils, leur utilisation fait déjà partie de nos vies quotidiennes.

Beaucoup plus de données sur les individus sont maintenant disponibles et utilisables. Ces quantités de données sont récoltées à des fins de prévision, d'analyse ou de prédiction. « Master Data Management », « Big Data », « Open Data », « Data Mining » sont au cœur des préoccupations des entreprises. Ces technologies revoient la façon dont les entreprises sont amenées à gérer les données dont elles disposent ou peuvent disposer sur leurs clients, leurs prospects, leurs employés, leurs partenaires… Ainsi toutes les entreprises manipulent des données à caractère personnel.

Certaines données à caractère personnel sont collectées sans même que le responsable de traitement ait conscience des impacts que ces données peuvent provoquer. Les cookies sont aujourd'hui présents pour la gestion des statistiques d'audience et pour analyser la navigation des utilisateurs dans la majorité des sites web. Néanmoins, encore très peu d'entreprises ont adopté une politique d'utilisation des cookies.

Les logs d'utilisation des systèmes sont également présents dans toutes les entreprises. Ils font rarement l'objet de formalités auprès de la CNIL alors que ces traitements agrègent une myriade de données personnelles sur les navigations du personnel et peut permettre aux entreprises de retracer les temps d'activité.

Comme l'article 34 de la loi Informatique et Libertés impose au responsable de traitement d'assurer la sécurité des données personnelles des traitements liés à son activité dont il a défini les finalités et les moyens, toutes les entreprises devraient se sentir visée par la nouvelle règlementation. Par exemple, Elles ont bien défini des traitements concernant la fonction commerciale pour effectuer les opérations relatives à la gestion des clients ou effectuer des opérations relatives à la prospection. Ainsi chaque organisme se doit de sécuriser les données à caractère personnel de ses clients, de ses prospects et des utilisateurs liés à son activité.

De plus, comme évoqué dans les précédents chapitres, ce nouveau règlement sur la protection des données a élargie son périmètre d'application. En effet, toutes les entreprises ayant des relations commerciales ou de services avec des citoyens européens quel que soit l'endroit où se trouve l'entreprise doivent le respecter. Ainsi elle se rapproche des lois américaines et allemandes sur la protection des données. Par exemple, une société établie en Chine comme « alibaba » ayant des clients français doit impérativement respecter le règlement européen sur la protection des données.

Alors êtes-vous toujours convaincu que cette nouvelle règlementation ne s'applique pas à votre organisation ? Alors peut être que votre société souhaite prendre le virage du numérique et revoir sa stratégie digitale. Ces données à caractère personnel sont au cœur de ce virage.

La donnée à caractère personnel une valeur marchande en devenir

Au sein de la nouvelle économie, les données à caractère personnel ont une valeur financière. La donnée est en effet devenue l'actif stratégique des nouveaux pure players que sont Google, Apple, Facebook ou Amazon. Les informations sur les utilisateurs et les clients permettent d'acquérir ou de conserver un avantage concurrentiel pour les entreprises. Elles permettent aussi d'optimiser leurs activités en termes d'acquisition, de rétention, de ciblage, de tarification adaptée, etc. Tout en permettant d'optimiser et de mieux valoriser ses propres espaces publicitaires.

Cette valorisation des nouvelles entreprises se voit souvent calculée à partir de leur base d'utilisateurs et des données qu'elles renferment. Par exemple, la société Whatsapp, lors de son rachat par Facebook, a été valorisé à 19 milliards de dollars, soit environ 30$ pour chacun de ses 600 millions d'utilisateurs estimés. Lors du rachat de Minecraft par Microsoft, le cout estimé du portefeuille client et des informations les concernant était de 25$. Dans ces cas de figure, la variabilité du prix va dépendre du type de données que l'entreprise collecte, de son activité et du profil de sa population.

Plus les informations collectées au sein de sa base client sont riches et complètes, plus l'entreprise pourra monétiser ses utilisateurs, et donc plus grande en sera sa capitalisation.
Dans les années à venir grâce aux technologies de « Big Data », deux types d'acteurs vont voir leur développement exploser :

- les collecteurs/fournisseurs de données personnelles
- les entreprises capables d'analyser ces volumétries afin d'en tirer une connaissance et de les exploiter.

Les courtiers en données sont des sociétés qui recueillent et agrègent des renseignements sur les consommateurs à partir d'un large éventail de sources, afin de créer des profils détaillés d'individus. Ces entreprises vendent ou partagent vos informations personnelles avec d'autres. Les courtiers en données sont parfois aussi appelés revendeurs d'informations, fournisseurs de données ou courtiers en information.

Généralement, les courtiers de données sont des sociétés avec lesquelles les individus n'interagissent pas ou ne font pas affaire directement. Les courtiers en données peuvent vendre les informations qu'ils compilent à d'autres sociétés (y compris d'autres courtiers de données), à des organisations, à des organismes gouvernementaux ou à d'autres

personnes. Dans certains cas, ils pourraient échanger ces informations dans le cadre d'un accord de coopération plutôt que de les vendre. Dans d'autres cas, ils peuvent fournir l'information sans frais, faire de l'argent par la publicité ou des renvois.
La Federal Trade Commission (FTC) a défini les courtiers en données comme des «sociétés qui recueillent des renseignements, y compris des renseignements personnels sur les consommateurs, à partir d'une grande variété de sources afin de revendre de telles informations à leurs clients à diverses fins.

