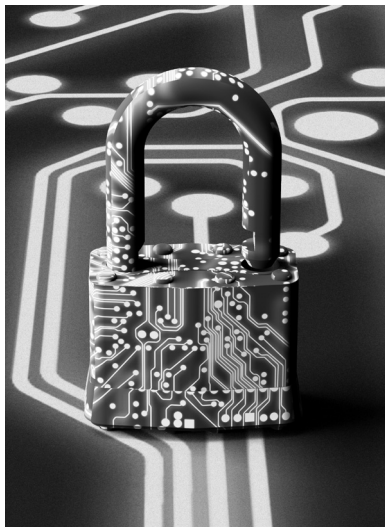
La sécurité des données



En obligeant les entreprises à déclarer toute violation de données à caractère personnel aux autorités de contrôle et à notifier la violation aux personnes concernées, le RGPD incite fortement les organismes à mettre en place une solide politique de sécurité de leurs systèmes d'information ainsi que de protection de leurs données sensibles.

CHRISTOPHE BOUTONNET
Ancien directeur des systèmes d'information du Conseil d'Etat

I. LE CONTEXTE GÉNÉRAL

La mise en œuvre du Règlement relatif à la protection des données à caractère personnel (ci-après « RGPD »)[1], à partir du 25 mai 2018, intervient dans un contexte d'évolution de plus en plus rapide des technologies de l'information. Après la révolution bureautique, la révolution Internet et celle des réseaux sociaux, les entreprises investissent désormais dans plusieurs domaines qui touchent aux données en général et aux données personnelles en particulier[2] :

– intelligence artificielle et traitement de très gros volumes de données ;

– Internet des objets ;

– mobilité et généralisation de l'informatique « ubiquitaire ».

Cette omniprésence de l'informatique comme formidable levier de modernisation, mais aussi pierre angulaire des business models des entreprises et institutions, est aussi de nature à fragiliser leur édifice, les obligeant à revoir continuellement leur politique de sécurité.

La mise en œuvre du RGPD vient amplifier, dans un sens ou dans l'autre, les forces et les faiblesses du système d'information (SI) au regard de la donnée personnelle. Contrairement à la directive 95/46/CE qu'il remplace, le RGPD ne nécessite pas, par nature, sa transposition dans les lois nationales des pays membres et sera contraignant dès sa date d'application.

Alors que la directive européenne de 1995 reposait sur une logique déclarative, le RGPD répond à une logique de conformité dont la responsabilité incombe au « *responsable des traitements* », sous le contrôle et l'accompagnement de l'autorité administrative. De plus, les sanctions encourues en cas de non-respect sont particulièrement lourdes : elles pourront s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires.

Cet article présente les principaux niveaux de risques et quelques recommandations pratiques indispensables, permettant de transformer le risque en opportunité de création de valeur tout en respectant le droit à la vie privée des clients, des usagers ou des employés, en faisant de l'économie des données personnelles un business éthique.

II. LA VALEUR MARCHANDE D'UNE DONNÉE À CARACTÈRE PERSONNEL, SOURCE DE NOMBREUSES CONVOITISES

Actif stratégique de l'entreprise, la donnée personnelle traitée est devenue source de convoitise avec un prix de marché qui se monnaye au prix fort. Si les données nues ont peu de valeur, c'est le résultat de leur traitement qui leur en fait prendre. Pour donner un exemple[3], on peut prendre la capitalisation de Facebook et diviser par le nombre d'abonnés, ce qui correspond environ à 40 dollars par personne.

On peut aussi estimer cette valeur en calculant le manque à gagner quand les données disparaissent, à la suite d'un piratage ou d'un accident. C'est ce qui est arrivé à Target aux États-Unis où les données de 110 millions de personnes ont été volées. Le calcul montre que ces données valent 1,18 dollar par personne. Chez les Data Brokers, une profession interdite en France, il y a un début de Bourse des données : aux États-Unis, une adresse vaut 50 *cents*, une date de naissance 2 dollars, un numéro de sécurité sociale 8 dollars, un livret militaire (*military record*) 35 dollars. Inversement, on peut estimer la valeur de ses données personnelles en calculant combien coûte leur non-divulgation : une *start-up* californienne, Protect my ID, propose une protection moyennant un abonnement de 15,95 dollars par mois.

