Les Echos SPÉCIAL
HIGH-TECH

RÉGLEMENTATION // Le nouveau règlement européen sur la protection des données est capital pour l'univers data-sécurité-mobile. Mais il est encore loin d'être appliqué à la lettre dans les entreprises, surtout parmi les PME.

RGPD : les entreprises s'adaptent à pas comptés

La mise en conformité des TPE-PME n'en est qu'à ses balbutiements. *Photo Shutterstock*

A fin septembre 2018, soit cinq mois après le coup d'envoi du règlement européen sur la protection des données (RGPD), la CNIL a dressé un bilan chiffré : 24.500 organismes avaient désigné un délégué aux données personnelles (DPO) et 600 notifications de violation des données avaient été reçues, concernant environ 15 millions de personnes. La preuve, selon la CNIL, que les *« professionnels se sont emparés de ce nouveau cadre et que sa mise en œuvre est effective en France »*.

L'arrivée du RGPD n'est pas non plus passée inaperçue auprès du grand public. Dans les jours qui ont suivi son entrée en vigueur, les internautes ont été submergés d'e-mails de sociétés demandant un consentement à l'utilisation de leurs données personnelles. Une bonne nouvelle pour les consommateurs. Mais aussi un signe de fébrilité de la part des entreprises. Et pour cause : le RGPD impose aux organisations toute une série d'obligations, dont certaines mettront du temps à s'appliquer. Pour Xavier Leclerc, CEO de DPMS et président de l'Union des Data Protection Officer, l'un des volets compliqués porte sur la conservation des données : *« Il existe des quantités de situations à traiter. Par exemple, les données sur les salariés ayant quitté l'entreprise doivent être sorties de la base active pour être archivées ailleurs. »*

Portabilité des données

Le droit des utilisateurs de supprimer leurs données personnelles pose aussi des problèmes pratiques. Tout comme le fameux droit à la portabilité permettant à un ancien client d'exiger le transfert de ses informations personnelles vers son nouveau fournisseur ou prestataire. Peu après le 25 mai 2018, certaines entreprises ont été assaillies de messages d'internautes, jusqu'à plusieurs centaines par semaine, demandant à exercer ces droits de transfert. Souvent débordées, les organisations concernées n'ont pas encore eu le temps de s'adapter. *« A l'instar de nombreux autres acteurs, nous devons mettre en place des solutions pour consolider et automatiser le traitement de ces demandes »*, reconnaît François-Xavier Vincent, responsable en chef sécurité informatique chez Oodrive.

Reste aussi, pour certains sous-traitants, à modifier les contrats les liant à leurs donneurs d'ordre afin de les rendre « RGPD compatibles ». Une démarche délicate, à en croire Olivier Simonis, cofondateur de Qualifio, prestataire dans le marketing interactif et la collecte de données : *« Sur 400 clients, seulement la moitié ont pour l'instant répondu à nos propositions d'avenants. Si les négociations durent, c'est que certains grands groupes veulent imposer leur propre modèle de contrat. »*

D'une façon générale, la majorité des TPE-PME n'ont pas du tout anticipé le RGPD. Leur mise en conformité n'en est qu'à ses balbutiements. *« Le sentiment qui domine dans les petites structures, c'est comment se débarrasser du sujet »*, juge Emmanuelle Cornet-Ricquebourg, vice-présidente de Cyberlex, association du droit des nouvelles technologies, qui pointe l'impréparation générale. *« Celles qui n'ont rien budgété cette année, et c'est la majorité, ne commenceront à entamer une démarche qu'en 2019. »* Dépourvus de moyens, beaucoup de DPO, nommés à la va-vite en mai dernier, sont un alibi pour attester de la conformité.

Changer les habitudes

Même si les sanctions prévues (jusqu'à 4 % du chiffre d'affaires) sont dissuasives, les retardataires comptent sur la bienveillance de la CNIL au moins jusqu'à fin 2018. Pour l'application des nouveaux droits introduits par le RGPD (droit à portabilité, par exemple), l'autorité administrative se dit prête à « accompagner » les organisations. Mais en cas de manquement sur la sécurité des données, la CNIL sera sans pitié. Dans les grands groupes, la problématique est différente. Si l'arrivée du RGPD a été largement anticipée, l'un des principaux obstacles est d'ordre « culturel ». Selon Fabrice Haccoun, CEO d'Advanced Schema, *« au-delà des investissements techniques pour cartographier et monitorer les traitements des données, il y a dans chaque groupe un vaste chantier d'éducation à mener pour modifier les habitudes des collaborateurs »*. Un travail de sensibilisation réalisé à la SNCF. Le groupe ferroviaire a mis en place un chatbot interne « spécial RGPD » qui répond automatiquement aux questions des salariés. En un mois, cet outil développé par la start-up Clevy avec le cabinet d'avocats Desmarais aurait répondu à 1.200 questions.

— ***Bruno Askenazi***

« Les entreprises non européennes sont sur un pied d'égalité avec les acteurs européens »

DR

1 Pour l'Union européenne, le RGPD est-il un moyen d'ériger des barrières à l'entrée de son marché ou de rééquilibrer les forces ?

Le RGPD s'applique, en effet, à des entreprises hors UE, dans le cas où ces entreprises détiennent des données relatives à des citoyens ou des organisations basées en Europe. Dans ces situations, ce nouveau règlement met les entreprises non européennes sur un pied d'égalité avec les acteurs européens. C'est un traitement d'égalité pour des acteurs qui ont vocation à s'adresser aux mêmes consommateurs et à leur offrir des biens ou des services similaires.