Il est à noter que pour l'heure, le seul acteur de notre nouvelle économie qui ne s'intéresse que très peu à ces données est finalement l'individu qui en est lui-même la source, Nous. Et cela alors que des sujets comme l'usurpation d'identité ou la protection des données font régulièrement l'actualité.

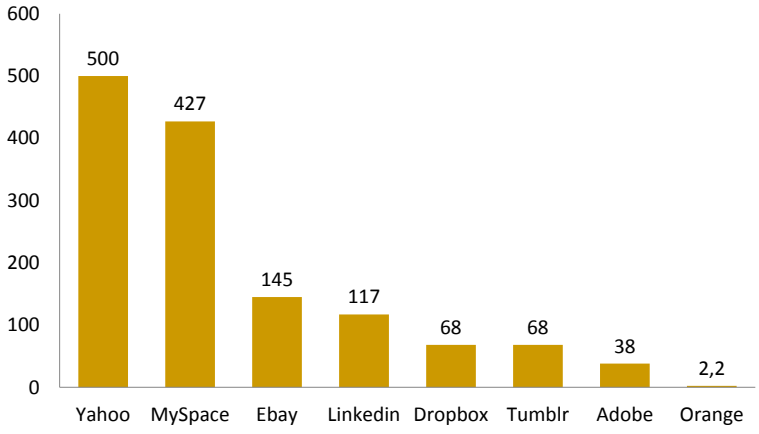
Le paradoxe humain : où se trouve la frontière de la violation de l'intimité ?

A travers les âges notre rapport avec l'intimité a beaucoup évolué et continue de changer. Il est tributaire de notre culture. Dans l'antiquité nous nous lavions dans des bains publics, nous nous montrions nus. Au fil des siècles, le souci des convenances, l'image de soi ont imposé un cloisonnement et une séparation de nos vies avec plusieurs échelles d'intimité. Or dans notre nouvelle ère, nous observons un revirement de ce qui est de l'ordre du public et de ce qui est de l'ordre du privée.

Les « stars » et les politiques exposent dans les médias leurs ruptures, leurs rencontres. Les émissions de télé-réalités envahissent nos écrans. Les gens se racontent, se dévoilent sur les réseaux sociaux, les blogs ou autres pages personnelles. Bref nous opposons très peu de résistance à confier et diffuser nos données personnelles. Mais parallèlement, l'opinion publique s'indigne face à des cas de violation de notre intimité par des gouvernements. En effet, les révélations d'Edward Snowden ont provoqué une prise de conscience des internautes poussant les géants du web - considérés comme de simples informateurs de la NSA - à revoir leur politique de protection des données afin d'assurer la confiance des utilisateurs mise en péril à chaque publication d'article traitant de la surveillance généralisée.

Des violations toujours récurrentes dans un but lucratif

Selon le sondage de Trend micro, 71% des DSI ont confiance en leur entreprise lorsqu'il s'agit de protection des données. La conformité à la nouvelle règlementation ne devrait donc pas poser de problème à ces entreprises. Mais permettez-nous d'avoir un doute sur ce degré de confiance. Les violations de données personnelles sont monnaie courante aujourd'hui et font l'objet de nombreux articles à travers la presse. Par exemple, en 2015 l'accès frauduleux d'une base de contacts de France Télévision comportant plus de 100 000 téléspectateurs (nom, prénom, adresse postale, email et téléphone) qui s'étaient inscrits à des jeux. Bien que cela représente moins de 1% des 12 millions de contacts que France Télévisions possède dans ses bases, cela a une incidence à la fois sur la crédibilité de l'entreprise (déjà mis en cause avec l'affaire TV5 monde), mais aussi sur les personnes individuelles qui sont impactées.



Les principaux vols de données personnelles depuis 2013 en millions
Sources : Le Monde, Motherboard, Leakedsource

Ces violations nous font courir, en tant qu'individu, le risque de se voir voler notre identité, d'être impliqué dans des actions frauduleuses à notre insu ou bien encore de nous faire subir des pertes financières. Et si nous, en tant qu'entreprise, venions à être à la source d'une violation, nous devrions faire face au risque de payer des amendes ou de perdre la confiance de nos clients, partenaires et investisseurs. Le risque de violation n'est donc pas à prendre à la légère.

Le marché noir du piratage de données personnelles

L'objectif de ce genre d'attaque est bien souvent la revente d'informations à caractère personnel au sein du « Dark Web ». Les cybercriminels recherchent toute les informations possibles, les achètent, les exploitent et les revendent. Ils vont s'intéresser :

- Aux adresses postales pour des DropBox (boites aux lettres physiques pour se faire envoyer des produits acquis avec des données bancaires piratées) ;
- Des adresses mails pour réaliser des actions de phishing ou de spams ;
- Des factures et fiches de paie pour des escroqueries bancaires ;
- Des informations relatives aux cartes d'identités et autres permis de conduire pour des usurpations d'identités.

