GÉRER LES CONTRAINTES SÉCURITAIRES LIÉES AUX DONNÉES PERSONNELLES

Dans le cadre du RGPD, entré en application en 2018, la sécurité des données est devenue un principe fondamental non négociable. Un coût pour les entreprises mais une opportunité pour les revendeurs.

Par Cécile Dard

Quand on a vu arriver le RGPD, nous avons eu peur. Mais c'est devenu une opportunité, car nous vendons des data centers sécurisés, et la loi a montré que la sécurisation des données est non seulement obligatoire, mais essentielle », **confie Harmony Barcatta, directrice adjointe marketing et communication de Xefi.** D'ailleurs, au sein de cette enseigne propriétaire de ses propres data centers, composée d'agences et de franchisés, on se réjouit de ces nouvelles réglementations qui obligent ses clients et l'ensemble des sociétés à contrôler les données des utilisateurs. *« Nous avons refait notre documentation pour expliquer pourquoi nous sommes* RGPD compliant. *Nous avons créé un contrat Data Protection assorti d'une panoplie complète d'offres de services dédiés »,* précise Harmony Barcatta, chez Xefi. Ces exigences règlementaires inédites, auxquelles les entreprises doivent s'adapter sous peine d'amende, constituent donc aussi un argument marketing. *« Être conforme est un avantage pour la communication, et cela encourage les entreprises à être en régularité »,* souligne Gamliel Bellahsen, expert en sécurité des données chez IBM.

OPPORTUNITÉS POUR LE CHANNEL

Les contraintes imposées par le RGPD ont donc changé les demandes et le comportement des clients devenus très scrupuleux dans la gestion et la préservation des données personnelles. *« Sur la partie protection, nous avons vu se multiplier les demandes de chiffrement des données,* explique Christophe Bardy, Solution Strategist, chez Nutanix. *Avant, peu de clients demandaient le chiffrement. Aujourd'hui, cette exigence est permanente, car personne ne veut que des données non chiffrées sortent de l'entreprise, en cas d'intrusion. Mais comme le RGPD n'oblige pas le chiffrement total, il faut savoir le gérer efficacement, en s'entourant des équipes compétentes. C'est une contrainte supplémentaire. »* Une obligation difficile à appréhender pour les entreprises qui manquent de discernement dans ce que le RGPD leur impose ou non, ce qu'experts, éditeurs, revendeurs et clients confirment à la lecture des contraintes légales. *« La confusion règne chez les clients en matière de réglementation. Le RGPD est compliqué pour des PME qui ont déjà du mal à comprendre comment gérer les cookies, quatre ans après le démarrage du Règlement,* constate Christophe Bardy, chez Nutanix. *Et la loi ne fournissant pas la recette de cuisine, c'est à chaque entreprise de définir quels processus l'amèneront à être conforme. Là, les intégrateurs ont un rôle à jouer. »* Selon ce spécialiste, les intégrateurs possèdent l'expertise pour traduire les processus fixés par la réglementation. *« L'intégrateur agit comme une courroie de transmission entre nous et les clients qui formulent un besoin métier. »* Quatre ans après, les sociétés sont, malgré tout, plus conscientes des changements qu'elles doivent opérer, grâce notamment aux actions de la Cnil. Mais elles ne possèdent pas encore toutes les clés.

