LE TEXTE EUROPÉEN VA SOUFFLER SA PREMIÈRE BOUGIE

Un an de RGPD : les données sous contrôle ?

Le règlement général sur la protection des données (RGPD) a fait transpirer les départements juridiques et informatiques des entreprises. Pour quels résultats ? **GILLES QUOISTIAUX**

En mai 2018, le règlement européen sur la protection des données (RGPD) entrait en vigueur. L'objectif de cette législation est de mieux protéger les données personnelles des citoyens, consommateurs et travailleurs. Les entreprises ont été contraintes de revoir leurs processus internes de stockage et d'utilisation de leurs bases de données. En un an, ce texte majeur a bousculé les habitudes dans les entreprises, donné des cheveux blancs à certains directeurs juridiques et commencé à inspirer des législations au-delà des frontières européennes. Premier bilan en sept questions.

1. Les entreprises sont-elles en ordre ?

Il y a un an, à l'approche de la date fatidique d'entrée en vigueur du RGPD, c'était l'effervescence dans les directions juridiques des entreprises. Il faut dire que le texte a bénéficié d'une publicité rarement atteinte par une législation européenne. Un battage alimenté notamment par les consultants, qui ont multiplié les offres de formations et de modules de mise en conformité.

Peu d'entreprises sont passées à côté du sujet. « Les grandes entreprises s'y sont certainement prises à temps. Mais les sociétés de toutes tailles ont réagi et se

GETTY IMAGES

sont progressivement mises en ordre », souligne Stéphanie De Ridder, avocate chez Reliance. Dans sa pratique, l'avocate a constaté un gros pic des sollicitations aux alentours de mai 2018 : « A l'époque, je ne faisais que cela. Les demandes ont progressivement diminué. On est maintenant plutôt sur des questions de routine ».

Parmi les plus petites entreprises, certaines ont cependant renoncé à se mettre en ordre : « La charge administrative est énorme pour les petites structures », reproche Nathalie Ragheno, conseillère juridique à la FEB. Cette spécialiste estime aussi que l'inaction de l'Autorité de protection des données (*voir plus loin*) a convaincu certaines entreprises qu'elles ne risquaient rien : « Nous conseillons à toutes les entreprises de se mettre en conformité, poursuit Nathalie Ragheno. La première étape est de rédiger le registre des activités de traitement. » Ce document interne répertorie les bases de données que possède l'entreprise et détaille l'usage qui en est fait. C'est la pierre angulaire du système de contrôle mis en place par le RGPD.

2. Le RGPD a-t-il coûté cher aux entreprises ?

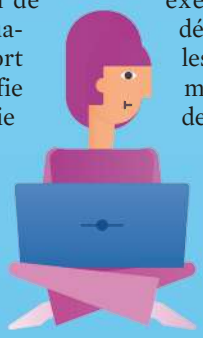
D'après une étude réalisée par le consultant EY avant l'entrée en vigueur du texte, le RGPD risquait de coûter 7,8 milliards de dollars aux entreprises du « Global 500 », les 500 plus grandes entreprises du monde. Les coûts liés au RGPD se répartissent entre les coûts humains (engagement d'un ou plusieurs spécialistes, temps passé par le personnel sur la mise en conformité, frais de consultance, etc.) et les coûts d'infrastructure (protection informatique). « C'est un coût astronomique pour les grandes entreprises, réagit Nathalie Ragheno. Chez Total, par exemple, ils ont dû engager huit consultants à 1.000 euros par jour pendant trois ans ! »

Pour les PME, le choix s'est souvent porté sur des modules vendus par des sociétés spécialisées comme OneTrust, qui proposent des packages en ligne permettant de se mettre dans les clous du règlement européen. Les plus petites entreprises ont fait appel à des consultants. « C'est un texte qui engendre plus de contraintes que de retombées positives immédiates, il a donc été vu par certains comme une réglementation qui risquait de tuer leur business. Mais souvent, le processus de mise en conformité n'est pas si compliqué que ça, rassure Damien Jacob, consultant chez Retis. Le texte est finalement assez judicieux et logique. On arrive toujours à trouver des solutions simples. Acheter un pare-feu à 20.000 euros, c'est rarement utile pour une petite société. Il vaut mieux adapter les processus internes pour éviter les erreurs humaines, qui sont les causes principales des fuites de données. »