Pour les cybercriminels, le Saint Graal, c'est votre « Fullz », ou votre ensemble complet de données personnelles. Et ils vont aller très loin pour l'obtenir.

Depuis 2005, plus de 6000 entreprises et organisations ont signalé des violations. A en juger par les tendances antérieures, environ la moitié de ces infractions sont susceptibles d'exposer des informations sensibles, où les noms des consommateurs sont jumelés avec des données supplémentaires telles que des adresses, des numéros de téléphone, des

dates de naissance, des numéros de sécurité sociale et des dossiers médicaux. En 2015, près de 165 millions de fichiers contenant des numéros de sécurité sociale ont été compromis dans 338 violations, selon « Identity Theft Resource Center ».

Les cybercriminels cherchent à réunir les informations complètes d'un individu pour faciliter le vol d'identité, permettre l'achat de biens et de services sur Internet et ouvrir de nouveaux comptes au nom de la victime. Les « Fullz » sont également en vente dans les marchés souterrains et le dark web, entre 15 et 65 dollars pour l'enregistrement complet d'un citoyen des États-Unis, selon les données recueillies par les services de sécurité société Dell SecureWorks.

Alors que l'industrie de la sécurité est axée sur la prévention des violations, les criminels sont concentrés sur l'extraction de valeur à partir des données volées. Comme une entreprise construisant un profil d'un client, les criminels essaient de créer un dossier numérique complet sur les victimes potentielles.

Les gens ne sont pas la seule cible de la collecte d'identité. Des dossiers assez complets sur les entreprises, principalement des entreprises russes, peuvent être achetés entre 40 000 et 60 000 roubles (de 500 à 800 dollars), selon le rapport de Dell Secureworks. Les dossiers comprennent les statuts constitutifs de la société, les contrats de location et le numéro d'identification fiscale.

Vos bases de données un actif fortement convoité

Une autre pratique s'est développée au sein des groupes de pirates informatiques, le chantage à la diffusion d'informations personnelles. Ce business consiste à pirater des bases de données de société et de demander une rançon sous peine de revendre les informations ou de les diffuser. Le groupe Rex Mundi s'est fait connaitre au travers de tels exploits chez de grandes entreprises tel que Domino's pizza, la Banque Cantonale de Genève (BCGE), Numéricable, le laboratoire médical Labio, etc. Le montant des chantages est relativement faible ; pour l'instant entre 10 et 30K€.

Ainsi, les bases de données représentent aujourd'hui des actifs stratégiques pour les organismes qu'ils soient publics ou privés. Elles jouent un rôle majeur dans la fonction commerciale. Un grand nombre d'informations liées aux clients y sont stockées. On peut aussi y retrouver les informations inhérentes aux différents produits ou services. Elles représentent une véritable valeur économique au sein du patrimoine des entreprises et sont une composante clé de leur compétitivité. Comme tout objet de valeur, ce patrimoine informationnel suscite donc des convoitises.

La pire situation à laquelle une entreprise peut être confrontée – mais qui pourtant est un grand basique du piratage – s'appelle le "dump". Il s'agit de l'extraction complète de la base de données de l'organisme qui implique souvent une violation de données à caractère personnel.

Ce type d'attaque peut être effectué par des entités externes à l'organisme, tel que REX Mundi ou des entreprises concurrentes. Mais ces attaques sont le plus souvent réalisées par des acteurs internes à l'entreprise qui se rendent responsables de fuites vers l'extérieur par méconnaissance ou volontairement lorsqu'ils quittent l'entreprise en emportant avec eux des données (une base de contact commerciale par exemple).

Afin de lutter contre ces comportements, on peut travailler sur la sensibilisation du personnel. Mais il est préférable de prévenir toutes dérives potentielles en créant les conditions d'une protection adéquate de ces actifs immatériels. Le système de chiffrement symétrique par exemple est un dispositif technique qui permet de limiter les conséquences collatérales d'un piratage en chiffrant le contenu des bases.

Toujours pas convaincu que cette règlementation s'applique à votre entreprise ? Nous vous proposons de regarder un dernier prisme qui finira de vous convaincre : Vos référentiels employés.

Si vous n'avez pas de clients, vous avez des employés

Lorsqu'on parle de données à caractère personnel, les gens se focalisent sur leurs clients, leurs prospects ou leurs usagers. Il ne faut pourtant pas oublier le premier référentiel de données personnelles que toute entreprise a : sa base d'employés.
Les données du personnel de l'organisme sont donc également des données qui doivent faire l'objet de formalités, qui peuvent dans certaines situations être considérées comme sensibles.

