Affaire Facebook: comment le RGPD pourra (peut-être) mieux nous protéger?

Guillaume Desgens-Pasanau, maître de conférences, spécialiste de la protection des données

Publié le 22 mars 2018 – Mis à jour le 7 novembre 2018

Le 25 mai 2018, le règlement européen sur la protection des données (RGPD) entrera en application. Il remplacera la loi française "Informatique et libertés", qui n'est plus en mesure de bien protéger nos données personnelles sur Internet. Explications par Guillaume Desgens-Pasanau, magistrat, enseignant au Cnam et ancien chef du service juridique de la Cnil.

© TheDigitalArtist-Pixabay

Facebook s'est retrouvé lundi 19 mars 2018 au centre d'une polémique autour de l'utilisation indue des données personnelles de millions d'utilisateurs par une société liée à la campagne de Donald Trump, un scandale qui touche au cœur de son modèle économique lié à la revente des données personnelles des utilisateurs, notamment à des fins publicitaires. Les accusations, niées par l'entreprise britannique en question, Cambridge Analytica (CA), ont fait perdre à l'action Facebook près de 6,8% à Wall Street et ont déclenché des promesses d'enquêtes tous azimuts des deux côtés de l'Atlantique.

Cette affaire illustre parfaitement l'importance des enjeux liés à la protection des données personnelles, et les conséquences néfastes, sur le plan commercial ou de l'image, lorsqu'une entreprise manipule des données sans (manifestement) se préoccuper des règles de protection des données.

La loi " Informatique et Libertés " remplacée par le RGPD

En Europe, c'est aujourd'hui une petite révolution qui se joue. Le RGPD (règlement général européen sur la protection des données) remplace, à compter du 25 mai 2018, la célèbre loi « Informatique et Libertés » adoptée il y a plus de 40 ans en France.

Qu’est-ce qui change avec le RGPD ?

Si les grands principes de protection de données restent globalement inchangés, les modalités de gestion de la conformité sont totalement bouleversées, et les risques en cas de non-conformité (sanctions pénales, sanctions financières de la Cnilet risque d'image) sont significativement renforcés.

Au-delà, le RGPD ambitionne d'améliorer la protection des personnes fichées, dans le contexte du développement exponentiel des technologies (de la prédominance des algorithmes en passant par les objets connectés et les nouveaux usages que tout un chacun fait de l'internet) et l'exploitation de nos données personnelles par des opérateurs établis dans le "nuage informatique" (des tigres asiatiques en passant par les "GAFAM" américains [acronyme des géants du Web : Google, Apple, Facebook, Amazon et Microsoft] ou les prestataires de services de l'océan indien).

En particulier, le RGPD vise à mieux protéger les internautes européens, lorsque leurs données personnelles sont manipulées par des opérateurs établis en dehors de l'Union européenne, comme c'est le cas des grands opérateurs américains de l'Internet (Facebook, Google, Microsoft, etc.).

Internet se révèle en effet être un terrain mal adapté à l'exercice des droits reconnus par l'actuelle loi « Informatique et Libertés ». Une difficulté est notamment liée à la question de la localisation des données et des règles de droit applicable. Ainsi que l'a récemment relevé la Commission européenne, la rapidité des évolutions technologiques et la mondialisation modifient en profondeur la façon dont un volume sans cesse croissant de données à caractère personnel est collecté, consulté, utilisé et transféré. De nouveaux modes de partage de l'information via les réseaux sociaux et de stockage à distance de grandes quantités de données sont entrés dans les habitudes de plus de 250 millions

d'internautes en Europe. La problématique des « paradis de données » est d'ailleurs l'illustration de cette contradiction fondamentale à laquelle se heurte le droit de l'informatique : alors que les outils de communication sont, par essence, globalisés, ils ne sont régis que par des fragments de réglementations nationales dont le champ d'application est, par essence, étroit, limité à un territoire et à un champ de compétence ordonné et balisé.

Contraindre les opérateurs non européens à respecter les règles européennes de la protection des données

Le RGPD ambitionne de dépasser cette difficulté et est ainsi venu renforcer les droits des personnes concernées en indiquant que le droit européen s'appliquera dorénavant aussi au traitement de données relatives à des personnes qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées :

> à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdi personnes. Le RGPD précise à cet égard que des facteurs tels que « *l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union* » peuvent indiquer que le responsable du traitement envisage d'offrir des biens ou des services à des personnes qui se trouvent sur le territoire de l'Union européenne.
> au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union. Le RGPD indique sur ce point que sont concernées notamment les techniques de profilage d'une personne physique permettant « *notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit »,*comme par exemple les dispositifs de *« ciblage comportemental* » et de « *publicité ciblée* » mis en cause dans l'affaire Facebook.