3. L'arsenal législatif belge est-il prêt ?

Si le règlement est en soi directement applicable en Belgique, certaines mesures nécessitent une adaptation dans notre arsenal législatif. Deux lois ont vu le jour dans la foulée du RGPD. La dernière date de septembre dernier : « Cette loi est énorme et complexe, elle compte plus de 200 articles », commente Axel Beelen, consultant juridique et auteur du *Guide pratique du RGPD* (éditions Bruylant). Complexité institutionnelle oblige, la Belgique a réparti les compétences de contrôle entre plusieurs autorités. Outre l'autorité fédérale (APD) responsable dans la plupart des cas, des autorités régionales ont été créés, et certaines matières spécifiques comme les questions de police ont été confiées à d'autres entités : « Il faudra des accords de coopération pour régler d'éventuels conflits de compétence », soupire Axel Beelen.

Un point particulier de la loi fait par ailleurs l'objet d'un recours devant la Cour constitutionnelle. La Belgique a exonéré les pouvoirs publics d'éventuelles amendes administratives en cas d'infraction au RGPD, ce qui est loin de plaire à la FEB : « C'est une situation discriminatoire par rapport aux entreprises, qui ne se justifie absolument pas, pointe Nathalie Ragheno. C'est aussi un mauvais signal de la part des autorités publiques. Nous estimons qu'elles doivent se sentir tout autant concernées que les entreprises, qui risquent des amendes importantes ». Les sanctions peuvent atteindre 20 millions d'euros ou 4 % du chiffre d'affaires.



4. L'Autorité de protection des données est-elle opérationnelle ?

Les nouveaux directeurs de l'Autorité de protection des données (APD) viennent seulement d'entrer en fonction. La faute, notamment, à des exigences linguistiques très élevées qui ont retardé l'engagement d'un responsable maîtrisant l'allemand. Résultat : l'APD, qui succède à la Commission vie privée, n'a pas pu fonctionner à plein régime pendant presque un an. Le nouveau directeur, David Stevens, passé par Telenet et Nielsen, veut appuyer sur l'accélérateur : « L'époque du *sit back and relax* (*de se reposer sur ses lauriers, Ndlr*) est révolue », a-t-il déclaré à nos confrères du *Tijd*.

Pour l'APD, il reste énormément de travail à rattraper. Depuis l'entrée en vigueur du RGPD, la structure publique, qui occupe une soixantaine de personnes, n'a pas infligé une seule amende. Dans le même temps, ses alter ego européens n'ont pas chômé. En France, la CNIL (Commission nationale de l'informatique et des libertés), souvent présentée comme l'une des autorités les plus organisées et avancées, a déjà frappé à plusieurs reprises, notamment contre Google et Dailymotion. En Grande-Bretagne aussi, les manœuvres ont commencé, avec des sanctions contre Uber, Google, Yahoo !, Facebook, etc.

L'autorité belge devra mettre les bouchées doubles pour instruire les plaintes, mais aussi pour activer son service d'inspection, chargé de contrôler le respect du RGPD par les entreprises. Ces dernières savaient qu'elles ne risquaient pas grand-chose jusqu'à présent. Cela pourrait changer, mais vu la masse de travail que cela représente, l'APD va devoir établir des listes de priorités. En France, par exemple, la CNIL a notamment décidé de centrer ses contrôles sur les données relatives aux mineurs, mais aussi sur la délicate question de la répartition des responsabilités entre les entreprises et leurs sous-traitants en cas d'échange de données.

L'APD n'est pas seulement le gendarme du secteur. L'autorité est également censée conseiller les entreprises, ➤

les indépendants et les entrepreneurs dans le processus de mise en conformité au RGPD : « L'autorité doit assurer l'accompagnement des PME. Elle ne peut pas se contenter de brandir le bâton », estime Damien Jacob, consultant chez Retis. Dans d'autres pays, de véritables *guidelines* ont été mis sur pied pour aider les petites structures à se mettre en ordre. On les attend toujours en Belgique.