En effet, il existe un certain nombre de finalités de traitement liées aux ressources humaines comme : la gestion du personnel, la gestion de la paie, le fichier de recrutement, la vidéosurveillance au sein de l'entreprise, la gestion des réunions des instances représentatives du personnel, la gestion de l'annuaire du personnel, la gestion des œuvres sociales et culturelles, le contrôle de l'utilisation d'internet, le contrôle de l'utilisation de la messagerie, la gestion de la téléphonie, la géolocalisation des véhicules professionnels, le contrôle des horaires, la gestion de la restauration, le contrôle d'accès à des lieux physiques ou virtuels, le fichier des sanctions disciplinaires, l'enregistrement des conversations téléphoniques sur le lieu de travail à des fins de preuve dans le secteur bancaire ou encore l'enregistrement des conversations téléphoniques sur le lieu de travail à des fins de formation.

Les enjeux RH vis-à-vis de la protection des données à caractère personnel

Il est presque tautologique de parler protection des données à caractère personnel vis-à-vis d'une fonction clé de l'entreprise qui – il n'y a pas si longtemps encore – se nommait "Direction du Personnel". Il est évident que plus aucun DRH n'ignore les fondamentaux relatifs à la protection des données. Ils les appliquent dans la mise en œuvre de son action et la conduite des projets RH. Pour autant, les récentes évolutions en matière de protection des données à caractère personnel ont de nouvelles implications pour la fonction RH qui nécessitent une évolution dans les pratiques et la mise en œuvre de projets spécifiques à court terme.

Parler de données RH évoque naturellement les activités de reporting et de contrôle de gestion social qui se sont beaucoup développées ces dernières décennies, conjointement à l'intérêt croissant des dirigeants et des actionnaires pour les indicateurs dits "non-financiers".

Rassurons-nous, ce domaine n'est que peu impacté par les nouvelles exigences à venir en matière de protection des données personnelles. En effet, dans la production d'analyse RH, les données sont la plupart du temps agrégées et anonymisées. Ainsi, le principe de confidentialité est respecté. De plus, les sources de données entrent généralement dans le cadre des normes simplifiées relatives à la gestion du personnel et bien connues des DRH.

En revanche, trois pratiques sont en forte évolution au sein des DRH et nécessitent une prise de conscience sur les risques associés à la protection des données à caractère personnel : le marketing RH, la gestion des connaissances et les baromètres de qualité de vie au travail. Le marketing RH se développe depuis une dizaine d'année. Il consiste à segmenter les populations gérées par la DRH et à adapter et promouvoir l'offre de services en conséquence auprès de ces populations.

A l'origine de cette pratique, une concurrence accrue sur le marché des "talents" parmi lesquels se trouvent pêle-mêle les jeunes diplômés des grandes écoles, les détenteurs de compétences rares et les personnes ayant occupé des postes à responsabilité à l'international et souvent un mélange de tout cela.

Aujourd'hui, l'approche marketing s'est déployée et s'applique à toutes les populations RH ou presque : candidats, jeunes recrues, senior, top managers, etc. Les segmentations RH tendent vers plus de complexité et de détail afin de proposer une offre de service toujours

plus adaptée et surtout d'en démontrer l'efficacité, voire le retour sur investissement. La constitution et le suivi de ces segments de population RH fait appel à la collecte de données très diverses. Par souci d'efficacité du dispositif, il peut être tentant d'intégrer aux algorithmes marketing des données de plus en plus personnelles telles que le profil psychologique du salarié, ses affinités (sujets ou personnes) au sein de la plateforme sociale interne, son comportement au sein d'une équipe, etc. Ce faisant le DRH serait tenu de faire une demande d'autorisation à la CNIL spécifique à ces données et les traitements qu'il envisage de mettre en œuvre. Mais ce n'est pas tout, l'approche marketing si elle va jusqu'à définir des offres de service automatique en fonction des profils entre en tension avec le principe en vigueur s'attachant à ce qu'« aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité » (art. 10 al. 2 de la loi du 6 janvier 1978).

Le management des connaissances et des compétences constitue un autre enjeu RH au cœur des préoccupations des DRH. L'analyse de la performance individuelle et collective, la détection des expertises, la construction de plans d'évolution ou de carrière constituent autant de processus clés dans le management du capital humain. Dans le même temps, ce sont des processus fortement exposés aux exigences en matière de protection des données personnelles. Les discussions sont souvent âpres en comité d'établissement lorsqu'il est question de positionner les salariés individuellement par rapport aux évolutions prévisibles de leurs métiers. Pourtant, seul un positionnement individuel permet de définir des parcours d'évolution adapté et d'optimiser les investissements financiers et les temps passés par chaque partie prenante dans la mise en œuvre de ses parcours.