2 Le RGPD commence-t-il à inspirer d'autres pays ?

Le California Consumer Privacy Act de 2018 est le fruit du RGPD. Mais avec quelques différences notables. Le législateur californien avait surtout dans son viseur la vente de données de consommateurs à des tiers. Désormais, les sites doivent faire apparaître une bannière spécifique à ce sujet permettant aux internautes de s'opposer à la vente de leurs données personnelles à d'autres sociétés.

Le RGPD est, lui, axé sur la notion de consentement et non d'opposition. Par ailleurs, certains pays hors UE souhaitent se voir reconnus par l'Europe comme offrant une protection adéquate pour le traitement des données. C'est le cas du Japon où l'on pourra bientôt transférer des données personnelles sans pour autant mettre en œuvre des mécanismes propres à ce pays.

3 Le RGPD européen est souvent plus strict que la plupart des législations, notamment en Asie. Est-ce un désavantage pour les acteurs européens notamment vis-à- vis de leurs concurrents chinois ?

Au contraire, beaucoup d'entreprises, européennes ou pas, ont pris conscience qu'une certaine éthique en matière de traitement des données des consommateurs leur fait gagner en crédibilité vis-à-vis des acteurs européens. A condition toutefois d'avoir la capacité à démontrer un traitement de ces données de façon raisonnée.

Reste, il est vrai, des difficultés claires pour les entreprises chinoises dans la mise en œuvre du RGPD dans les cas où elles sont soumises à ce règlement. En matière de protection de la vie privée, elles ont une culture différente qui les rend moins sensibles à ce sujet. Elles ont donc du mal à appréhender les objectifs du texte européen. Surtout, les sociétés chinoises ont des obligations vis-à-vis de leur gouvernement qui peuvent entrer en contradiction avec l'application du RGPD. Ce problème de conflit entre législations n'est pas encore résolu. ■

Propos recueillis par ***B. A.***

Talent Soft, la sécurité des données au cœur du modèle économique

Cet éditeur français, spécialisé dans la gestion du capital humain en mode cloud, était fin prêt pour le RGPD bien avant son entrée en vigueur.

« Nous avons intégré la sécurité au cœur de notre développement, dès notre création, en 2007 », confie Joël Bentolila, directeur technique et cofondateur de Talentsoft. Une nécessité absolue pour cette plate-forme de gestion RH, qui réalisera cette année un chiffre d'affaires de 66 millions avec 600 personnes dans 15 pays. Le règlement européen sur la protection des données personnelles ne l'a donc pas pris de court puisque Talentsoft gère, en mode cloud, des données à caractère personnel pour ses clients. La société a commencé par sécuriser les infrastructures de ses 10 data centers dans le monde : pare-feu, sondes de détection d'intrusion, cloisonnement des sous-réseaux, double protection de pare-feu entre la partie Web et la partie serveur... A aucun moment les données des clients ne sont exposées sur Internet. *« Cela rend étanche chaque segment du centre de données »*, reprend Joël Bentolila. Qui plus est, Talentsoft recourt à une solution de « security information event management » (SIEM), qui analyse, grâce à une intelligence artificielle, les connexions et requêtes dans un lac de données afin de détecter en temps réel la plus infime menace.

Côté logiciel, *« il faut veiller à la sécurité des données de bout en bout, dès le départ et en continu. Par son coté itératif, cette méthode va de pair avec les méthodes de développement agile,* reprend le directeur technique de Talentsoft, entreprise certifiée ISO 27001 (pratiques sécuritaires). *Pour chaque fonctionnalité, un binôme de développeurs écrit le code, qui est relu par une autre personne avant de le verser au pot commun. Cela rajoute de la fertilisation croisée et de la transparence »*. Talentsoft utilise également différents étages de chiffrement : les données en transit sont cryptées via des réseaux privés virtuels (VPN), d'autres le sont à l'intérieur de la base de données. Pour accélérer ce processus, l'éditeur utilise, d'une part, des cartes de chiffrement/déchiffrement spécialisées et, d'autre part, un coffre-fort de clefs de cryptage. De quoi être confiant lors des audits réguliers de ses 1.900 clients.

— ***Erick Haehnsen***

A aucun moment les données des clients ne sont exposées sur Internet. *Photo DR*

DONNÉES // La sécurité des données n'est plus un choix mais une nécessité. Le coût de l'audit et de la mise en conformité varie en fonction de la sensibilité de l'activité. Attention aux fausses promesses de prestataires !

Diagnostic : de l'auto-évaluation à la mise en conformité sur-mesure

Après Optical Center, Dailymotion et Assistance Centre d'appels, l'Alliance française Paris Ile-de-France s'est vue infliger par la Commission nationale de l'informatique et des libertés (CNIL) une amende de 30.000 euros. Motif : l'Alliance a laissé accessibles 413.144 documents contenant des données à caractère personnel (DCP), contrevenant ainsi au règlement général sur la protection des données personnelles (RGPD). Le pouvoir de sanction de la CNIL est désormais important : l'amende peut atteindre 4 % du chiffre d'affaires mondial ou 20 millions d'euros.