Au-delà de l'attrait pour la donnée personnelle et à sa valeur d'échange, les risques « classiques » de sécurité des SI ne doivent pas être écartés car

1. Règlement 2016/679 du 4 mai 2016 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.
2. Symposium 2016 du Gartner Group à Barcelone : IT 2020.
3. Selon Mouloud Dey, directeur Solutions et marches émergents chez SAS, d'après un article de la revue *Challenges*.

ils peuvent toucher indirectement à la donnée personnelle. Par exemple une attaque par déni de service[4] bloquant l'accès au SI bloque également l'accès à l'information personnelle. En effet, c'est le maillon le plus fragile de la chaîne qui compte quand il s'agit d'évaluer la fragilité d'un dispositif.

III. LES DONNÉES PERSONNELLES INTERNES À L'ENTREPRISE

En se focalisant sur la protection des données de ses clients, on a tendance à oublier ses propres employés et la nécessité de protéger la base de données du SI RH, bien souvent le premier référentiel de données à caractère personnel (ci-après « DCP ») d'une entreprise.

Parallèlement aux activités de *reporting* et de contrôle de gestion social se sont développées des activités de *marketing* RH et de gestion des connaissances, qui méritent une vigilance particulière en matière de protection des données.

La concurrence sur le marché des talents, d'une part, et la recherche d'information sur l'organisation précise d'une entreprise et les personnes clés, d'autre part, attirent bien des convoitises, soit pour bénéficier d'un avantage concurrentiel déloyal, soit pour faire pression sur les bonnes personnes, soit pour réaliser illégalement des opérations en leur nom.

IV. LES OPÉRATEURS D'IMPORTANCE VITALE ET LA CYBERGUERRE

Selon l'agence nationale de sécurité des SI[5], plus de 200 opérateurs publics ou privés dont les activités sont indispensables au bon fonctionnement et à la survie de la Nation ont été recensés, une liste gardée confidentielle pour des questions de sécurité nationale. Les opérateurs d'importance vitale (OIV) et leurs activités sont définis par le code de la défense[6].

Plus précisément, un OIV gère ou utilise un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou de mettre gravement en cause la santé ou la vie de la population. Il a l'obligation de notifier à l'ANSSI tout incident de sécurité sur son SI[7]. Il convient de rappeler que le secteur bancaire, en ce qui concerne les moyens de paiement, fait partie des OIV.

Au-delà des OIV, les attaques visant les intérêts d'un pays prennent actuellement un éclairage particulièrement marqué, notamment à la suite des élections présidentielles américaines. Les récentes déclarations du Président Obama visant la Russie confirment la nécessité de protéger plus particulièrement les entreprises et organismes sensibles. Pour mémoire, des dizaines de milliers de messages de responsables démocrates et du président de l'équipe de campagne d'Hillary Clinton, John Podesta, ont été dérobés puis mis en ligne en 2016, notamment dans le dernier mois avant le scrutin, jetant une lumière crue sur les délibérations internes du camp Clinton et brouillant le message de la candidate.

Sans aller encore jusqu'à parler de cyberguerre, on s'en approche cependant davantage. On se souvient par exemple de l'attaque Stuxnet attribuée aux États-Unis et à Israël contre les installations nucléaires iraniennes en 2010. Les hackers se sont infiltrés dans les ordinateurs qui contrôlaient la vitesse de rotation d'une centrifugeuse d'uranium, l'ont fait aller plus vite, jusqu'à provoquer des pannes et des explosions.

V. LES RISQUES

L'usine Digitale, dans un article du 24 mai 2016, identifie cinq nouvelles menaces qui visent tout particulièrement les entreprises parmi toutes celles identifiables. La plupart d'entre elles touchent directement les données à caractère personnel. Cependant, se limiter aux menaces sur la protection des données personnelles serait réducteur de l'ensemble des risques encourus.

En effet, les risques liés à la sécurité sont de plusieurs natures. Ils peuvent ainsi concerner :
– de vraies attaques, qu'elles touchent directement ou indirectement les données personnelles : – déni de service, *fishing*, intrusion dans le SI à travers une faille de sécurité ;
– l'usage et l'exploitation abusive des données personnelles (usage du *data mining*) ;
– le niveau de confiance qu'attache un usager à l'exploitation des données personnelles qu'en fait l'entreprise ;
– la fragilité du dispositif de ses partenaires ou de ses sous-traitants. Il ne faut pas oublier que le risque doit être évalué sur l'ensemble de la chaîne et pas seulement sur son propre SI.