De manière plus triviale, les DRH vont devoir intégrer à leur plan de formation 2017 et 2018 la formation des DPO ainsi que des actions de sensibilisation des salariés et des managers.
La mise en place de la future réglementation européenne instaure le rôle de Data Protection Officer (DPO) et ce nouveau rôle dépasse en bien des points le profil de compétences d'un CIL. Or, en vertu de la clause du "Grand Père" qui semble s'imposer, ce sont ces CIL qui vont dans la majorité des cas endosser le rôle de DPO dans les entreprises. Ainsi, la formation systématique des CIL semble incontournable. Parallèlement, il semble opportun d'engager des actions de sensibilisation auprès des salariés. L'objectif premier de ces actions est d'éveiller la prise de conscience chez l'ensemble des salariés sur les risques que présentent la collecte et l'analyse des données à caractère personnel et à instiller chez chacun quelques bonnes pratiques et usages quotidiens. Par exemple, il peut s'agir d'apprendre à restituer des études de manière non-nominative. Indirectement, ces actions bénéficieront à l'image employeur de l'entreprise qui vantera alors son respect des données personnelles de ses salariés.

Les baromètres sociaux de plus en plus répandus représentent la troisième pratique à risque en termes de protection des données personnelles. En effet, très peu d'entreprise garantissent l'anonymat des réponses des salariés au enquêtes et baromètres internes, sur des thématiques qui relève pourtant parfois du champ privé (mal-être au travail, pratiques managériales, équilibre avec la vie privée, etc.) : soit les questions relatives à la fonction du salarié permettent de l'identifier de manière certaine, soit l'adresse IP ou d'autres données identifiantes sont collectées, et souvent les clauses de confidentialité du contrat ne sont pas suffisantes, voire inexistantes.

Enfin, et de manière assez peu attendue, la nouvelle réglementation européenne invite les DRH à passer leur pratique de prévention des risques professionnels et psychosociaux au crible des nouvelles exigences sur les données à caractère personnel.

Focus sur la prévention des risques professionnels et psychosociaux

Les obligations de l'employeur quant à la garantie de la bonne santé physique et psychologique des salariés remontent au XIXe siècle. La création des Comité d'Hygiène, de Sécurité et des Conditions de Travail (CHSCT) en 1982 a constitué un jalon important dans la prise de conscience des directions, notamment des ressources humaines, de la nécessité de prendre en compte ces aspects dans leur politique et surtout leur action. L'histoire continue et semble s'être amplifié au cours des deux dernières décennies.

Plusieurs facteurs ont en effet accru les enjeux relatifs à la prévention de ces risques professionnels. Parmi les principaux, citons la prise de conscience politique et les évolutions législatives qui ont fait suite au scandale de France Telecom en la matière, les évolutions technologiques et la surabondance d'information ainsi que l'automatisation de la production de bien et de services qui en découlent, les exigences réglementaires croissantes de l'Europe en la matière.

Or la prise en compte de ces exigences impliquent bien souvent de collecter, de traiter et de sauvegarder des données à caractère personnel, voire des données sensibles comme celles relatives à la santé d'un salarié. La direction RH se trouve donc dans une situation paradoxale l'obligeant tout à la fois à un management des risques professionnels tenu à une obligation de résultat d'un côté et à la protection des données personnelles de l'autre côté. Quelle est la réalité de cette apparente injonction paradoxale ? Quelles peuvent être les bonnes pratiques et les pistes d'action à mettre en œuvre ?

Afin d'appréhender plus précisément cette question, Antoine ANGLADE, notre responsable de la pratique RH au sein du cabinet Infhotep a interviewé Madame Armande BRU-FRANCOIS, Consultante Informatique et Libertés chez DEVOTEAM. Titulaire d'une Licence en science politique, d'une Maîtrise en droit international, d'un Master en droit européen elle a soutenu une thèse : « La gestion des risques psychosociaux à l'épreuve de la loi Informatique et Libertés ? » dans le cadre son Mastère spécialisé en Management et Protection des données à caractère personnel de l'Institut Supérieur d'Electronique de Paris (ISEP) et est considérée aujourd'hui comme une experte de cette problématique spécifique à la protection des données à caractère personnel.

La gestion des risques psychosociaux à l'épreuve de la loi Informatique et Libertés ?

Antoine ANGLADE : Comment en êtes-vous arrivée à vous intéresser à cette problématique croisant la prévention des risques psychosociaux (RPS) et la protection des données à caractère personnel ?

Armande BRU-FRANCOIS : En tant que juriste, le sujet des RPS est très intéressant. Il est un concept récent et encore très mal défini. Le sujet est également intéressant parce qu'il est de plus en plus présent dans l'entreprise, en écho direct au mouvement de fond en faveur de la qualité de vie au travail. Ma formation universitaire et mes appétences professionnelles ont été à l'origine de cette problématique originale qui lie RPS et protection des données à caractères personnelles.

AAN : Pourquoi ce focus particulier sur les RPS plutôt que sur les risques professionnels dans leur globalité ?

ABF : Je vois au moins trois raisons à cela.

