L'Europe risque de ne pas être prête à temps pour garantir la protection des données

▶ Il reste à peine plus de 100 jours avant l'entrée en vigueur du règlement européen sur la protection des données.
▶ Mercredi, la Commission européenne a tiré la sonnette d'alarme car « 26 pays sont dans l'urgence ».

L'intervention de la Commission, ce mercredi, visait à prendre les États et les entreprises par la main dans l'espoir qu'ils accélèrent la cadence. Car dans moins de 100 jours, le règlement européen sur la protection des données (RGPD) entre en vigueur. Une enveloppe de 3,7 millions d'euros est par ailleurs disponible pour les aider dans cette transition. Si l'Allemagne et l'Autriche sont fin prêtes, l'Italie inquiète particulièrement, puisqu'elle n'est venue à aucune des treize réunions préparatoires à l'entrée en vigueur du texte.

Puisque c'est un règlement, la plupart des dispositions seront applicables automatiquement dès le 25 mai prochain. Mais les pays européens doivent tout de même introduire plusieurs changements législatifs, notamment pour doter leur organe de protection de la vie privée de nouveaux pouvoirs, comme celui d'imposer des amendes aux entreprises allant jusqu'à 4 % de leur chiffre d'affaires mondial (voir ci-contre). Mais quels sont les enjeux de ce texte ?

1 Pourquoi ce règlement Le RGPD a été âprement négocié pendant quatre ans et fortement marqué par l'affaire Snowden, où le monde a découvert que les Américains faisaient de l'espionnage à grande échelle grâce à Internet.

Dans une société toujours plus connectée (le Belge passe en moyenne 4 heures par jour à surfer), le règlement permettra de renforcer les droits de consommateurs dans le traitement de leurs données personnelles. *« Nos règles dataient d'il y a 23 ans. D'un point de vue technologique, c'était une période préhistorique »*, a expliqué la commissaire aux Consommateurs et à la Justice Vera Jourova.

La Commission européenne estime que la valeur des données personnelles des citoyens européens pourrait atteindre près de 1.000 milliards d'euros par an d'ici 2020. Un marché juteux puisque nos données sont monétisées, alors que les utilisateurs n'ont pas toujours conscience de ce qu'Internet sait de nous ou ce qu'il fait de ces informations.

Rien qu'un rapide test avec Facebook est éloquent. Dans l'onglet « Préférences publicitaires », un utilisateur peut découvrir l'ampleur de ce que le réseau social sait sur lui et à quel type de consommateur il l'assimile. Cela va de ses centres d'intérêt, à la marque de son smartphone, en passant par sa messagerie électronique ou son supermarché de prédilection, son fournisseur de gaz, s'il est « proche des expats », ou encore si c'est un acheteur actif.

2 Ce que le RGPD prévoit Le RGPD prévoit qu'une personne aura le droit à s'opposer à tout moment au partage de ses données et à son profilage à des fins commerciales. Ce droit devra « explicitement être porté à l'attention » des utilisateurs.

Le RGPD introduira plus généralement donc la notion de consentement non ambigu qui devra se traduire par « un acte positif clair ». Concrètement, cela pourrait se faire en cochant une case lors de la consultation d'un site internet ou par tout comportement *« indiquant clairement que dans ce contexte, la personne concernée accepte le traitement proposé de ses données à caractère personnel »*, dit le règlement. Un silence, des cases cochées par défaut ou l'inactivité ne pourront pas être prises pour un consentement. Les paramètres « par défaut » des sites web devront toujours être les plus favorables à la protection de la vie privée.

Le texte introduit des dispositions encore plus strictes (le consentement « clair ») en ce qui concerne les données relevant de « l'origine ethnique, les opinions politiques, religieuses » ou l'orientation sexuelle d'une personne.

Le droit à l'oubli très médiatisé dans l'affaire Google ne sera quant à lui pas inconditionnel, afin de protéger la liberté d'expression et d'information. Un politicien, par exemple, ne pourra pas voir ses déclarations rayées du net. Un internaute pourra par contre demander que ses données soient effacées si elles ne sont plus nécessaires à l'objectif spécifique pour lequel il a donné son consentement, par exemple s'il n'utilise plus un service.

Le RGPD introduit l'obligation pour les entreprises d'avertir dans les 72 heures leurs utilisateurs et les autorités d'un piratage de leurs données. La commissaire a rappelé le cas d'Uber, qui a caché pendant un an à près de 60 millions d'utilisateurs le piratage de leurs données, ou le cas des poupées Cayla en Allemagne, détournées par des hackers pour espionner les enfants.

Enfin, pour l'anecdote, une proposition législative visant à soumettre les institutions européennes à des règles similaires à celles du RGPD peine à faire l'objet d'un accord. Ce qui signifie qu'elles-mêmes risquent de ne pas être prêtes à temps pour le 25 mai. ■

ELODIE LAMER

ET LA BELGIQUE ?