1. Les risques directs

1.1. Les *ransomwares*

Un *ransomware*, rançongiciel ou logiciel de rançon est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, il chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Un *ransomware* peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent. Un rançongiciel se propage typiquement de la même manière qu'un cheval de Troie (en anglais *Trojan Horse*) : il pénètre le système par exemple via des logiciels malveillants ou à travers des campagnes d'e-mails malicieux. Il exécute ensuite une charge active[8]

4. Une attaque par déni de service (en anglais, *denial of service attack* [DoS] ou *distributed denial of service attack* [DDoS]) est une attaque informatique ayant pour but de rendre indisponible un service en empêchant ses utilisateurs légitimes de l'utiliser.
5. Site de l'ANSSI : https ://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/.
6. Voir plus particulièrement les articles L. 1332-1, L. 1332-2, R. 1332-1 et R. 1332-2.
7. Article 22 de la loi de programmation militaire du 18 décembre 2013.
8. Désigne la partie du code exécutable d'un virus qui est spécifiquement destinée à nuire (par opposition au code utilisé par le virus pour se répliquer notamment).

(*payload*), par exemple un exécutable qui va chiffrer les fichiers de l'utilisateur sur son disque dur.

Parmi les nombreux exemples rencontrés, deux ont particulièrement attiré l'attention des médias.

Le premier a touché le métro et les bus de San Francisco (novembre 2016) : les distributeurs de tickets de métro, tram et bus de San Francisco ont été bloqués, rendant les transports gratuits pendant 24 heures. Une rançon de 73 000 *bitcoins*, soit l'équivalent de 50 millions d'euros, a été réclamée pour un retour à la normale.

Le deuxième a touché un hôpital américain, victime d'un piratage des données de ses patients (février 2016) : le Hollywood Presbytarian Medical Center avait été paralysé pendant une semaine. L'établissement avait dû verser une rançon de 17 000 dollars pour assurer la récupération de données particulièrement sensibles, dont les fiches d'admission ou les fichiers médicaux d'environ 900 patients.

1.2. Le vol massif de données personnelles

Si le *cloud* et le *Big Data* constituent indéniablement une très grande opportunité pour les entreprises, ils attirent également la convoitise des criminels, qui organisent le vol, l'exploitation et la revente de quantités importantes de données. C'est ce qui est par exemple arrivé à Yahoo et à LinkedIn, mais aussi plus près de chez nous à Orange.

Les informations de 167 millions de comptes LinkedIn ont ainsi été mises en vente en ligne pour la somme de 5 *bitcoins* (environ 2 000 euros). Sur l'ensemble de ces comptes, 117 millions comporteraient des identifiants de connexion complets (*e-mail* et mot de passe). Dans un email envoyé aux utilisateurs, LinkedIn indique que les données proviennent d'une fuite datant de 2012 dont l'entreprise pensait jusqu'ici qu'elle n'avait touché que 6,5 millions de comptes.

De même, Yahoo ! a confirmé le 22 septembre dernier que 500 millions de comptes de ses utilisateurs ont été piratés en 2014, par un « *nation-state actor* », soit une entité liée à un État. Il a précisé par la suite avoir été victime en 2013 d'une cyberattaque encore plus importante, touchant plus d'un milliard de comptes [9].

1.3. Le piratage mobile

Les *smartphones* sont à présent massivement utilisés comme outil informatique standard, ayant maintenant dépassé en usage les ordinateurs classiques. Ils sont par conséquent devenus la cible de nombreuses attaques. Ils regorgent souvent d'informations sensibles et personnelles et attirent tout naturellement les criminels, d'autant qu'ils peuvent servir de tremplin pour pénétrer d'autres systèmes. Ils sont souvent vulnérables au travers de bugs et d'une absence de mises à jour.

Ainsi, un groupe de hackers composé d'adolescents est parvenu à prendre le contrôle des appels du directeur du renseignement national des États-Unis. Il s'était déjà fait connaître en piratant le compte *e-mail* du directeur de la CIA. Les hackers avaient par la suite pénétré une série de sites et services *web* gouvernementaux et s'étaient emparés de milliers d'informations sensibles. Ils ont notamment publié des informations détaillées sur plus de 2000 fonctionnaires à des postes clés [10].