Flirtant avec le sentiment d'urgence et de crainte, un florilège d'arnaqueurs tente de profiter de l'aubaine : fausses listes des entreprises certifiées pour la réalisation d'audit, numéros de téléphone surtaxés pour se renseigner, guides de mise en conformité comme produits d'appel… Pas de panique ! Pour les dirigeants désireux de savoir comment se mettre en conformité, la CNIL et bpifrance ont réalisé le « Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises ». « *En 62 pages, celui-ci traite le sujet de façon simple, limpide et pragmatique* », indique Dominique Soulier, administrateur au Club de la sécurité de l'information français (Clusif).

La CNIL propose une liste de prestataires labellisés pour l'audit et la formation. *Photo Shutterstock*

Ce guide propose de passer à l'action en quatre étapes : d'abord cartographier les données personnelles et construire le registre de leurs traitements (recrutement, paie, gestion commerciale…), puis détruire les données inutiles. Ensuite, respecter l'obligation de transparence : la raison de la collecte des DCP, le processus pour les modifier ou les retirer de la base. Enfin, sécuriser ces données… Ce travail peut être aussi confié à des prestataires. La CNIL propose une liste de prestataires labellisés pour l'audit et la formation : cabinets d'avocats, sociétés de conseil, cabinets de conseil en cybersécurité… Cette liste n'est pas exclusive – la CNIL a d'ailleurs cessé de délivrer ces labels et travaille sur une certification – et des prestataires non labellisés peuvent être tout aussi sérieux. Le cabinet de cybersécurité Akerva, qui n'est pas labellisé, a ainsi élaboré deux modules d'e-learning, le premier sur la sensibilisation des collaborateurs au RGPD et le second sur la protection des données.

Tenue des registres

Le prix de l'audit et de la mise en conformité varie en fonction de l'activité et de la taille de l'entreprise et de sa maturité en cybersécurité. Les TPE et PME, dont le cœur de métier ne porte pas sur les DCP, peuvent établir elles-mêmes leur diagnostic, qui débouche sur la tenue du registre des traitements et la sécurisation des données personnelles. En s'adressant à un cabinet d'audit, « *pour 2.000 euros, elles obtiennent le registre des traitements ainsi que la revue des mentions à publier sur le site Web et les documents commerciaux (factures, CGU, CGV…) pour informer les personnes de leurs droits* », détaille Morgan Matrat, consultant sécurité chez Akerva.

Pour des entreprises ayant besoin d'un accompagnement complet (juridique, organisationnel et technique), « *il en coûtera de 10.000 à 20.000 euros pour une TPE-PME, jusqu'à plusieurs millions d'euros pour une multinationale* », souligne Jérémy Harroch, PDG de Quantmetry, une start-up d'IA spécialisée dans la valorisation de la donnée.

Afin de couvrir ces risques, il est également conseillé de contracter une cyberassurance.

Afin de couvrir ces risques, il est également conseillé de contracter une cyberassurance. Toutefois, « *aucun assureur ne couvre le risque "diagnostic RGPD"*, prévient François Beaume, vice-président de l'Association pour le management des risques et des assurances de l'entreprise (Amrae). *En revanche, certains proposent des assurances cyber qui prennent en charge une partie de l'exposition liée au RGPD. Entre autres, les frais de notification aux usagers, les frais de communication et de perte d'exploitation.* »

— ***Erick Haehnsen***

L'ENJEU

Privacy by Design : la méthode pour des logiciels « RGPD native »

Respecter les données personnelles avant même d'écrire la première ligne de code nécessite de travailler en équipe.

L'exercice qui associe développeurs, juristes et utilisateurs se révèle rentable.

Respecter le règlement général sur les données personnelles dès la conception d'un logiciel, tel est l'enjeu du Privacy by Design. « *La chose à ne surtout pas faire, c'est de développer d'abord le code pour le mettre ensuite en conformité* », souligne Jérémy Harroch, PDG de Quantmetry qui, depuis 2011, élabore des applications à base d'intelligence artificielle.

Avec le Privacy by Design, développeurs et spécialistes de la protection des données sont appelés à travailler main dans la main. « *Il y a deux grandes questions à se poser : a-t-on le droit d'utiliser telle donnée et comment sera-t-elle protégée ?* » indique Morgan Matrat, consultant chez Akerva, un cabinet de conseil en cybersécurité.

Minimiser les flux

Premier exemple avec l'assureur Swiss Life et la conception d'Aïda, une application mobile pour les commerciaux. En amont du projet, certains conseillers commerciaux avaient participé à un atelier de Design Thinking, afin de concevoir leur futur outil sur smartphone. Dans ce groupe de travail figuraient aussi un chef de projet, cinq développeurs, un directeur et un délégué à la protection des données (DPO). « *Nos conseillers voulaient optimiser leur temps d'itinérance. Notamment saisir vocalement leurs comptes-rendus sur smartphone, les convertir automatiquement en texte et les envoyer dans notre application centrale de gestion de la relation client (CRM)*, décrit Eddie Abecassis, directeur marketing stratégique, data science et innovation chez Swiss Life. *Ils voulaient aussi pouvoir interroger la fiche client du prochain rendez-vous. De même, en cas d'annulation de dernière minute, voir comment en profiter pour organiser une autre visite à proximité.* » Pour réaliser cette application, Swiss Life a choisi l'algorithme de reconnaissance vocale créé par la start-up Quantmetry. L'assureur et la start-up se sont demandé comment minimiser les flux de données sensibles.

