RGPD : la bataille des données personnelles en Europe a commencé

Le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) prendra effet dans l'ensemble des pays de l'Union. Sera-t-il capable de contenir l'appétit des GAFA pour nos données personnelles ? Il en a déjà changé la nature.

Qu'est-ce une donnée personnelle ?

Toute information associée explicitement à un individu, c'est-à-dire une personne physique, est une donnée à caractère personnel. On ne parle pas de données personnelles pour une personne morale. Ainsi, le nom, le numéro de la carte d'identité ou l'adresse sont des données personnelles. Une adresse IP de connexion internet n'en est une que si elle renferme un moyen d'identifier son utilisateur. On parlera de données « anonymisées », lorsque de telles informations ont été supprimées. Ainsi, on conservera le code postal des personnes plutôt que leur adresse complète, un intervalle d'âge plutôt que leur date de naissance.

Les données personnelles ont une valeur

La criticité des données (*data* en anglais) varie selon leur type. Les identifiants de connexion et mots de passe, les numéros de cartes bancaires sont évidemment les cibles privilégiées des pirates. Les données à valeur probante, présentes sur les justificatifs d'identité, de domicile ou de revenus servent pour les démarches administratives ou commerciales. Leur diffusion incontrôlée peut conduire à des usurpations d'identité. On estime à 200 000 le nombre d'usurpations d'identité chaque année en France, même si une majorité d'entre elles est réalisée à partir de supports non-numériques. Les données médicales regroupent les prescriptions, les résultats d'examen, l'histoire vaccinale et opératoire des patients. Elles sont régies par le secret médical. Les données à caractère commercial se limitent souvent aux informations sur les ventes, la date et le lieu de l'achat, l'identifiant ou le nom du client, le détail des achats, les montants dépensés. Mais les données comportementales ayant un intérêt commercial couvrent tout le spectre imaginable : du dernier livre que vous avez lu à votre lieu de villégiature préféré, de votre couleur favorite au trajet que vous avez effectué dans les rayons d'un supermarché. Enfin, le contrôle des données privées est à la fois un enjeu de sécurité crucial dans un contexte international tendu, et aussi une question démocratique forte. Les autorités judiciaires des Etats doivent avoir accès aux informations sur certains individus, conformément à la loi. D'un autre côté, cette surveillance ne peut pas se faire à n'importe quel prix. Ainsi, pour Edward Snowden, « lorsque vous dites 'le droit à la vie privée ne me préoccupe pas, parce que je n'ai rien à cacher', cela ne fait aucune différence avec le fait de dire 'Je me moque du droit à la liberté d'expression parce que je n'ai rien à dire', ou 'de la liberté de la presse parce que je n'ai rien à écrire'. ». Les données personnelles de leaders d'opinions, d'hommes politiques, de journalistes, de responsables syndicaux, de dirigeants d'entreprises sont donc un enjeu démocratique voire un sujet de sécurité nationale.

Le Règlement Général de Protection des Données

Après la Loi française Informatique et libertés de 1978, puis la directive européenne de 1995 sur la protection des données personnelles, le RGPD constitue une nouvelle étape très importante. Tout

d'abord, à la différence des directives (dont celle de 1995) qui se déclinent en lois nationales avec les biais que l'on peut craindre, ce règlements'applique immédiatement dans tous les Etats-membres, sans modification. Il concerne également toutes les entreprises extra-européennes gérant des données personnelles de citoyens européens. Celles-ci doivent choisir une autorité nationale de protection des données (la CNIL pour la France) qui leur servira de référent.

Cette nouvelle réglementation conditionne l'accès aux données personnelles d'un individu à son accord explicite et libre (*opt-in* en anglais). Autrement dit, la demande doit être formulée clairement, en présentant les données concernées (accord explicite). Elle ne peut pas être la condition à la fourniture d'un service (accord libre). Ainsi, les téléchargements d'application sur GooglePlay ou AppStore devraient être rendus possibles même si l'utilisateur a refusé de donner l'accès à ses données.

Le profilage est interdit. L'accès à un service ne peut dépendre d'un traitement automatique. L'historique de paiement ne peut être un argument pour refuser un service à un futur client, sauf exception.

Les citoyens ont le droit d'accéder à leurs données personnelles, détenues par une administration ou une entreprise.

Le droit à l'oubli est pérennisé sous la forme d'un droit à l'effacement. On peut demander l'effacement de données à caractère personnel pour des motifs précis.

Le droit à la portabilité est également pérennisé : un fournisseur de services ne pourra refuser de transférer les données commerciales d'un client vers un autre fournisseur, dès lors que le client le demande.