2. Les risques indirects

Même si certains risques ne visent pas directement les données personnelles, leur importance est de nature à fragiliser le SI au point d'empêcher leur accès voire permettre leur piratage.

2.1. Le déni de service

L'attaque par déni de service est l'une des plus connues. Elle a pour objectif de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser, le plus souvent en surchargeant un serveur de requêtes jusqu'à ce qu'il ne puisse plus y répondre. Pour y parvenir, les criminels infectent préalablement un grand nombre de machines connectées à Internet et mal protégées : des ordinateurs personnels mais aussi des serveurs ou même des objets connectés. Les motivations de ces attaques varient, mais leur conséquence peut être sévère pour les sites marchands ou toute entreprise pour laquelle le *web* est essentiel.

Par exemple, une attaque en déni de service distribué menée contre l'infrastructure managée de DNS [11] du fournisseur DYN, à partir de centaines de milliers d'équipements connectés à Internet, a interrompu le 21 octobre dernier pendant plusieurs heures l'accès à des services comme Twitter, Spotify ou Airbnb. L'attaque a également engendré des problèmes sur l'accès à des sites web en France.

2.2. Les objets connectés (IoT) de l'entreprise sont encore bien loin d'être complètement sécurisées.

Les objets connectés sont de plus en plus présents en entreprise et intègrent désormais le SI. Ils n'embarquent pas toujours la puissance de calcul nécessaire à leur sécurisation et, de ce fait, constituent une source importante de risques.

Ainsi l'attaque de déni de service citée plus haut concernant la société DYN a utilisé majoritairement des objets connectés (caméras de surveillance IP, routeurs Wi-Fi).

Comme dans de nombreux autres secteurs, les objets connectés entrent aussi de plain-pied dans le monde de l'assurance ou de la banque, cette fois-ci comme un service offert aux clients. Ainsi, MasterCard s'est lancé dans un partenariat avec une start-up qui a mis au point un bracelet connecté identifiant l'utilisateur par son rythme cardiaque. L'objectif serait de sécuriser les paiements grâce à ce nouveau moyen d'authentification.

Ce type d'innovation impose de rassurer le consommateur sur le niveau de protection de son identité et de ses données. Une grande partie des clients restent, par exemple, réticents aux technologies NFC (*Near Field Communication*). Seuls 15 % des Français utilisaient en janvier 2015 leur carte NFC [12], pour autant que leur organisme financier leur en donne la possibilité.

9. http://www.generation-nt.com/yahoo-piratage-milliard-comptes-donnees-actualite-1936998.html.

10. Article de Julien Bergounhoux publié dans *L'Usine digitale* du 14 janvier 2016.

11. Le *Domain Name System* (ou DNS, système de noms de domaine) est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP, identifiant par exemple un serveur internet.

12. Sondage réalisé en janvier 2015 par Syntec numérique, en partenariat avec l'institut Odoxa.

PANORAMA DES MENACES LES PLUS RECENSÉES

3. Les risques de sanctions au regard du RGPD

Le RGPD oblige les entreprises à déclarer toute violation de données à caractère personnel aux autorités de contrôle. Ainsi, l'article 33 du règlement impose que les responsables du traitement informent dans les meilleurs délais 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, sauf dans certaines conditions[13].

Tout manquement dans la gestion et la protection des données personnelles expose une entreprise ou un organisme à des contentieux, une altération de son image et à des pénalités financières importantes, qui peuvent se traduire 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.

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'affaires mondial annuel si cette seconde valeur est supérieure. Par ailleurs, le risque financier se superpose à un risque pénal : le fait de ne pas procéder à la notification d'une violation de données à caractère personnel auprès de la CNIL[14] ou auprès de l'intéressé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende[15].

C'est dire l'intérêt financier à renforcer la sécurité de ses SI et protéger l'accès aux données personnelles.

13. Article 4.3 du RGPD.

14. Condition nécessaire mais non suffisante : par exemple, la décision n° 385019 du Conseil d'État lue le 30 décembre 2015 explique pourquoi le fait de notifier une faille ne suffit pas pour échapper à une sanction ultérieure par la CNIL, la responsabilité du responsable du traitement restant engagée quand la faille vient d'un sous-traitant.