5. Le « data protection officer », une nouvelle espèce rare ?

En vertu du RGPD, certaines sociétés, a priori les plus grandes, ont dû embaucher un *data protection officer* (DPO). Ce responsable de la gestion des données est un juriste ou un informaticien. De nombreuses formations, organisées à la Solvay Brussels School ou à l'Ichec par exemple, sont apparues pour donner des outils à ces nouveaux profils, de plus en plus demandés.

Chez Lexgo, le site internet de référence pour les offres d'emploi juridiques, les annonces pour les spécialistes de la protection des données ont explosé. Depuis 2016, le nombre d'offres d'emploi pour ce type de profil a été multiplié par deux ou trois chaque année. Ils représentent désormais entre 4 % et 7 % des offres sur Lexgo, ce qui est une proportion significative, d'après Hugo De Martelaere, responsable de la plateforme. « Alors qu'il s'agissait au départ principalement d'offres pour des consultants externes ou des avocats, nous constatons qu'il s'agit désormais à 70 % d'offres pour des juristes en interne », précise ce spécialiste du recrutement. Selon Hugo De Martelaere, la demande est forte au point que certaines entreprises recrutent désormais un deuxième DPO. Mais il n'y a pas encore de signe de pénurie.

6. Les géants du Net doivent-ils trembler ?

Les grandes plateformes internet sont les cibles principales du RGPD. Des entreprises comme Google ou Facebook ont basé leur *business model* sur la valorisation des données personnelles à des fins publicitaires. Les autorités européennes souhaitent encadrer cette collecte effrénée. Avec le RGPD, elles ont donné une nouvelle arme aux Etats membres.

PG

STÉPHANIE DE RIDDER (RELIANCE)
« On est maintenant plutôt sur des questions de routine. »

PG

NATHALIE RAGHENO (FEB)
« Un coût astronomique pour les grandes entreprises. »

PG

AXEL BEELEN (GUIDE PRATIQUE DU RGPD)
« Le California Consumer Privacy Act est une sorte de RGPD version light. »

La CNIL, l'autorité de protection des données française, s'en est saisie dès janvier dernier, gratifiant Google d'une amende de 50 millions d'euros pour « manquement à ses obligations de transparence et d'information vis-à-vis de ses utilisateurs ». Cette amende majeure ne représente pas grand-chose pour une multinationale qui réalisait en 2018 un chiffre d'affaires de 136 milliards de dollars. Mais c'est indéniablement un premier coup de semonce.

Parallèlement, Google a d'ailleurs annoncé son intention de rapatrier en Irlande la gestion des données de ses clients européens. L'idée de l'entreprise est de se soumettre à l'Autorité de protection des données irlandaise, réputée plus laxiste que ses coreligionnaires européens. « Les grandes entreprises cherchent des *data paradises* pour tenter d'échapper aux amendes. Mais l'étau se resserre », commente Thomas Faelli, avocat spécialisé en protection des données chez Ethikos Lawyers.

7. Le RGPD fait-il des émules ?

Le nouveau règlement a fait parler lui au-delà des frontières européennes. En Californie, une législation similaire entrera en vigueur dans les prochains mois. Le *California Consumer Privacy Act* est une sorte de « RGPD version light », schématise le consultant juridique Axel Beelen. Particularité californienne : le texte prévoit des peines de prison pour les CEO qui contreviendraient à ses dispositions.

Signe que les temps changent aux Etats-Unis, Facebook s'attend aussi à subir les foudres de la Federal Trade Commission, le régulateur du commerce, suite au scandale Cambridge Analytica. Pour rappel, cette société contrôlée par des proches de Donald Trump a collecté, dans des circonstances troubles, les données personnelles de dizaines de millions de profils Facebook d'Américains afin de les bombarder de *fake news* au cours de la dernière campagne présidentielle. Dans cette affaire de fuite de données pour laquelle le CEO Mark Zuckerberg s'est excusé à de nombreuses reprises, Facebook a provisionné la bagatelle de 3 milliards de dollars. L'entreprise s'attend à une sanction record, représentant entre 3 % et 9 % de son chiffre d'affaires. Le GDPR semble bien faire des émules. ⊙