Commençons par la plus centrale : l'absence de définition claire de la notion même de RPS. Or comment assurer la conformité d'un traitement dont le concept même n'est pas défini ? La plus grande ambiguïté concerne la finalité même de la prévention demandée à l'employeur : les dispositifs et actions mises en place visent-ils à prévenir les risques (au sens de facteur ou de cause), leurs conséquences ou les deux ? S'agit de prévenir les risques attachés à une personne ou un groupe de personnes physiques, à leurs fonctions

dans l'entreprise ou aux deux ? Je ne crois pas à une évolution plus restrictive de la notion de RPS à court terme de cette situation. Cette acception large de la notion de RPS convient *a priori* au législateur et aux plaignants en laissant beaucoup de souplesse dans l'interprétation des cas et la prise en compte de leur diversité et des éléments de contextes très particuliers qui y sont associés. Aujourd'hui le périmètre d'accord du Ministère du Travail et des syndicats nationaux et internationaux se limite à l'identification de quatre grands facteurs de risques que sont le stress (comme source extérieure), le harcèlement, la violence et la souffrance au travail. Ils constituent les références exclusives aux déterminants pouvant entraîner la survenance du risque (la dépression, le mal-être, le *burn-out*, voire malheureusement dans certains cas extrêmes le suicide).

Ensuite, s'il est vrai que la seule prévention des risques professionnels impliquait déjà une attention particulière en termes de mise en conformité des traitements de données, les RPS entraînent de nouvelles natures et de nouvelles sources de données. Or ces dernières ne bénéficient pas *a fortiori* de référentiels ou de catégorisation établis. Prenons un exemple. Est-ce que le signalement d'un comportement de fatigue chronique relevé sur le lieu de travail constitue implicitement une donnée de santé ? Autrement dit l'employeur doit-il dans ce cas se conformer nécessairement aux exigences accrues en termes de traitement des données sensibles ? Aucun référentiel ne permet aujourd'hui de l'affirmer définitivement. Il en va de même pour la qualification d'informations nominatives relatives au handicap, au ressenti du stress, au sommeil, ou encore faisant état d'une crise de larmes, ou d'un comportement désorienté ?

Ajoutons enfin une différence notable de positionnement entre la CNIL et l'Union Européenne sur la définition d'une donnée de santé. La CNIL en pose une définition assez restrictive alors que l'Europe au contraire défend une acception plus large et englobante. Il y a donc un champ juridique à investiguer et cela constitue une partie de l'intérêt de mon travail de recherche.

AAN : Concrètement quelles sont les actions qui nécessite d'intégrer une démarche de protection des données à caractère personnel ?

ABF : Toutes ! C'est ma déformation professionnelle. *(rires)* Plus sérieusement, qu'il s'agisse des dispositifs de prévention, d'évaluation ou d'alerte, tous doivent passer par le crible des exigences de conformité que sont l'information des salariés concernés, la finalité des traitements dans le double aspect de pertinence et de proportionnalité, le droit à l'oubli, le respect de la confidentialité ainsi que certaines obligations de déclaration préalables.

Rappelons aussi que la notion de traitement est très large. Elle recouvre de nombreux cas de figure, d'une simple collecte d'informations à l'utilisation d'un fichier Excel en passant par une base de données.

Par ailleurs et pour faire face à la difficulté qui consiste à garantir la conformité d'un traitement dont la visée ne peut être définie précisément, une approche par les risques s'avère souvent la meilleure option possible.

AAN : Quelles sont les principales bonnes pratiques à retenir en matière de conformité des traitements de données dans le cadre de la prévention des RPS ?

ABF : Du point de vue de la finalité des traitements d'abord, il semble prioritaire de définir le(s) facteur(s) de risque(s) recherché(s). Ainsi, il sera possible de s'assurer que les données collectées pour l'évaluation ou la mesure d'un risque sont bien proportionnées et non excessives.

Ensuite, le focus doit être porté sur la confidentialité des traitements. Il faut ici veiller à empêcher l'identification du salarié dans les résultats d'une enquête ou l'exploitation d'un traitement. J'attire l'attention des DRH sur l'utilisation des fonctions ou des titres professionnels des salariés. Ceux-ci permettent dans bien des cas qu'il m'a été donné d'étudier d'identifier de façon certaine le salarié. Il convient donc d'utiliser des agrégats de fonction ou des emplois-types plus génériques. C'est aussi le cas de l'identifiant qui est

parfois utilisé afin d'éviter qu'un même salarié réponde plusieurs fois à un questionnaire. Il existe des moyens pour garantir à la fois l'unicité des réponses et la confidentialité du répondant.

Si l'anonymisation des données n'est pas possible ou non pertinente, il faut s'assurer du consentement exprès et non équivoque du salarié ou de la population concernée. En plus, il est essentiel de fiabiliser les circuits d'information et d'empêcher tout accès aux informations nominatives de manière directe ou indirecte au CHSCT ou à des personnes en charge du suivi global des risques professionnels.

Le recours à un prestataire externe s'avère être aussi une bonne pratique à condition de s'assurer de la présence des clauses de sécurité, de confidentialité, de durée de conservation et de destruction dans le contrat liant l'employeur au sous-traitant. Les prestations de soutien psychologique externalisées en sont un exemple, certains contrats prévoient par défaut l'anonymisation des appelants, d'autres non.