15. Art. 226-17-1 du Code pénal.

VI. QUELQUES RECOMMANDATIONS

L'application du règlement européen nécessite, pour être appliquée, la mise en place de dispositions structurantes en termes de gouvernance et de réalisations techniques.

1. Renforcer la protection de ses infrastructures

La protection technique des infrastructures et des données face aux risques décrits plus haut nécessite la mise en place d'un certain nombre de stratégies, dont certaines sont frappées au coin du bon sens. En voici quelques-unes, notamment pour se protéger contre les *ransomwares* :

– au niveau du réseau, il convient d'empêcher toute infection par *ransomware* au niveau des passerelles réseau et de messagerie. Cela passe par une segmentation du réseau d'entreprise en différentes zones de sécurité ;

– il faut mettre en place une stratégie de sauvegarde et de restauration très régulière, afin de pouvoir très rapidement déclencher un plan de reprise d'activité (PRA) ;

– on utilisera ensuite des outils de sécurité de messagerie et Internet, qui contiennent une fonction d'analyse, notamment des pièces jointes ;

– les systèmes d'exploitation et logiciels doivent être régulièrement mis à jour afin de combler rapidement les failles de sécurité exploitées par les logiciels malveillants ;

– il apparaît nécessaire d'établir une liste des applications autorisées au téléchargement, afin de se prémunir contre les fausses applications ;

– face aux vulnérabilités des mobiles, il convient bien sûr de mettre à jour systématiquement les applications embarquées mais également de se munir de protections spécifiques aux mobiles, capable d'identifier et de signaler tout comportement d'applications dangereuses et malveillantes ;

– pour prévenir les fuites de données à partir d'appareils mobiles, il est nécessaire de contrôler le flux de données entrant et sortant. En les « conteneurisant » et en mettant en place des *workflows* partagés, on peut garder ces données à l'intérieur du périmètre de l'entreprise. Il devient alors possible d'effacer à distance n'importe quelle donnée professionnelle ainsi isolée, lorsque la situation l'exige, comme dans le cas où un appareil serait perdu ou volé, ou suite au départ d'un employé ;

– enfin, la gestion des terminaux mobiles (MDM) doit être renforcée par une approche de « conteneurisation » s'appuyant sur un chiffrement applicatif et indépendant du terminal.

2. Gestion du patrimoine de données

La gestion des données consiste à les définir, les stocker, les maintenir, les distribuer et imposer une vue complète, fiable et à jour de celles-ci au sein d'un SI, indépendamment des canaux de communications, du secteur d'activité ou des subdivisions métiers ou géographiques.

Plus particulièrement, la gestion des données de référence ou gestion des données maîtres (GDR, plus connue sous le vocable anglais de *Master Data Management* ou MDM) mérite une attention particulière car elles constituent la pierre angulaire de nos SI et souvent l'un des points de fragilité. En effet, les systèmes informatiques des organisations, utilisés par différentes fonctions métier (*marketing*, fonction commerciale, recherche et développement…) vont nécessairement partager des données de référence (les produits, les clients ou les fournisseurs, le *reporting* financier pour les comptes consolidés, etc.). Il est donc crucial pour une organisation d'utiliser ces données référentielles d'une façon cohérente à travers chacun de ses systèmes.

La gestion du patrimoine des données est composée de plusieurs étapes[16].

2.1. Étape 1 : Référencement des données

Il consiste à identifier les données et leurs propriétaires/responsables ainsi que leur rôle dans les applications informatiques.

2.2. Étape 2 : Niveau de sécurité attendu

L'évaluation du niveau de sécurité attendu pour chaque donnée est réalisée au moyen des quatre critères :

– **disponibilité** : la disponibilité est la propriété d'une donnée ou d'un processus d'être accessible à la demande, en temps et en heure ;

– **confidentialité** : la confidentialité est la propriété d'une donnée ou d'un processus de n'être accessible qu'aux utilisateurs autorisés. De la confidentialité découle la capacité à tracer l'accès aux données ;

– **intégrité** : l'intégrité est la propriété d'exactitude et de complétude d'une donnée ou d'un processus ;

– **date de péremption des données** : pour chaque donnée collectée, il s'agira de déterminer une date de péremption afin d'en connaître sa durée de vie avant archivage.