Et comment, dès la conception de l'application, protéger les données du client. « *Après une analyse complète, nous nous sommes rendu compte qu'il n'était pas nécessaire de véhiculer certaines données comme les contrats des clients ou l'analyse des portefeuilles, mais juste les plus utiles en mobilité, par exemple la géolocalisation de leur lieu de résidence,* reprend Eddie Abecassis. *Par ailleurs, il fallait appliquer à la mobilité un haut niveau d'exigence en matière de sécurité et de cryptage des données.* »

Un travail salutaire, car qui dit moins de données à transporter, dit temps de chargement plus rapide. Développée en méthode agile, l'application est testée en grandeur réelle auprès d'une vingtaine de conseillers depuis juin 2018. « *Désormais, nous appliquerons cette méthode de Privacy by Design à tous nos prochains projets* », confie Eddie Abecassis.

Une approche éthique de la donnée

Autre exemple de l'intérêt de tenir compte en amont des contraintes du RGPD, celui de la start-up Vectaury, créée en 2014 et spécialisée dans les campagnes de marketing digital. « *Nous achetons l'accès à des données personnelles auprès d'une vingtaine d'éditeurs d'applications mobiles (actualités, météo…) qui, chacune, demandent à l'internaute mobile son consentement pour collecter ses données personnelles*, décortique Mathilde Ferriol, DPO qui travaille avec les développeurs et les experts en sécurité de Vectaury. *Ensuite, notre technologie trie, agrège, nettoie, analyse ces données avant de lancer les campagnes ou de vendre des études aux marques.* »

Point fort de la solution : les données sont « pseudonymisées », c'est-à-dire que chaque profil est réduit à un identifiant publicitaire et une géolocalisation. Outre les 180 mesures de sécurisation de son système d'information, la start-up chiffre les données pseudonymisées avec un cadenas qu'elle est seule à détenir. « *Dès le départ, notre modèle économique repose intégralement sur les données personnelles. Nous avons choisi d'avoir une approche éthique à ce sujet* », souligne Mathilde Ferriol. Une stratégie de Privacy by Design qui gagne la confiance des annonceurs et des investisseurs : Vectaury vient de lever 20 millions d'euros pour se développer à l'international. — ***E. H.***

CONTRÔLE // Les fichiers de consultation, appelés « cookies », sont désormais soumis au consentement préalable des internautes. Conséquence : leur nombre a fortement diminué, surtout dans la publicité ciblée.

Après le RGPD, l'économie du cookie dans le pétrin

Effet direct de l'application du RGPD : l'économie du cookie vacille, assure une récente étude de l'université d'Oxford. L'enquête réalisée entre avril et juillet 2018 sur 200 sites d'information européens révèle que le nombre de cookies, ces fichiers stockés sur les ordinateurs et les smartphones lorsque vous consultez un site, a chuté de 22 % en Europe. Une baisse qui atteindrait même 32 % en France.

La tendance concerne les cookies « tiers » laissés par des sociétés autres que le site propriétaire à des fins de ciblage publicitaire. Le phénomène s'explique pour deux raisons. « *Dans la mesure où beaucoup d'entreprises interprètent le RGPD comme imposant l'accord de l'internaute avant d'installer un cookie, elles ont commencé à faire le ménage* », explique Mickaël Avoledo, directeur associé de M13h, agence de conseil en data marketing. La technique la plus efficace consiste donc à éliminer certains tags à l'origine du déclenchement de ces cookies. « *Par ailleurs, au moment de la demande de consentement qui se matérialise par l'apparition de petites bannières, une proportion non négligeable d'internautes, entre 5 et 20 %, ont saisi l'occasion pour refuser certains cookies* », ajoute-t-il.

Coup de froid sur la publicité ciblée

Aussi, de plus en plus de sites Internet s'équipent de systèmes automatisés de management de cookies pour fournir au visiteur des informations sur ces fichiers (utilité, intrusivité, durée de vie, éditeurs), et éventuellement leur permettre de les bloquer. Cette raréfaction des cookies rebat aujourd'hui les cartes des méthodes de ciblage que les marques mettaient jusqu'à présent en œuvre pour rendre plus efficace leur communication sur le Web.

Dans le monde de la publicité en ligne, de nombreux acteurs voient aussi leur business menacé. En première ligne, les régies publicitaires et les fournisseurs de données tierces (« data providers »). Criteo, l'un des leaders mondiaux du ciblage publicitaire, paraît ainsi très exposé. Mais, estime Cédric Vandervynckt, vice-président Europe, Moyen-Orient et Afrique de l'entreprise, cet impact serait « *moindre pour Criteo* », qui a anticipé depuis plusieurs années l'arrivée du RGPD. « *Le nouveau règlement est pour nous une évolution, pas une révolution. Dès 2008, nous avons laissé le choix aux consommateurs d'arrêter de recevoir nos bannières grâce à l'opt-out.* » Même si le RGPD va plus loin en imposant un consentement préalable, c'est-à-dire l'opt-in, ce sera pour Criteo moins problématique que la récente décision d'Apple. Fin 2017, la marque à la pomme a proposé aux utilisateurs de son navigateur Safari de bloquer s'ils le souhaitaient la technologie de suivi publicitaire Criteo. Une initiative qui avait fait plonger le cours de Bourse de la société française de 28 % en une journée. Toutefois, selon un bon connaisseur du secteur, Criteo a pourtant autant à craindre du RGPD que des paramétrages de plus en plus agressifs des navigateurs.