Pour terminer par les procédures et les dispositifs de signalement de risques avérés, je conseille d'utiliser des formulaires de déclaration qui limitent autant que faire se peut les champs de saisie libre et par là-même le risque de remontée d'informations non pertinentes ou non proportionnées. La question de l'anonymat du déclarant est sujet à polémique.

D'un côté l'anonymat facilite la remontée de signalement, mais aussi la délation, voire la diffamation. De l'autre côté, une déclaration nominative diminue le risque de délation, mais réduit aussi le courage de prise de parole en cas de harcèlement institutionnalisé dans certaines directions.

AAN : A quel point la multiplication des données et de leurs usages dans l'entreprise, notamment au sein des DRH, constitue-t-elle en elle-même un facteur de risques psychosociaux ?

ABF : C'est une extension intéressante de la problématique initiale. Les données collectées, notamment dans un système d'information RH sont de plus en plus nombreuses et diverses. Les déclarations simplifiées de type 46 pour la gestion du personnel ou 42 pour la gestion des contrôles d'accès couvrent de moins en moins cette diversité. Pensez par exemple au caractère personnel des publications d'un salarié sur la plateforme sociale, collaborative ou d'innovation participative de son entreprise ou autre exemple, à sa réponse à un baromètre social du type "Quelle est votre humeur aujourd'hui ?". Ce type de contribution au patrimoine informationnel de l'entreprise expose le salarié. Dans un environnement où ce dernier ne se sent pas en confiance, voire forcé à contribuer par le biais de certains procédés d'émulation collective et de gamification (*Dispositifs managériaux s'appuyant sur les leviers du jeu collecte de points ou de badges, progression par niveau, défis, utilisation d'avatars, etc*.) pour motiver un individu ou une équipe à réaliser des actions pour l'entreprise, l'étape de collecte de données peut constituer un facteur de stress professionnel.

Il en va de même pour les systèmes de notation, d'évaluation, de *ranking* ainsi que pour les systèmes de recommandations interpersonnelles ou de profilage psychologique. Dans chacun de ces cas, le salarié se voit "réduit" à un modèle et un ensemble de données à caractère personnel qui le définit dans le système d'information. Ici, la finalité des traitements associés à ces données est cruciale. Celle-ci doit être clairement définie et communiquée aux différentes parties prenantes, dont les salariés. Il en va différemment d'une finalité qui viserait à améliorer les parcours de développement professionnel sur la base des acquis et du potentiel individuel de chacun, d'une autre finalité qui servirait à alimenter des critères en vue d'identifier la population concernée par un licenciement collectif. Evidemment, la seconde orientation est anxiogène et constitue une source de RPS. Ces discussions ne manquent d'ailleurs jamais de survenir lors de la négociation d'un accord de gestion prévisionnelle des emplois et des compétences.

Enfin, le développement croissant et la diffusion d'objets connectés est une autre source

en devenir de données à caractère personnel dans l'entreprise. Ceux-ci se proposent de collecter des données biométriques. En l'espèce, la conformité aux exigences en matière de protection des données personnelles constitue autant une nécessité qu'un moyen de convaincre les salariés et leurs instances représentatives du bien fondé d'une telle action. Pour aller plus loin, une approche de type *Privacy by Design* me paraît tout à fait recommandée ici afin de rassurer et protéger les parties prenantes et par là même réduire les RPS qui y seraient associables.

AAN : Pour conclure, comment relieriez-vous la création récente du statut de lanceur d'alerte avec votre sujet ?

ABF : La délibération de la CNIL du 30 janvier 2014 constitue en effet un sujet connexe à notre problématique. L'une des principales nouveautés de la délibération concerne l'élargissement du périmètre d'action du lanceur d'alerte au domaine de la santé, de l'hygiène et de la sécurité au travail. Ainsi, le signalement d'un cas de harcèlement ou de violence dans l'entreprise entre sous la protection de la nouvelle délibération.

En soi, cela semble être une avancée. La seule interrogation qui est mienne concerne la question de l'anonymat.

En effet, l'étude terrain des pratiques de plusieurs entreprises dans le cadre de ma thèse m'oriente vers des dispositifs de signalement dans lesquels le lanceur d'alerte est bien évidemment protégé par l'exigence de confidentialité, mais dans le même temps clairement identifié. D'abord parce que ce lanceur constitue la plupart du temps une ressource clés dans l'instruction et la résolution du cas signalé.

Ensuite parce que force est de constater que sous couvert d'anonymat, les dénonciations à caractère délateur ou infamant sont plus fréquentes.

En conclusion : comment anticiper le règlement général sur la protection des données

Il est possible de voir cette nouvelle règlementation comme une évolution ou une continuité de la directive 95/46/CE. Les entreprises qui respectent les bonnes pratiques informatiques ou les normes type PCI DSS, ISO 27001, PSSI, PCA, et qui sont déjà en conformité avec les lois nationales, ne devraient pas avoir de difficultés à appréhender ce virage en remaniant leurs processus internes. En revanche, pour les autres, la conformité risque d'être un vrai défi.