3. La bonne gouvernance des données personnelles

Afin d'assurer une bonne gouvernance des données personnelles, il convient d'être attentif à de nombreux processus de l'entreprise ayant recours ou étant susceptibles de recourir à des bases de données sensibles et/ou personnelles. La désignation d'un responsable des données (*data owner*), comme le suggère le rapport CIGREF « Enjeux *business* des données » (2014), est essentiel. Il convient tout d'abord d'assurer l'intégrité et les qualités des données dès leur source. Un travail sur les métriques permet d'assurer de manière constante le niveau de qualité exigé. Dès que les données personnelles sont classifiées (selon les catégories définies par la CNIL) et que les autorisations sont accordées pour des besoins métiers ou des projets de recherche et développement[17], il convient d'assurer un travail de monitoring permanent. Le travail de cartographie des données, tenant compte de la complexité des SI, est également essentiel pour avoir une vision d'ensemble du cycle de vie des données personnelles dans l'entreprise (leur provenance, leur partage avec des tiers ou en interne,

16. Pour une analyse plus détaillée, on pourra utilement se référer au rapport du CIGREF : « Valorisation des données dans les grandes entreprises » (octobre 2016).

17. Les autorisations de CNIL sont appelées à disparaître avec le RGPD, sauf nécessité de recourir à une analyse d'impact prévue aux articles 35 et 36 du RGPD s'agissant des traitements comportant des risques particuliers pour les personnes (*scoring*, données sensibles, vidéosurveillance, données génétiques ou biométriques, usage de nouvelles technologies).

leur stockage, leur usage, leur traitement et leur suppression).

La mise en œuvre doit pouvoir s'appuyer sur des propriétaires désignés des données et des traitements associés. Ceux-ci sont identifiés et désignés lors de la première étape et portent pour ce qui concerne leur périmètre la deuxième étape. Ils sont chargés de tenir à jour la liste des utilisateurs et de leurs droits d'accès. Pour ce qui concerne les données à caractère personnel, ils sont les interlocuteurs du délégué à la protection des données.

4. Rapprocher le délégué à la protection des données (DPD[18]) et le RSSI

Le règlement européen fait du délégué à la protection des données un acteur essentiel et incontournable du dispositif. Il devra accompagner l'entreprise ou l'institution qui l'a désigné pour vérifier l'application des nouveaux principes, et plus particulièrement la déclinaison de l'*accountability*, l'application du droit à la portabilité ou à l'oubli, l'obligation de notifier toute violation de données à caractère personnel aux instances de contrôle ainsi qu'aux personnes concernées.

Pour cela, le DPO devra s'appuyer sur le RSSI, chargé de définir et de s'assurer de la mise en œuvre de la politique de sécurité. Celui-ci sera particulièrement sollicité pour documenter les démarches de protection, afin d'assurer un suivi de la traçabilité des données personnelles et une véritable transparence vis-à-vis de la réglementation.

Compte tenu du caractère stratégique et sensible du traitement des données personnelles, ces deux fonctions constituent tout naturellement un maillon essentiel du dispositif de gouvernance. Elles doivent donc pouvoir tout naturellement rendre compte en tant que de besoin directement au comité exécutif, afin de raccourcir la chaîne de décision. C'est d'ailleurs l'une des conclusions des Assises de la sécurité 2016, qui réunit chaque année à Monaco les principaux décideurs européens en matière de sécurité des SI. C'est également une demande de l'article 38-3 du RGPD[19].

5. Appliquer l'*accountability* : *security by design* et *privacy by design*

L'*accountability* impose une gouvernance renforcée du cycle de vie des produits et services et des données personnelles qui y sont associées[20]. Il est donc à la fois l'affirmation de la responsabilité de l'entreprise ou de l'institution mais aussi, et surtout, il permet d'évaluer sa capacité à démontrer qu'elle a bien respecté les exigences réglementaires en matière de protection des données.

Cette bonne gouvernance conduit à penser conjointement « *security by design* » et « *privacy by design* ».

La *privacy by design* fait partie des principes fondateurs du RGPD[21] : il s'agit d'intégrer le respect du cadre réglementaire dès la création et tout au long de la chaîne d'un service/produit reposant sur un traitement de données personnelles. Les moyens de consentement des personnes doivent par exemple être prévus dès le départ.