Les Gafa grands gagnants

Reste que quelques acteurs du marketing en ligne y ont gagné au change. Selon Olivier Simonis, cofondateur de la plate-forme de collecte de données Qualifio, « *de plus en plus de clients laissent tomber leurs prestataires américains qui n'apportent pas les garanties suffisantes en matière de stockage de données. Ils se tournent alors vers des sous-traitants européens comme nous* ».

Avec une exception, les Gafa, qui n'ont, eux, pas grand-chose à craindre. D'après l'étude de l'université d'Oxford, ces géants américains ont assez peu souffert du coup de frein des sites d'information européens sur les cookies. 96 % des sites consultés par l'étude ont par exemple conservé les marqueurs de Google.

Si, pour la plupart des sites, demander un consentement clair aux internautes afin d'exploiter leurs données personnelles présente un risque non négligeable de refus, dans le cas des Gafa, ce risque est réduit. Obtenir l'adhésion des visiteurs est presque une formalité. « *La proposition de valeur de Facebook, Google ou Amazon est tellement forte qu'elle induit un consentement évident, immédiat, mais pas nécessairement plus éclairé,* constate Charles de Gastines, cofondateur de la fintech Paylead. *Les Gafa sont les grands gagnants du RGPD.* »

— ***Bruno Askenazi***

La tendance concerne les cookies « tiers » laissés par des sociétés autres que le site propriétaire à des fins de ciblage publicitaire. *Photo Shutterstock*

L'IDÉE

WeProov fait le ménage parmi ses prestataires

Progressivement, l'application a intégré le stockage sécurisé, le chiffrement des données et la blockchain. *Photo DR*

La start-up d'états des lieux sécurisés a procédé à un audit de ses prestataires.

WeProov a fait le tri dans les multiples cookies de son service Web et mobile de constat d'assurance et d'état des lieux. L'entrée en vigueur du RGPD est passée par là. Pas le choix pour cette start-up qui développe depuis mars 2016 une application d'envois de photos sécurisés. Dans un premier temps, l'entreprise de 20 salariés a commencé par réaliser un « audit de cookies ». Résultat, elle s'est rendu compte que certains services tiers n'avaient plus leur place sur sa plate-forme. Plusieurs de ces fichiers ont donc été retirés. A l'instar de nombreux autres acteurs du Web, WeProov envisage maintenant d'automatiser la gestion des cookies sur son site grâce à un « tag manager ».

Plus de transparence

Pour Gabriel Tissandier, cofondateur de la start-up, « *cet outil se doit d'avertir le visiteur via une bannière et lui permettre de débloquer les cookies à loisir en lui fournissant une information complète, claire et concise sur les cookies présents et sur leurs éditeurs* ». Bref, instaurer plus de transparence pour les clients vis-à-vis des marqueurs utilisés sur le site.

Dans le même temps, WeProov a changé de fournisseur pour son outil de relation client. Le CRM d'origine n'était pas conforme aux nouvelles exigences du RGPD en matière de conservation des données. A la trappe aussi un prestataire américain d'envoi de SMS. Son service récupérait des cookies, en contradiction avec le nouveau règlement. Il a été remplacé par une société européenne.

Moyens humains et financiers

Ces multiples changements ont réclamé des moyens humains et financiers supplémentaires. A commencer par l'implication d'une déléguée aux données personnelles, recrutée il y a un an pour mettre en œuvre la conformité. Rien que pour les cookies, la facture est estimée à 15.000 euros. « *Il s'agit d'une démarche stratégique et non subie,* souligne Gabriel Tissandier. *Mieux, nous voulons faire de ces investissements RGPD un argument marketing puissant qui fait sens avec notre rôle d'acteur de confiance dans les échanges de biens.* » De fait, WeProov a toujours considéré la sécurité numérique comme stratégique dans son modèle économique. Dès 2016, la start-up a planché sur la protection des données de ses clients (180 aujourd'hui). Progressivement, l'application a intégré le stockage sécurisé, le chiffrement des données et, plus récemment, la blockchain afin de garantir la confidentialité et l'intégrité des données. Couronnement de ces efforts, WeProov vient de rejoindre la Fédération nationale des tiers de confiance du numérique (FNTC) en tant que « prestataire et éditeur de confiance ». Un contexte favorable pour aborder le RGPD en tant que nouvelle opportunité et non comme une contrainte pesante.

— ***B. A.***

INTERVIEW // ALAIN BOUILLÉ Président du Club des experts de la sécurité de l'information et du numérique (Cesin)

« Ne pas confondre conformité et sécurité »

Propos recueillis par ***Erick Haehnsen***

Quels sont les liens entre RGPD et sécurité ?

Ces liens sont relativement naturels car, dans quasiment toutes les grandes organisations, il y a un responsable de la sécurité des systèmes d'information (RSSI) qui s'occupe déjà de la sécurisation de toutes les données. Pas seulement des données à caractère personnel (DCP). Par conséquent, il leur a été assez simple de mener le projet de mise en conformité au RGPD pour la partie sécurisation des DCP.

Avec sa menace d'amende et la date butoir du 25 mai 2018, le RGPD a mis une lentille extrêmement grossissante sur les données personnelles. Les entreprises pouvaient alors se retrouver avec le risque de laisser sur le bord de la route d'autres projets de sécurisation de données plus importantes. Parmi les données sensibles qui ne sont pas à caractère personnel, je rappelle qu'il y a, par exemple, les brevets, les projets de recherche et développement, les secrets commerciaux… Lorsqu'une entreprise se lance dans un projet de classification des données, elle aboutit à des mesures de sécurisation plus fortes sur les données les plus sensibles. Or, un grand nombre de données à caractère personnel ne sont pas sensibles. C'est le cas de l'annuaire de l'entreprise auquel tout le monde accède en interne. En clair, le RGPD a pu conduire à retirer certains budgets en matière de sécurité. Il a fallu faire des arbitrages.