PME ET GRANDS GROUPES INÉGAUX DEVANT LA LOI

Dans l'application et la gestion de la nouvelle règlementation sur la sécurité des données, les entreprises – de taille disparate – ne se battent pas à armes égales. *« Les grandes entreprises avaient commencé à travailler sur le sujet, avant le fameux 25 mai 2018, grâce à des moyens financiers et humains significatifs. En revanche, les plus petites structures ont pensé, au départ, que les grands groupes seraient les premiers touchés et contrôlés. À court terme, les PME ne se sont pas senti concernées, ni n'ont vu le retour sur investissement. Elles ne disposent pas non plus d'une armée de juristes pour se défendre en cas d'incident, contrairement aux grands groupes qui sauront faire diminuer les amendes »,* assure Gamliel Bellahsen, chez IBM. L'impact du RGPD est donc absorbé très différemment selon les changements que cela implique dans l'organisation de l'entreprise et ses process. *« Selon la taille de l'entité, c'est plus ou moins complexe. Elle peut se faire accompagner par des cabinets pour se mettre en conformité,* conseille Saikou Fall, Senior Consultant IT Security RGPD, chez TNP Consultant. *Pour les PME et TPE, un minimum d'exigences sont à remplir pour se placer sur une trajectoire de mise en conformité, en mettant, en premier lieu, l'accent sur les priorités. »* La sécurité des données est devenue un principe fondamental, en quelques années. Sur le terrain, le bilan est encore mitigé, mais le rapport aux risques semble avoir changé au sein des entreprises. *« Tout le monde a compris, car il n'y aura pas de protection des données personnelles sans sécurité des systèmes d'information »,* poursuit Saikou Fall. Du côté des utilisateurs, les manipulations sont encore trop complexes ou opaques pour un usager qui veut supprimer ses données, malgré la simplification préconisée par le RGPD. *« L'utilisateur n'a pas les moyens de vérifier la suppression réelle de ses données. La partie archivage où elles sont stockées est encore opaque,* note Gamliel Bellahsen, chez IBM. *Malgré la sensibilisation de chacune et chacun à ces problématiques ou au RGPD, quand ils arrivent sur un site internet, les utilisateurs cliquent sur le bouton OK, sans rien maîtriser. »*

DAVANTAGE DÉTERMINÉE, LA CNIL ENREGISTRE UNE HAUSSE DES PLAINTES ET DES AMENDES

Le nombre de plaintes auprès de la Cnil a augmenté de 27 % en 2019, soit 14 317 plaintes par rapport à 2018. Ainsi l'an dernier, sur 300 entreprises contrôlées par l'autorité administrative, 42 ont été mises en demeure, huit ont écopé d'une amende pour un total de 51,4 M€ environ (dont 50 M€ pour Google), cinq ont reçu une injonction sous astreinte, et deux ont bénéficié d'un non-lieu. Les grosses sanctions commencent aussi à tomber avec, par exemple, l'Ico *(Information Commissioner Office)* en Grande-Bretagne, qui a infligé une amende de 183 M£ à British Airways. *« La Cnil, elle, n'est plus clémente comme avant, y compris pour les TPE et PME,* alerte Harmony Barcatta, chez Xefi. *Toutes les semaines, la Cnil audite des sociétés dont certaines sont parfois dénoncées par les clients mécontents, surtout en B2C ».* Cependant, le contexte pourrait adoucir les sanctions : *« Beaucoup d'amendes infligées n'ont pas encore été payées, et la crise sanitaire ralentira les paiements »,* estime Gamliel Bellahsen, expert chez IBM. Mais pour Christophe Bardy, chez Nutanix, plus que les amendes, *« le pire, pour une entreprise, c'est l'intrusion puis l'extraction de téraoctets de données, et leur révélation sur la place publique. »*

« Nous avons créé un contrat Data Protection assorti d'une panoplie de services dédiés »

Harmony Barcatta, directrice adjointe marketing et communication, Xefi

UN MILLEFEUILLE LÉGISLATIF DIFFICILE À DIGÉRER

Le RGPD fait partie d'un dispositif législatif européen composé de plusieurs couches de sécurité. *« Ces règles de protection existent en France depuis 1978. Le RGPD apporte des nouveautés, mais les principes fondamentaux de la protection des données n'ont pas changé »,* rappelle Saikou Fall, chez TNP Consultant. En Europe, une série de règlements existent aussi pour les organisations spécifiques comme les OIV (opérateurs d'importance vitale), les hébergeurs de santé et les OSE (opérateurs de services essentiels), selon la Network Information Security de 2016. Certains cumulent les strates d'obligations. *« Il y a des limites à ce que l'humain peut gérer en matière de complexité. Le RGPD est une couche nécessaire, mais elle vient s'ajouter à d'autres,* souligne Christophe Bardy, chez Nutanix. *Ce millefeuille de réglementations en cascade pèse fortement sur l'IT. »* Et ce n'est pas fini, prévient Saikou Fall : *« Il existe l'*e-privacy, *en cours de négociation au niveau européen. Il est destiné à encadrer le commerce électronique et la vie numérique des citoyens, les cookies, etc. Il n'y a pas encore de date annoncée mais les propositions suscitent beaucoup de* débats. » À suivre, donc.

« La protection des données personnelles n'existera pas sans sécurité des systèmes d'information »

Saikou Fall, Senior Consultant IT Security RGPD, TNP

Suite du dossier p.118