Toutes les entreprises autres que les entreprises unipersonnelles disposent de données personnelles. Si ce ne sont pas celles de leurs clients, elles doivent au moins protéger celles de leurs salariés. Le RGPD leur impose un ensemble d'obligations :

- Ces données personnelles doivent être protégées dès la conception d'une nouvelle base de données (*protection by design*)
- Tout nouveau projet doit faire l'objet d'une étude d'impact sur la vie privée des personnes concernées
- Tout système d'information doit comporter des mesures de sécurité (*security by default*)
- Un responsable de la protection des données doit être nommé (*Data Protection Officer*) dans des organismes publics ou bien dans des entreprises manipulant de grandes quantités de données personnelles. Il a en charge la coordination des actions de ce domaine. Le responsable d'un traitement informatique (en général le chef de projet informatique) demeure néanmoins l'unique responsable de la mise en œuvre de mesures de protection des données
- Dans le cas d'une fuite de données accidentelle ou malveillante (*data leak*), les entreprises sont tenues d'informer les clients détenteurs de ces données dans un délai de 72 heures, sous peine de sanctions
- En cas de manquement aux obligations précédentes, l'amende peut aller jusqu'à 4% du CA consolidé mondial de la société. C'est là encore une nouveauté très importante, après des montants de sanctions jusqu'à présent trop faibles pour dissuader les gros acteurs de n'en faire qu'à leur tête.

L'ambiguïté de certaines dispositions

La protection des données personnelles percute parfois d'autres obligations. Ainsi, les banques qui se doivent légalement de « connaître leur client », à des fins de lutte contre le blanchiment notamment,

n'ouvriront pas de compte à un client qui refuserait de donner des pièces justificatives. Pourtant, celui-ci pourrait invoquer le consentement libre du RGPD pour obtenir le service.

De la même manière, des organismes de prêt ont recours à des sociétés spécialistes de la notation (scoring) pour *profiler* leurs clients, une pratique interdite par le RGPD mais qui permet là encore de lutter contre le blanchiment.

Enfin, on comprend l'importance des Autorités nationales de Protection des données, comme la CNIL en France, à la fois conseillers et policiers de cette transformation. Auront-elles les moyens de l'ambition prêtée au RGPD ? Rien n'est moins sûr.

Plusieurs pierres dans le jardin des GAFA

A défaut de gêner durablement les GAFA (Google, Apple, Facebook, Amazon), des dispositions du RGPD pourraient modifier leur modèle économique (*business model*).

Ces Baal-Moloch de l'ère numérique dévorent avec autant d'appétit les données personnelles, qu'ils en ont plusieurs usages. Elles leur permettent d'abord d'offrir à leurs annonceurs des informations pour un marketing toujours plus ciblé. A la différence d'une pub télévisée qui balaie un large public, les annonces dans une vidéo sur internet ou sur un bandeau publicitaire peuvent se concentrer sur un panel très précis. Par exemple, en jouant une publicité de voitures à quelqu'un qui a recherché sur le net avec le mot clef "voiture". Depuis une dizaine d'années, ces données servent aussi à optimiser leurs applications d'Intelligence Artificielle. Le *Machine Learning* ou *Deep Learning* recourt à des millions de données pour résoudre l'équivalent de millions d'équations comportant autant d'inconnues. C'est ainsi qu'à partir de milliers de clichés radiographiques, des IA ont appris à diagnostiquer des affections mieux que le meilleur des radiologues humains.

Comme tout acteur économique prévoyant, les géants du Web ont anticipé les conséquences de la réglementation. Google et Facebook se sont déjà ouverts au droit à l'oubli. Ils ont aussi modifié à plusieurs reprises leurs règles de protection de la vie privée, pour faciliter le contrôle et l'accès aux données personnelles. Google a supprimé les pubs ciblées présentes dans le bandeau droit de gmail. La firme de Mountain View s'est visiblement rendue compte que s'« inspirer » du contenu des mails pour passer des annonces commerciales n'était peut-être pas très respectueux de la vie privée…

On a pu lire à plusieurs reprises dans la presse spécialisée que le RGPD obligerait les GAFA à rapatrier en Europe leurs bases de données hébergées aux Etats-Unis. Le texte en tout cas ne semble pas le mentionner. Leurs opérations devront néanmoins dépendre d'une Autorité de Protection des données européenne, sans doute l'autorité irlandaise. L'Irlande reste donc la tête de pont sur le continent européen pour la plupart des entreprises américaines.

Le RGPD pourrait induire une évolution majeure dans le modèle économique des GAFA. Et si l'on vous payait pour accéder à vos données personnelles ? L'idée semble faire son chemin. Le conditionnement du téléchargement d'application pour smartphone à l'accès aux données personnelles n'est plus toléré par le RGPD. Ces applications pourraient donc devenir payantes, tandis que la fourniture de données personnelles serait rémunérée.

Ces derniers changements demeurent de pures conjectures. Nous y verrons sans doute un peu mieux après le 25 mai 2018, date de début d'application du RGPD. Car les géants de l'internet ne manquent pas d'imagination. Quand les autorités françaises ont interdit à Amazon d'offrir le port gratuit des livres, en vertu de la loi Lang sur le prix unique du livre, celui-ci s'est mis à le facturer… 0,01 € !

Restons optimistes. D'évidence, la nouvelle réglementation a d'ores et déjà gagné son pari. Elle a modifié l'environnement des données personnelles, dans un sens favorable pour le consommateur et le citoyen.

Emmanuel Bertrand-Egrefeuil