Comment se répartissent les rôles entre RSSI et délégués à la protection des données ?

Il existait déjà le duo RSSI/Correspondant informatique et libertés (CIL). Dans notre baromètre de 2017, le Cesin avait indiqué que, dans 35 % des cas, la même personne cumulait les fonctions de RSSI et de CIL. En ce qui concerne le RGPD, bien des RSSI/CIL ont été mobilisés afin de conduire le projet de conformité. Notamment pour dresser l'inventaire des données personnelles. Dans le cadre du RGPD, il a également fallu désigner un délégué à la protection des données ou « data protection officer » (DPO). On s'en doute, de nombreux RSSI/CIL sont devenus DPO.

« Il faut mettre en place des processus de protection documentés ainsi que des processus de gestion de crise et d'incident. » *Photo DR*

Les entreprises ont pu aussi créer un nouveau poste. Jusqu'ici, le RSSI relevait soit de la direction des risques soit de la DSI. Les nouveaux DPO sont liés à la direction de la conformité soit, à défaut, à la direction juridique. Généralement, le DPO a un profil de juriste ou peut être issu des métiers. Sa compétence est souvent éloignée de l'informatique.

Le RGPD constitue-t-il un gain pour les entreprises ?

En sécurité des systèmes d'information, il y a un un adage : conformité ne signifie pas forcément sécurité. Ce n'est pas parce que l'on est conforme à la réglementation que le système d'information sera sécurisé. Ce fut le cas de la chaîne américaine de supermarchés Target. Elle était conforme au règlement Payment Card Industry Data Security Standard sur les cartes bancaires. Pourtant, en janvier 2014, elle a été victime d'un vol de son fichier de cartes bancaires qui a affecté 110 millions de clients… C'est là que le rôle du RSSI est d'une importance cruciale pour inventorier les données à caractère personnel, mais encore faut-il les protéger à bon escient. Il faut aussi mettre en place des processus de protection documentés ainsi que des processus de gestion de crise et d'incident. Et ce n'est pas tout : il faut les tester.

> Généralement, le DPO a un profil de juriste ou peut être issu des métiers.
>
> Sa compétence est souvent éloignée de l'informatique.

Quid de la mobilité ?

Ce qui rentre en ligne de compte en termes d'utilisation, c'est la finalité de la collecte des données personnelles. A cet égard, le RGPD a considérablement renforcé la loi informatique et libertés en réclamant aux entreprises de dire à quoi vont servir les données personnelles collectées. L'idée, c'est de protéger le citoyen ou le salarié-citoyen contre le détournement de finalité. Par exemple, les données de géolocalisation pour assister les travailleurs isolés en situation potentiellement dangereuse ne doivent pas servir à l'employeur à les espionner. ■

MÉTIER // Depuis l'entrée en application du règlement général sur la protection des données, les organisations utilisant des informations à caractère personnel doivent s'en remettre à un « data protection officer ».

Délégué à la protection des données, une expertise utile

Avec le règlement général sur la protection des données (RGPD), entré en vigueur dans l'Union européenne le 25 mai 2018, les entreprises doivent assumer de plus grandes responsabilités. Et dans toutes les organisations concernées, la cheville ouvrière en est le délégué à la protection des données, aussi appelé « data protection officer » ou « data privacy officer » (DPO). Ses missions sont définies par le RGPD. En résumé, il ou elle doit veiller à la conformité de son entreprise ou organisation avec ce nouveau cadre juridique, et rendre vertueux le traitement des informations relatives aux clients et aux collaborateurs.

Si la fonction de DPO est désormais très visible dans nombre d'organigrammes, qu'on ne s'y trompe pas, ce métier ne vient pas d'éclore. *« Une directive européenne de 1995, transposée en droit français en 2004, avait conduit de nombreuses collectivités territoriales et grandes entreprises à nommer un correspondant informatique et libertés qui était chargé de s'assurer de la bonne application de la loi. Avec le RGPD, les sanctions ont changé d'échelle, le DPO a donc un rôle bien plus stratégique et une mission élargie »*, indique Paul-Olivier Gibert, président de l'Association française des correspondants aux données personnelles (AFCDP), organisme fondé en 2004 qui fédère plus de 4.000 adhérents.

Fin septembre 2018, selon la CNIL, 24.500 organismes avaient soit promu leur correspondant informatique et libertés en DPO soit recruté… Quelques semaines avant la mise en application du RGPD, la CNIL estimait qu'au total 80.000 organisations étaient concernées par l'obligation de désigner un délégué à la protection des données.