Il existe diverses formes de « gestion » de la « *privacy* » dans la gouvernance des données[22] :

– par les risques (sécurité des systèmes, des méthodes) ;

– par l'éthique[23] (règles internes, culture, responsabilisation) ;

– par la technologie (évaluer leurs potentialités et leurs impacts sur la vie privée en réalisant des EIVP[24]).

Les principes de la « *security by design* » sont définis dans le Livre Blanc « *Privacy and Security by Design : An Entreprise Architecture Approach* »[25], coréalisé par Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario, et Mark Dixon, architecte d'entreprise chez Oracle.

Comme pour les rôles respectifs de DPO et de RSSI, les enjeux de « *privacy* » et de sécurité sont inséparables. Il serait inapproprié de parler de « *privacy by design* » si, d'ores et déjà, les enjeux de sécurité ne sont pas pris en compte dans l'architecture des SI.

Ces dispositions ne sont pas seulement prises pour assurer la protection des *assets* des entreprises, elles sont aussi des « *facilitateurs de business* ». L'entreprise peut avoir des objectifs métiers améliorés, que ce soit avec ses partenaires commerciaux, ses fournisseurs ou ses clients, par le simple fait de garantir la mise en place de plates-formes sécurisées et d'assurer le respect des trois fondamentaux de la sécurité de l'information qui sont l'intégrité (veiller à l'authenticité de l'information et se prémunir des risques de modification ou de destruction), la confidentialité (les données ne sont accessibles qu'aux personnes autorisées) et la disponibilité (assurant un accès rapide et fiable aux informations mises à disposition dans les SI). Toute réflexion sur l'architecture de sécurité doit se construire à partir d'une analyse des besoins métiers. Cela permet en effet de définir plus rapidement les priorités et les actifs à protéger en fonction des objectifs business.

Il existe des outils logiciels et matériels permettant d'intégrer et de contrôler l'intégration des prérequis de sécurité dans la conception d'application. On trouve en particulier des solutions logicielles d'analyse du code d'une application pour vérifier sa conformité[26].

6. Privilégier l'autoformation en continu

Face à des menaces sur la sécurité qui touchent au comportement des

18. Ou *Data Protection Officer* (DPO) dans la version anglaise du RGPD.

19. « *Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant* ». Cf., dans ce hors-série, la contribution de Bénédicte Fauvarque-Cosson et Emmanuel Jouffin consacrée au DPD.

20. Sur cette notion, cf. G 29 opinion 3/2010 *on the principle of accountability* du 13 juillet 2010.

21. Cf. art. 24-1 du RGPD.

22. Rapport du CIGREF sur l'« Économie des données personnelles : les enjeux d'un business éthique » (octobre 2015).

23. Sur cette question, cf. notamment CIGREF rapport « Ethique et Numérique, enjeux et recommandations à l'intention des entreprises ».

24. EIVP : Étude d'impact sur la vie privée, cf. *supra*. Et la méthodologie préconisée par la CNIL : https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-BonnesPratiques.pdf.

25. https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf.

26. À titre d'exemple, présentation aux Assises de la sécurité 2016 de la société Checkmarx au cours de l'atelier « Intégrer la sécurité dans le cycle de développement des applications ».

personnels de l'entreprise, les actions de sensibilisation pour protéger les données sont bien sûr essentielles. Selon Deloitte, elles représentent 50 % des actions entreprises par les organisations[27]. Cependant, l'efficacité de sessions de formation classiques montre ses limites car l'utilisateur finit par commettre à nouveau ses erreurs initiales, au bout d'un temps relativement court après la formation, oubliant les recommandations formulées. C'est pourquoi il convient de privilégier l'usage des outils permettant d'organiser des tests aléatoires réguliers en conditions réelles, comme par exemple des messages d'alerte sur les applications sensibles ou l'usage de logiciels de faux *phishing*.

Lors d'une campagne de sensibilisation, ces derniers outils sont utilisés, sans prévenir nécessairement l'utilisateur, pour envoyer de façon aléatoire des messages d'hameçonnage comprenant une pièce jointe. L'outil analyse le comportement de l'utilisateur et prévient celui-ci en cas de manipulation inappropriée (consistant par exemple à ouvrir la pièce jointe). À la place de l'action déclenchée par un vrai message d'hameçonnage, l'outil prévient l'utilisateur que son action n'était pas appropriée et lui montre ce qu'il aurait fallu faire.