Encore une loi à préparer

« *Je n'ai rien entendu d'alarmant* » au sujet de la préparation de la Belgique à l'entrée en vigueur du RGPD, nous a assuré la commissaire à la Justice, Vera Jourova. La Belgique a adopté, en novembre 2017, la réforme de la commission de la vie privée. Cet organisme consultatif doit devenir, pour le 25 mai, un véritable régulateur indépendant capable d'imposer de lourdes sanctions. Elle s'appellera alors l'autorité de protection des données.

Si le RGPD est plutôt prescriptif en ce qui concerne les obligations imposées aux entreprises privées en matière de traitement des données, il laisse plus de flexibilité aux pays européens pour celles qui incombent au secteur public. Au cabinet de Philippe De Backer, secrétaire d'État à la Protection de la vie privée (VLD), on nous indique être en train de rédiger une loi qui permettra au service public de se mettre en conformité. La Belgique estime donc être dans la bonne voie pour être en règle à temps sur tous les aspects du règlement.

E.LR

PROXIMUS

Des conséquences sur la manière de fonctionner

Chez Proximus, l'échéance du 25 mai ne semble pas avoir initié un branle-bas de combat. L'opérateur télécoms assure avoir pris de longue date la mesure de l'enjeu du futur RGPD. Un groupe de travail d'une cinquantaine de personnes a été érigé dès la mi-2016, dont la structure est en partie virtuelle : « *Le texte génère des conséquences sur la manière de fonctionner de l'entreprise à de multiples niveaux* », commente Haroun Fenaux, porte-parole. « *Des centaines de procédures de collecte et de traitement des données ont été revues afin de nous assurer de leur conformité. Tous les nouveaux projets, par exemple, son screenés d'un point de vue "privacy" (vie privée, NDLR).* »

Il y a les procédures, mais aussi le « business ». Autrement dit : ces nouvelles règles, sensées être plus restrictives, plus protectrices, vont-elles impacter les relations avec les clients ? « *Ce n'est pas l'objectif* », poursuit le porte-parole. « *Nous n'allons pas arrêter d'être à l'écoute de nos clients afin de leur proposer des services de plus en plus personnalisés. L'élément crucial, ce sera le consentement du consommateur.* »

Cette étape franchie, l'opérateur ne perçoit pas de changements majeurs dans son activité. Des modifications de procédures, certes, pas de la stratégie en tant que telle...

B.J.

business model La base, c'est la donnée

Si quelque chose est gratuit, le produit, c'est vous. Cette loi régit le développement de l'économie numérique depuis le précambrien d'internet. Son corollaire, c'est la pub, modèle d'affaires par défaut et péché originel du web, qui a permis de financer l'innovation technologique, d'incuber des millions de start-up et de bercer 3,8 milliards de Terriens dans la douce illusion de surfer aux frais de la princesse. Le deal est clair (ou pas) : « *Je te donne mes données, tu les exploites et, en échange, je profite de tes services.* »

« *Une fois que nous avons supposé que la publicité est le modèle d'affaires par défaut de l'internet, l'étape suivante est évidente : nous avons besoin de plus de données pour créer des annonces ciblées qui semblent plus efficaces* », explique Ethan Zuckerman, directeur du Centre pour les Médias Civiques du Massachusetts Institute of Technology, dans une tribune pour *The Atlantic*.

Prenons un exemple au hasard : Facebook. Soit 2 milliards d'« amis » qui, sans même être sur le site, déversent leur intimité dans les serveurs du réseau social : les sites visités, leurs photos, leurs « *like* », leurs amis, leurs vacances, leur resto préféré, leur liste de courses, leur bulletin de santé (via leur montre connectée) et, par magie algorithmique, leurs intentions de vote... Et c'est encore pire si un « ami » parle de vous.« *Je dis souvent que Google possède plus de photos de moi que ma femme n'en possède* » ironise Bruce Schneir, un des « gourous » mondiaux de la sécurité, principal conseiller d'IBM.

Et donner, c'est donner. L'ogre stocke religieusement la moindre trace de vie numérique dans ses serveurs, sans jamais en effacer aucune (même si vous tentez de les supprimer dans vos paramètres). En 2011, alors que les aspirateurs à données de la Sillicon Valley n'étaient encore que des enfants de chœur, un étudiant autrichien, Max Schrems, a eu la surprise de recevoir un document de 1.222 pages après avoir réclamé ses données à Facebook.

« *La vie privée est un concept qui se négocie* »

ANTONIO CASILLI ET PAOLA TUBARO

Fin novembre 2017, le site au F bleu affichait un bénéfice trimestriel de 10,14 milliards de dollars (8,7 milliards d'euros), dont 88 % proviennent de la publicité (ciblée) sur mobile. Merci qui ? Les utilisateurs qui, à la grosse, louche, lui ont chacun rapporté 5 dollars. « *Ce bénéfice représente la différence entre la valeur de notre vie privée et le coût des services que nous recevons en échange* », estime Bruce Schneier.

