VIE PRIVÉE

« Après quatre ans de RGPD, le travail reste immense »

Quatre ans après l'adoption du Règlement général sur la protection des données, la vie privée est-elle mieux protégée aujourd'hui qu'avant ? « Oui, mais… », estime le juriste Jacques Folon.

« Des organisations sont évidemment plus avancées que d'autres, mais je les mettrais au défi d'affirmer qu'elles sont totalement en règle », déclare le juriste Jacques Folon, professeur à l'école de gestion bruxelloise Ichec. © PIERRE-YVES THIENPONT.

ENTRETIEN

PHILIPPE LALOUX

Il y a quatre ans, l'Union européenne adoptait l'un des textes les plus marquants de son histoire : le Règlement général sur la protection des données (RGPD). Il entendait changer la vie des citoyens, des entreprises, des institutions, des autorités publiques. La vie privée serait désormais la valeur cardinale pour la marche du web. Est-ce vraiment le cas ? Si le bilan est « positif », il reste du chemin, estime le juriste Jacques Folon, professeur à l'école de gestion bruxelloise Ichec. Dans son ouvrage, *RGPD 2022. Traitement des données dans les organisations* (édité par Corporate Copyright), il propose un « guide de survie à l'usage des délégués à la protection des données », ces nouveaux maîtres du temple de la vie privée dont la mission est parfois synonyme de galère.

RGPD, flop ou top ? Quel bilan dressez-vous après quatre ans ?

Le bilan est globalement positif. Avant le RGPD, les entreprises sécurisaient vaguement leurs données, mais il n'y avait pas pressions dans ce sens, sauf peut-être, celle d'informaticiens qui se réveillaient quand il y avait une catastrophe. Ce règlement les oblige désormais non seulement à mettre en place des systèmes de sécurité de l'information, mais surtout à les documenter, ce qui n'est pas toujours le cas.

Est-ce qu'il a atteint ses objectifs ?

Des organisations sont évidemment plus avancées que d'autres, mais je les mettrais au défi d'affirmer qu'elles sont totalement en règle. Aussi parce qu'il s'agit d'un travail constant. On croit trop vite qu'il s'agit d'un *one shot*, or il faut en permanence se mettre à jour en fonction de nouveaux traitements de données.

Mais est-ce réaliste ? Cela semble tellement complexe, comme un Graal inaccessible… Votre ouvrage apparaît d'ailleurs comme une sorte de guide de survie.

Le souci, c'est qu'il y a plein de zones grises. Le RGPD donne des principes, mais ne dit pas comment les appliquer. L'idée était donc de reprendre les questions les plus courantes et de dire, concrètement : dans tel ou tel cas, je fais quoi ? Exemple : on est obligé de fixer une durée de conservation des données. Ce qui veut dit que l'on doit les détruire au bout d'un certain temps. Quid, donc, en matière de commerce électronique ? Après combien de temps doit-on détruire les données d'un client après son dernier achat ? Il n'y a pas nécessairement une loi qui le précise. Donc, il faut le décider. Ce guide donne donc une série de recommandations sur la base de cas pratiques.

Avec le RGPD est née une nouvelle fonction : *Data Protection Officer* (DPO)…

Souvent, les directions des organisations ne comprennent pas à quoi il sert. On le considère souvent comme un emmerdeur. J'ai voulu préciser comment on mettait ce rôle en place. Et rappeler, surtout, que la responsabilité finale d'un traitement de données revient au responsable de l'organisation, pas au DPO. Donc, si celui-ci est confronté à une direction qui n'en a rien à cirer, le DPO se contente de l'acter. Il y a beaucoup de démissions de DPO parce que, justement, ils en ont assez qu'on ne les écoute pas, qu'on ne les informe pas.

Pour les entreprises, le RGPD apparaît donc comme une vraie contrainte, notamment en termes de coûts…

Certains pensent qu'il suffit de publier une « *privacy policy* » (règles de confidentialité) sur leur site. Le problème est beaucoup plus vaste. Et, bien sûr, cela a un coût. Mais avoir une meilleure vision de ses données permet aussi d'éviter des amendes, et une perte de réputation, en cas de plaintes. Or, le nombre de plaintes augmente chaque année.

Certaines entreprises sont-elles plus à la traîne ?

En Belgique, il y a environ 700.000 numéros de TVA, dont la plupart sont des indépendants et des PME. Et là, il y a un souci. De nombreuses petites entreprises ne bougent pas. Et quand on regarde les offres proposées pour se mettre en conformité, très souvent, ce sont des cabinets d'avocats ou de conseil, mais qui coûtent jusqu'à 6.000 euros. Trop cher pour un indépendant.

Le RGPD, justement, a engendré la naissance d'une armée de consultants. Il y a un problème avec eux ?