Pour se lancer dans ce projet, voici les différents domaines auxquels vous devriez consacrer dans un premier temps votre attention et vos ressources :

- Effectuer une analyse de votre situation déclarative et évaluer votre position de conformité par rapport aux exigences du label de gouvernance Informatique et Libertés.
- Désigner un Data Protection Officer.
- Cartographier (identification et classification) vos données au sein du SI. Il est important d'identifier où les données à caractère personnel sont gérées, stockées au sein de votre SI, que ce soit dans les formats non structurés des feuilles de calcul ou au sein des applications.

De plus, compte tenu des exigences de limitation de rétention des données, il est important de tracer les informations sur les dates de collecte, les raisons du recueil des données et leur finalité.

- Réaliser un audit des mentions légales et de vos clauses contractuelles clients et fournisseurs.
- Mettre en place une gouvernance des données.
- Mettre en place, pour les entités internationales, les mécanismes encadrant les transferts de données personnelles par le biais BCR, les Binding Corporates Rules.
- Mettre en place des mécanismes de supervision.

Dans un système idéal, cette supervision permet d'automatiser les purges en fonction des durées de conservation qui ont été définies. Le principe de notification de violation impose aussi aux équipes informatiques de superviser le SI afin de détecter les accès inhabituels aux fichiers et applications contenant des données personnelles. Cette supervision doit permettre de signaler promptement toute exposition à l'autorité de données locale afin d'éviter les nouvelles amendes. Pour l'heure, nous vous proposons de nous focaliser sur les deux premières étapes, les autres aspects seront abordés dans un prochain livre blanc.

Notre démarche d'état des lieux

La conformité avec le règlement général sur la protection des données, implique de nombreux chantiers et l'investissement de plusieurs acteurs.
En effet le Data Protection Officer, une fois désigné, devra être en relation avec :

- les juristes pour assurer la couverture des mentions légales et les relations contractuelles ;
- les ressources humaines pour organiser les sensibilisations et les formations ;
- le département sécurité et risque pour le suivi de la PSSI, la gestion de crise, etc. ;
- la direction des systèmes d'information afin d'être intégré en amont dans l'ensemble des projets en adaptant les processus projets, la mise en place de dispositifs techniques et de mesures organisationnelles pour assurer la conformité de l'ensemble des projets.

Il est facile de « s'y perdre ». Nous recommandons de faire un état des lieux des pratiques actuelles pour définir un plan d'actions qui vous soit propre. Ces chantiers doivent être ensuite priorisés de sorte que les problématiques de risques critiques et les principaux objectifs d'activité soient pris en compte avant d'autres éléments de moindre importance.

Notre démarche d'état des lieux consiste à effectuer :

- Une analyse de la situation déclarative des traitements.
- Une évaluation de sécurité des données à caractère personnel.
- Une analyse de l'adéquation des formalités effectuées.
- Une étude des processus déclaratifs et de contrôle de l'entreprise.
- Et diminuer le niveau d'exposition.

Le label de gouvernance informatique et libertés (et présentation d'adequacy 2018)

La CNIL a adopté le 11 décembre 2014 un nouveau référentiel pour les procédures de gouvernance. Face au besoin grandissant des entreprises et organismes publics d'identifier clairement les procédures à mettre en place pour une bonne gestion des données personnelles, la CNIL a décidé d'élaborer un nouveau référentiel : le label « gouvernance informatique et libertés ». La gouvernance « Informatique et Libertés », définit les règles et les bonnes pratiques permettant à un organisme d'assurer une gestion de ses données respectueuse des principes Informatique et Libertés**.**
Le CIL, ou le futur DPO, peut aussi utiliser ce référentiel comme mode d'emploi ou guide des procédures à suivre et se fixer comme objectif l'obtention du label pour son organisme**.**

En pratique, les 25 exigences de ce nouveau référentiel sont organisées en trois thématiques qui concernent :

- L'organisation interne liée à la protection des données.
- La méthode de vérification de la conformité des traitements à la loi Informatique et Libertés.
- La gestion des réclamations et incidents.

Véritable outil de responsabilisation des organismes traitant des données personnelles, le label est un indicateur de confiance pour les clients ou les usagers**.** Il constitue, pour les entreprises, collectivités, associations ou administrations, un cadre éthique et juridique adapté, témoignant de la volonté de l'organisme d'innover et de traiter les données personnelles de manière responsable. Enfin, cette démarche permet de les préparer au règlement européen, en intégrant notamment le principe d'accountability.
En plus de sa mission d'accompagnement de cette mutation, le cabinet Infhotep dans le cadre ses projets de recherche et développement, a mis en ligne une plateforme d'autoévaluation de la situation d'un organisme par rapport aux exigences de la PSSI de l'état et au label de gouvernance Informatique et Libertés. La plateforme Adequacy 2018 permet à chaque organisme d'évaluer sa conformité avec l'ensemble des exigences et des attentes règlementaires auxquelles il devra répondre en 2018.

Pour en savoir plus adequacy208.infhotep.com