Une étude menée au Royaume-Uni par l'agence Ebuzzing estimait en 2014 que les internautes devraient débourser chaque année 170 euros pour profiter de tous les contenus en ligne sans publicité. C'est là qu'est l'os, bien entendu, mais pas seulement. Sans partage de données, pas de personnalisation, pas d'expérience utilisateur « sur mesure », pas d'objets connectés avec lesquels nous créons autant d'interactions que de traces sur nos modes de vie et de pensée. Le surf en mode silencieux (comme le propose par exemple le navigateur web « Tor »), s'apparente plus à un parcours du combattant, laborieux et poussif. Un peu comme si Spotify ne proposait que du « heavy metal » à un fan d'Ella Fitzgerald. Le cadre législatif en cours de gestation se joue sur cet équilibre fragile entre croissance économique, expérience utilisateur et protection de sa vie privée.

« *La vie privée est un concept qui se négocie* » expliquent Antonio Casilli et Paola Tubaro, chercheurs, dans une tribune parue dans *Le Monde* de mercredi. Elle est « *surtout une négociation collective, une concertation entre plusieurs parties afin de définir des obligations réciproques et d'organiser une relation. Cette relation peut être conflictuelle.* » Car il n'y a désormais rien de plus collectif qu'une donnée personnelle... ■

PHILIPPE LALOUX

l'expert « Il y a une interrogation : l'Europe va-t-elle participer au big data ? »

ENTRETIEN

En matière de protection des données privées, Peter Swire est une pointure. Celui qui enseigne aujourd'hui la « cybersecurity and privacy » à l'université de Georgia Tech a notamment officié par le passé comme conseiller en chef sur la vie privée de l'administration Clinton. Il a également travaillé pour l'administration Obama. Il était de passage à Bruxelles cette semaine, à l'occasion de la conférence « Computers, Privacy, and Data Protection ». L'occasion d'aborder avec lui le nouveau règlement européen sur la protection des données (RGPD). Quand il a négocié fin des années 90 avec l'Union européenne l'accord Safe Harbor établissant les standards d'échange de données entre entreprises européennes et américaines, se rappelle-t-il, *« l'approche était la bonne : elle permettait à l'Europe de maintenir ses règles de protection des données, et quand celles-ci migraient vers les Etats-Unis, les compagnies américaines étaient tenues de respecter les standards européens. »* Il se réjouit donc que ce concept de base ait été repris dans le RGPD.

Comment le nouveau règlement européen va-t-il affecter l'économie des datas, les données sur le web ?

L'Europe a fait ses choix. Les Etats-Unis et la Chine sont les deux endroits du monde qui ont le plus développé le big data. L'Inde veut s'y mettre. Ces pays considèrent que quand vous récoltez une masse importante de données sur un large spectre, vous apprenez des choses au niveau de la recherche médicale, du business, du terrorisme, etc. Mais pour être en mesure d'analyser du big data, cela nécessite... des données ! Il y a donc une interrogation : l'Europe va-t-elle participer au big data ? L'interprétation qui sera faite du RGPD sera très importante. Il s'agira soit de trouver des méthodes pour faire du big data en respectant les nouvelles règles, soit d'interdire tout simplement le big data. Ce n'est pas clair à ce stade. L'autre grande décision concernera l'internet des objets et les smart cities. Dans les smart cities, il y aura nécessairement énormément de capteurs, comment va-t-on, avec le RGPD, gérer la collecte des données personnelles ? Si je marche dans les rues d'une ville, il est difficile pour moi de donner mon consentement à tous les capteurs. Comme pour le big data, il y a ici un choix fondamental pour l'Europe de savoir si l'internet des objets est légal ou pas.

Quelles seraient les conséquences d'une application stricte du RGPD ?

Elles seraient substantielles. Pour l'Europe, il y a le risque que la récolte des données personnelles soit souvent interdite. Et que les compagnies européennes qui veulent utiliser le big data et l'internet des objets se retrouvent dans la difficulté d'innover. Les personnes qui soutiennent la protection des données affirment que les entreprises européennes vont dès lors innover dans le domaine de la protection de la vie privée, justement. Dans certains secteurs, cela pourrait s'avérer. Mais je ne pense pas que vous puissiez collecter peu de données et gagner la bataille du big data.

Cela aurait aussi des conséquences en matière de sécurité ?

En matière de cybersécurité, l'analyse des adresses IP des ordinateurs qui se connectent aux sites internet d'une administration ou d'une entreprise est très importante. Or, le RGPD estime qu'une adresse IP est une donnée privée. Il est donc important de clarifier si le partage des adresses IP est autorisé ou pas sous le régime du RGPD. C'est vital. Sans quoi, cela compliquerait grandement les choses en matière de cybersécurité.

Vous plaidez donc pour qu'un maximum de données, y compris privées, puissent être récoltées ?

Non. Mais ces choix doivent être posés avec beaucoup de prudence. Parfois, aux Etats-Unis, on utilise trop les données privées, sans structures de protection suffisantes. Mais en Europe, les règles sont parfois trop strictes. En Europe, en matière de données privées, l'analyse juridique est souvent faite sur base des textes des droits fondamentaux. De mon côté, j'estime que les lois doivent émaner de constats empiriques et de jugements pragmatiques, et pas uniquement des textes fondamentaux. ■

Propos recueillis par
CORENTIN DI PRIMA