Il ou elle devra veiller à la conformité de son entreprise ou organisation avec ce nouveau cadre juridique. *Photo Shutterstock*

Le DPO rapporte au plus haut de la hiérachie

L'importance stratégique du DPO reflète la hauteur des nouveaux enjeux. *« La donnée revêtant une importance grandissante dans notre société, les métiers appelés à travailler sur son bon usage, tel le DPO, vont figurer parmi les plus porteurs de ces dix prochaines années. Il est certain qu'une nouvelle filière professionnelle est en train de se dessiner »*, estime Paul-Olivier Gibert. Les formations ont éclos dans les universités ou dans les grandes écoles de management et d'ingénieurs : par exemple à l'Ecole nationale de la statistique et de l'analyse de l'information (Ensai), à l'école d'ingénieurs du numérique (Isep), à Grenoble EM, à l'institut Mines-Télécom Business School, ou encore à l'université Panthéon-Assas…

Les compétences requises sont à la croisée de plusieurs expertises, allant de l'informatique au juridique. *« Surtout, le DPO doit maîtriser parfaitement la stratégie et le fonctionnement de l'entreprise, et disposer de capacités de communication, car il œuvre en interaction avec toutes les entités de l'entreprise, à l'instar de la direction des systèmes d'information et de la direction des ressources humaines »*, pointe Paul-Olivier Gibert. Le DPO, qui exerce un métier transverse, travaille également au plus près de la direction générale et du centre de décision, car, comme le stipule le RGPD, il doit être directement rattaché au plus haut niveau de la hiérarchie.

Des compétences recherchées

Le délégué à la protection des données a également un rôle d'évangélisation au sein de l'organisation, c'est lui qui contribue à diffuser cette nouvelle culture. *« Le travail du DPO ne sera pas le même suivant qu'il travaille dans une PME, dans une ETI, dans un grand groupe, dans une collectivité territoriale ou dans un établissement public. Néanmoins, quel que soit le contexte dans lequel il évolue, il doit systématiquement être en mesure d'expliquer à tous les membres des équipes la nécessité de s'appuyer sur la réglementation. C'est véritablement un métier d'échange »*, observe le président de l'AFCDP. Quant à sa rémunération, facteur clef pour attirer et fidéliser ces profils dorénavant chassés de toutes parts, *« compte tenu des enjeux, ce poste ne doit pas être sous-payé »*, convient Paul-Olivier Gibert. En regard des différentes études de rémunération des grands cabinets (Michael Page, Robert Walters, Hays…), un salaire annuel de DPO oscille autour de 35.000 euros brut pour les profils juniors, à près de 50.000 euros pour les profils plus seniors avec cinq ans d'expérience en data ou juridique.

— ***Julie Le Bolzer***

PROTECTION

Les DRH face aux données personnelles des salariés

Le RGPD s'applique à tout employeur et sous-traitant manipulant les données personnelles d'un salarié résidant en Europe.

Les directions des ressources humaines sont depuis longtemps rompues à l'exercice du traitement des informations confidentielles. *« Avant l'entrée en vigueur du RGPD, des normes simplifiées de la CNIL sur les questions de gestion du personnel donnaient déjà un cadre aux employeurs en matière de collecte des données personnelles relatives aux collaborateurs »*, rappelle Guillaume Bordier, associé chez Capstan Avocats, cabinet spécialisé en droit social.

Avec le RGPD, les entreprises se voient imposer un plus grand formalisme. Pour exemple, l'employeur est désormais tenu d'établir un registre des traitements, d'analyser les impacts et d'informer de façon plus précise les salariés sur les données dont dispose l'entreprise. *« L'organisation devait déjà communiquer auprès des équipes, mais le cadre se révèle beaucoup plus formel »*, confirme Guillaume Bordier. Ces nouveaux éléments constituent-ils une révolution pour les DRH ? *« C'en est une, mais ils ne partent pas d'une page blanche*, estime David Luponis, associé cybersécurité chez Mazars. *Avant le RGPD, nous constations des disparités de réglementations au sein de l'Union européenne, mais la France faisait partie des pays les plus avancés en termes de protection des données personnelles. »*

Règles contraignantes

Les principes de protection posés par le RGPD sont pertinents, mais ses règles sont aussi contraignantes pour les organisations qui font face à un volume grandissant d'informations. Outre les données nécessaires au recrutement, à la rémunération, au prélèvement des cotisations sociales (et bientôt de l'impôt sur le revenu), au suivi médical ou encore à la gestion des carrières, l'entreprise dispose d'autres données, notamment grâce au développement des nouvelles technologies. *« Si l'on prend le cas de la vidéosurveillance, l'image du salarié est une donnée personnelle. Si l'on prend le cas de la géolocalisation des véhicules mis à disposition par l'entreprise, les déplacements du salarié en dehors de son temps de travail constituent des données personnelles. Si l'on prend le cas des systèmes d'accès biométriques, là encore, il s'agit de données relevant de la vie privée »*, énumère Guillaume Bordier.

Les nouvelles formes d'organisation sont également une porte ouverte sur des renseignements d'ordre privé. Dès lors qu'un collaborateur en télétravail ou en mobilité utilise les outils mis à sa disposition par l'entreprise, il se livre sur ses usages. *« Même s'il ne s'agissait pas de cas fondés sur l'application du RGPD, il y a déjà des jurisprudences traitant de la frontière entre la vie privée et la sphère professionnelle. Le plus souvent, la Cour de cassation fait montre de tolérance vis-à-vis des employeurs, considérant que tout ce qui est stocké sur un appareil fourni par l'entreprise est présumé être professionnel, sauf mention explicite que le document est personnel ou privé »*, pointe Guillaume Bordier, notant cependant que *« le RGPD donne davantage d'armes au salarié pour attaquer l'employeur en cas de manquement »*.

> Les nouvelles formes d'organisation sont une porte ouverte sur des renseignements d'ordre privé.