7. Anonymiser les données personnelles

La mise à disposition des données personnelles dans une logique d'analyse et d'exploitation statistique ou d'*open-data* peut nécessiter de recourir à l'anonymisation. Il existe des méthodes qui permettent de rendre les données cohérentes, statistiquement significatives, sans être nécessairement nominatives. Pour aider à évaluer une bonne solution d'anonymisation, le G29 définit trois critères qui déterminent les risques de ré-identification :

– **l'individualisation** : est-il toujours possible d'isoler un individu ?

– **la corrélation** : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?

– **l'inférence** : peut-on déduire de l'information sur un individu ?

En France, la CNIL a travaillé par exemple avec de nombreux acteurs autour du Pass Navigo, des compteurs Linky, des téléphones Android dans des objectifs de conformité et d'innovation. La CNIL et la STIF (Société de Transport d'Île de France) ont décidé ensemble d'anonymiser les données à caractère personnel, sans que cela n'entrave la finalité poursuivie qui était l'optimisation du réseau. La STIF pouvait donc travailler sur des données qui n'étaient plus soumises à la loi « Informatique et Libertés » car anonymes.

Néanmoins, l'anonymisation devient chaque jour plus complexe, notamment avec l'émergence du temps réel, au point qu'il sera toujours possible de « désanonymiser » un « jeu de données anonymes » dans un contexte *Big Data*. Un jeu de données anonymes peut donc être de nouveau soumis à la loi Informatique et Libertés. L'anonymisation doit donc être sans cesse révisée dans le temps.

De plus, dans certains cas, la protection des données personnelles est assurée par un processus de pseudonymisation (remplacement d'un nom par un pseudonyme). Ce processus diffère de l'anonymisation car les données restent liées à la même personne dans tous les dossiers et systèmes informatiques sans que l'identité ne soit révélée.

Par ailleurs, l'anonymisation semble relever, en droit, de l'utopie compte tenu de la position de la CNIL, qui applique de manière stricte la lettre de la loi Informatique et Libertés. En effet, afin de déterminer si une donnée est personnelle ou pas, elle demande que soit pris en compte l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable de traitement ou toute autre personne[28]. C'est ce principe qu'elle a appliqué pour s'opposer au projet de la société JC Decaux[29]. De son côté, le RGPD encadre le principe de pseudonymisation[30].

C'est pourquoi le rapport du CIGREF sur l'économie des données personnelles[31] propose une piste alternative basée sur des plates-formes, des canaux de communication privilégiée permettant aux personnes de solliciter elles-mêmes leurs droits (informations, recueillement du consentement etc.).

VII. CONCLUSION

Dans un environnement ultra-concurrentiel et en constante transformation, où les entreprises sont de plus en plus exposées aux risques, une meilleure appréhension des dispositifs de sécurité à mettre en place fournira un avantage compétitif de taille. Les décisions stratégiques des entreprises pourront être réalisées sereinement, dès lors que la gestion des risques qui y est associée (identification, évaluation, réponse) sera non seulement orientée « protection » mais également « optimisation de la performance »[32].

Les organismes qui ont déjà mis en place une solide politique de sécurité de leurs SI ainsi que des dispositifs permettant de protéger leurs données sensibles auront juste à adapter leur dispositif à la traçabilité et à la surveillance du traitement des données personnelles. Pour les autres, le RGPD les oblige à réorganiser leurs dispositifs de protection et leurs méthodes de travail en profondeur dans leur propre intérêt juridique et économique.

Dans tous les cas, le nouveau règlement européen constitue une opportunité de transformer la contrainte réglementaire liée à la sécurité des données personnelles en avantage concurrentiel visant à augmenter le niveau de confiance de ses clients. ■

27. Étude Deloitte 2016: « Enjeux Cyber 2016, la face cachée de la cybersécurité ».

28. Article 2, alinéa 2, de la loi de 1978.

29. Délibération n° 2015-255 du 16 juillet 2015.

30. Selon son article 4, 5°, les données doivent être traitées de telle sorte qu'elles « *ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires* ».

31. Rapport du CIGREF sur « L'Économie des données personnelles : les enjeux d'un business éthique », octobre 2015.

32. Michael Bittan, associé responsable *Cyber Risk Services*, Deloitte France, étude Deloitte 2016 « Enjeux Cyber 2016, la face cachée de la cybersécurité ».