Oui, dans la mesure où il n'y a malheureusement pas encore de certification, en tout cas en Belgique. Plein de gens se sont autoproclamés expert en RGPD, au terme d'une pseudo-certification. C'est parfois pathétique. Et source de conflits d'intérêts. Le DPO ne peut pas être, en même temps, responsable informatique, directeur marketing ou patron de l'entreprise. Pour les petites structures, c'est évidemment un souci en termes de coûts. C'est souvent quelqu'un qui fait ça en plus du reste.

Quid de l'Etat ? Serait-il le mauvais élève de la classe ?

Le SPF Finances a commencé très tôt à s'y intéresser, bien avant le RGPD. La plupart des services publics fédéraux ont des DPO compétents. Mais le travail reste immense. Le nombre de bases de données qu'ils gèrent est absolument gigantesque. Si la prise de conscience est réelle pour les grands acteurs du secteur public, ce n'est pas du tout le cas pour les petites structures. Les petits CPAS, les petites communes, les écoles, les bibliothèques…

contrôle « Le gouvernement avait oublié de créer l'Autorité de protection des données »

PH.L.

Depuis deux ans, on voit que le secrétaire d'Etat Mathieu Michel, en charge de la matière, et le Parlement, en charge de l'institution, se refilent la patate chaude

Jacques Folon

Juriste et professeur à l'Ichec

Les autorités de contrôle jouent-elles leur rôle ?

Structurellement, en Belgique, l'Autorité de protection des données (APD) est sous-staffée. Le parlement, en charge de l'APD, ne lui donne pas les moyens de travailler efficacement. En plus, il y a eu une série de conflits d'intérêts, d'incompatibilités légales et de souci de compétences relevés par la cour des comptes ou la Commission européenne. Il est essentiel de préserver l'indépendance de cette autorité, notamment par rapport au gouvernement, parce que le RGPD précise bien que dès qu'un texte de rang législatif concerne les données personnelles, il faut l'avis de l'APD.

Or, il faut rappeler un truc hallucinant : le gouvernement fédéral avait oublié de créer l'APD au moment où le RGPD est arrivé… Cela montre qu'il n'était pas vraiment concerné. Et quand le parlement a nommé ses membres, il y avait quatre hauts fonctionnaires qui en faisaient partie. Ce qui, indépendamment de leurs compétences, est totalement contraire au RGPD. Il a fallu un certain temps pour faire en sorte qu'ils s'en aillent. Et depuis deux ans, on voit que le secrétaire d'Etat Mathieu Michel, en charge de la matière, et le parlement, en charge de l'institution, se refilent la patate chaude. Rappelons que la Belgique était à deux doigts d'être citée devant la cour de justice européenne par la Commission, pour non-respect du RGPD, comme la Hongrie.

Quid de nos voisins européens ? Il y a une Europe à plusieurs vitesses en matière de protection de la vie privée ?

Oui, clairement. L'autorité belge, donc, ne fonctionne pas bien. L'Irlande, où siègent la plupart des géants du numérique, ne fait pas grand-chose. Heureusement, une décision de justice européenne permet aujourd'hui à une autorité nationale de s'emparer d'une plainte, indépendamment du siège social. D'autre part, les associations de consommateurs peuvent désormais attaquer directement n'importe quelle entreprise dans leur pays. Donc en clair, Test-Achats pourrait attaquer Facebook en Belgique, devant l'APD.

Et puis, il y a la CNIL (Commission nationale de l'informatique et des libertés) en France, où la loi Informatique et libertés existe depuis 1978. Même dans l'ADN des députés, on sait que la CNIL existe. Et quand elle rend un avis, ils en tiennent compte. Ils ont un staff très important. Ils sont actifs.

Le RGPD est-il prêt pour l'intelligence artificielle et le métavers ?

Le problème, ce sont les algorithmes. Ils s'auto-alimentent. Comment dès lors peut-on contrôler les traitements de données ? Normalement, la personne concernée par le traitement doit donner son consentement libre et éclairé. Mais c'est compliqué d'expliquer ce que l'algorithme va faire avec ses données. A priori, le RGPD s'applique aux algorithmes. Mais donc, dans ce cas, la réflexion sur les questions de vie privée (quelles données on collecte, combien de temps on les garde…) doit se faire en amont du produit. C'est le principe de « *privacy by design* ». Or, malheureusement, ce n'est pas toujours le cas. Bien souvent, le programme est lancé. Et le DPO (*Data Protection Officer*) l'apprend après.

Les autorités ont-elles appliqué ce principe de « *privacy by design* » pour la gestion de la crise covid ?

Le RGPD impose de réaliser des analyses d'impact lorsque l'on collecte des données. Est-ce que les mesures de sécurité prévues pour protéger les données sont suffisantes ? Et là, très clairement, on s'est retrouvé dans un certain nombre de cas où cette analyse de risques n'a pas été faite. Je prends l'exemple de Bruvax où, si je disposais du numéro national d'une personne, je pouvais accéder à son statut vaccinal. Ce principe n'a pas été respecté.

RGPD 2022
JACQUES FOLON
Ed. Corporate Copyright, 272 p, 45 €, ebook 39,99 €