Le RGPD explicite aussi la nature de ce qui peut être collecté : l'employeur ne peut traiter que ce qui lui est strictement nécessaire. *« Dans le cadre d'un processus d'embauche, par exemple, il n'est plus coutume de demander la carte d'identité ou le numéro de sécurité sociale du candidat. Le RGPD indique que l'entreprise ne peut conserver que les informations indispensables, et cela dans un cadre sécurisé et anonymisé »*, note David Luponis.

Autre mutation induite par le RGPD, l'instauration d'une culture de protection de la donnée personnelle, avec l'obligation de prendre des mesures techniques et organisationnelles. Au final, le RGPD responsabilise les entreprises. *« N'étant plus soumise au principe de déclaration auprès de la CNIL, l'organisation doit décider par elle-même quelles données elle va traiter, dans quel but, pendant combien de temps et comment, avec le risque de sanctions ou de poursuites en cas de non-respect du cadre légal »*, conclut Guillaume Bordier. — ***J. L. B.***

L'ANTICIPATION

Délivrer des solutions adaptées

Nicolas Spéciel/DPO Ucopia

NICOLAS SPÉCIEL

« Je dois sensibiliser nos équipes au nouveau cadre juridique. »

Ingénieur en informatique et télécoms, Nicolas Spéciel a rejoint Ucopia en 2012. Cette PME française, qui réalise 7 millions d'euros de chiffre d'affaires, est le leader européen de la gestion d'accès wi-fi et du marketing de proximité. Même si l'entreprise ne collecte pas de données personnelles pour son propre compte, elle conçoit des solutions qui permettent le traitement des informations relatives aux clients de ses partenaires, à savoir 15.000 organisations sur tous les continents.

Soucieuse de délivrer un outil conforme au RGPD dès son entrée en vigueur, la direction générale d'Ucopia a anticipé la nomination d'un délégué à la protection des données personnelles. Il y a un an, elle a donc choisi Nicolas Spéciel pour occuper le poste de DPO.

> Soucieux de délivrer un outil conforme au RGPD, Ucopia a anticipé la nomination d'un DPO.

Avant de piloter la conformité RGPD et de participer au développement de la nouvelle version de la solution, Nicolas Spéciel, trente-trois ans, avait précédemment occupé les fonctions de consultant spécialisé dans la gestion des produits et de consultant senior chargé de la formation technique. *« Le fait que je maîtrise les questions liées au produit, aux contraintes techniques et à la relation client ont motivé ma nomination, car cette fonction nécessite une vision transverse de la stratégie et de l'activité de l'entreprise »*, analyse le DPO d'Ucopia, précisant qu'il a dû monter en compétences sur l'aspect juridique. *« J'ai analysé le texte et lu beaucoup d'articles à son sujet, j'ai travaillé avec un cabinet juridique et j'ai rencontré des experts de la CNIL. »* Au quotidien, Nicolas Spéciel est non seulement en lien avec les équipes développement et qualité, mais aussi avec les fonctions support qui accompagnent les clients en quête d'outils conformes. *« Je dois sensibiliser nos équipes au nouveau cadre juridique et faciliter les démarches de mise en conformité de nos clients et partenaires »*, précise le DPO, qui fait des points réguliers avec le CEO. *« Didier Plateau, notre président, me fait part de l'orientation stratégique et je lui indique les différentes orientations conformes que peut prendre l'entreprise. Je suis un apporteur de solutions. »* — ***J. L. B.***

LA BONNE PRATIQUE

Coordonner le plan de conformité

DR

GUILLAUME TOLLET

« La conformité RGPD est également devenue un enjeu business. »

Diplômé d'une école de commerce (Skema) et féru de nouvelles technologies, Guillaume Tollet a d'abord passé cinq années au sein d'un cabinet de conseil en stratégie, puis cinq autres années en data et innovation chez Orange, et enfin deux années chez iProspect, l'agence de marketing digital du groupe japonais Dentsu. Fort de cette expertise protéiforme dans l'orientation stratégique et le digital, le jeune homme de trente-cinq ans a été nommé en janvier 2018, data protection officer (DPO) de Dentsu Aegis Network, groupe spécialisé dans la publicité et le marketing.

> Faire remonter au plus haut niveau les points d'alerte.

Son rôle en tant que DPO ? *« Il s'agit de transformer le RGPD en bonnes pratiques concrètes applicables dans toute l'organisation, cela en lien avec les objectifs de l'entreprise*, explique Guillaume Tollet. *Car la conformité RGPD ne relève pas seulement du juridique, c'est également devenu un enjeu business. »* Rattaché au président de Dentsu Aegis Network France, Thierry Jadot, et au président d'iProspect, Pierre Calmard, le DPO fait remonter au plus haut niveau les points d'alerte et pilote la conformité. *« Ma mission est également de sensibiliser et d'accompagner les 1.300 collaborateurs de la filiale française pour généraliser la prise de conscience sur l'importance des données personnelles »*, explique Guillaume Tollet. Concrètement, il coordonne un plan de conformité, cartographie les risques, liste les mesures correctrices et est associé en amont à des projets stratégiques.

« Gouvernance éthique de la donnée »

Avant sa prise de fonction, Guillaume Tollet s'est attelé à acquérir une fine maîtrise du RGPD, en fréquentant assidûment les forums et salons dédiés, et en suivant une formation spécialisée à Sciences Po Paris. *« Le cursus conduisant à l'obtention du certificat data protection officer permet de comprendre les tenants et les aboutissants d'une gouvernance éthique de la donnée »*, conclut le DPO de Dentsu Aegis Network France. — ***J. L. B.***