Il y a ici une sorte d'effet "extraterritorial" du droit européen puisque l'objectif du RGPD est de contraindre des opérateurs non-européens à respecter les règles européennes de protection des données.

Une justice européenne très vigilante

Ainsi, les pratiques abusives reprochées à Facebook pourraient, si elles étaient avérées, donner lieu à l'application en France de sanctions pénales (jusqu'à cinq ans d'emprisonnement) ou financières (la Commission nationale de l'informatique et des libertés, Cnil, pourra, à compter du 25 mai 2018, prononcer des sanctions pécuniaires à hauteur de 20 millions d'euros ou 4% du chiffre d'affaires mondial d'une entreprise) particulièrement sévères.

La Cour de justice de l'Union européenne(CJUE) est également particulièrement vigilante concernant la protection de la vie privée des citoyens européens.

Dans un arrêt du 6 octobre 2015, dit « Schrems », la Cour de justice a par exemple invalidé la décision n° 2000/520/CE de la Commission européenne constatant que les États-Unis assuraient un niveau de protection adéquat aux données à caractère personnel transférées depuis l'Europe et permettait l'application de l'accord conclu entre les États-Unis et l'Union européenne appelé « Sphère de Sécurité » (« Safe Harbor »). Cette décision de la Commission, qui rendait possible le transfert de données personnelles entre entreprises de l'Union européenne et entreprises américaines, a été invalidée par la Cour au motif que ce pays ne présentait pas des garanties suffisantes en matière de protection des données personnelles. L'accord sur la « Sphère de Sécurité » posait un ensemble de principes de protection des données personnelles, auquel les entreprises établies aux États-Unis pouvaient volontairement adhérer afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union Européenne. La Cour de justice a estimé que ce dispositif, qui visait à compenser l'insuffisance de la législation américaine en matière de protection des données personnelles par rapport à la législation européenne, ne présentait pas des garanties suffisantes du fait des ingérences possibles des autorités publiques américaines dans les données personnelles ainsi transmises et qu'il violait les droits garantis par la Charte européenne des droits fondamentaux. À la suite de l'arrêt « Schrems », la Commission a conclu en février 2016 un nouvel accord avec les États-Unis sur le cadre des transferts transatlantiques de données intitulé « Privacy Shield ». Ce nouvel accord se veut plus protecteur mais beaucoup s'interrogent sur le risque que cet accord soit également invalidé, à terme, par la justice européenne.

La législation et les juges européens tentent donc actuellement de renforcer la protection des citoyens européens. Si le renforcement des règles juridiques est un indéniable progrès, ce n'est pas une fin en soi car se pose bien souvent une difficulté pratique de taille : comment assurer l'effectivité des nouvelles règles, si l'opérateur étranger mis en cause n'est pas physiquement établi sur le territoire de l'UE. Comment, dans ce cas, effectuer une perquisition, interpeller un dirigeant ou recouvrer une sanction financière ?

Sensibiliser les internautes

Au-delà des règles juridiques, la protection de la vie privée et des données passe donc aussi par des solutions de nature technique (par ex. utilisation d'outils de navigation sur internet "privacy by design" qui permettent de limiter les traces de navigation) ainsi que par la sensibilisation des internautes et l'application de certaines règles de prudence.

En réalité, l'enjeu n'est-il pas aujourd'hui d'assurer une meilleure sensibilisation de tous les acteurs et notamment des utilisateurs eux-mêmes (en particulier les plus jeunes), et de les encourager à plus de modération dans les informations qu'ils rendent délibérément publiques sur internet ? Si la réglementation « Informatique et Libertés » a été instaurée, il y a si longtemps, pour protéger les personnes contre le fichage abusif par les administrations ou par les entreprises, faudra-t-il désormais qu'elle les protège également contre elles-mêmes ?

Jusqu'à l'informatisation de nos sociétés, l'oubli était une contrainte de la mémoire humaine. Avec l'informatisation, l'oubli n'existe plus. Les capacités de la mémoire informatique sont aujourd'hui telles que la durée de conservation d'une information dépasse, de loin, la durée de la vie humaine. Ce tout savoir des machines peut ainsi devenir, potentiellement, un véritable livret social virtuel et, pour certains, un passeport pour l'exclusion.

Guillaume Desgens-Pasanau,
Magistrat,
maître de conférences associé au Cnam,
responsable national du certificat de spécialisation « délégué à la protection des données ».

Guillaume Desgens-Pasanau interviewé sur France info pour l'émission « L'info en 3D » à propos de l'Affaire Facebook et Cambridge Analytica.