Règlement européen sur la protection des données : ce qui va changer pour les internautes

Le règlement européen sur la protection des données – proposé il y a plus de quatre ans par la Commission européenne – a été publié au *J.O.* de l'Union européenne le 4 mai. Il sera applicable sur toute l'Europe le 25 mai 2018. Il renforce les droits des Européens sur leurs données personnelles.

Par Christiane Féral-Schuhl*, avocate associée, cabinet Féral-Schuhl/Sainte-Marie

Ayant constaté l'existence d'une fragmentation dans la mise en œuvre de la protection des données à caractère personnel dans l'Union européenne (UE), la Commission européenne a soumis le 25 janvier 2012 (1) au Parlement et au Conseil européens une proposition de règlement européen *« relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données »*.

Renforcement des droits de la personne

Cette nouvelle législation a fait l'objet d'un accord informel en trilogue le 17 décembre 2015, et a été votée définitivement le 14 avril dernier et publiée le 4 mai au *Journal officiel* de l'UE. L'une des avancées majeures du règlement « Protection des données » – entré en vigueur 20 jours après sa publication (soit le 24 mai), pour être applicable dans tous les pays de l'UE le 25 mai 2018 (les entreprises ont donc deux années entières pour s'y préparer) – est sans conteste le renforcement des droits de la personne.

Dans un univers dématérialisé où tout devient possible en quelques clics, l'UE avait dans une directive, dès 1995, souhaité protéger l'individu en lui accordant un certain nombre de droits. Elle prévoyait ainsi :

- un droit à l'information qui consiste en l'obligation, pour le responsable de traitement, de fournir certaines informations énumérées dans la directive ;
- un droit d'accès qui est le droit pour la personne concernée de réclamer de la part du responsable de traitement la consultation de certaines informations portant sur ses données personnelles et sur le traitement de ses données ;
- un droit de rectification qui consiste en la possibilité pour la personne concernée de demander la rectification, l'effacement ou le verrouillage des données qui sont incomplètes ou inexactes ;
- un droit d'opposition qui est le droit pour la personne concernée de s'opposer à tout moment à ce que ses données fassent l'objet d'un traitement, pour des raisons légitimes.

Pourtant, comme le soulignait Viviane Reding en 2012, lorsqu'elle était encore commissaire européenne à la Justice, aux Droits fondamentaux et à la Citoyenneté, les citoyens *« n'ont pas toujours le sentiment de maîtriser entièrement les données à caractère personnel les concernant »*.

En effet, qui n'a pas déjà reçu des publicités dans sa boîte aux lettres sans que l'on n'ait jamais ni effectué d'achats chez l'émetteur de publicités ni donné ses informations personnelles telles que les nom, prénom, et adresse ? Qui n'a pas réceptionné des appels téléphoniques inconnus dont l'objet est de promouvoir un produit, ou de vous solliciter pour un sondage téléphonique, l'interlocuteur connaissant déjà vos nom et prénom sans même que vous ne l'ayez déjà contacté de votre vie, ou sans même que les prestataires de services professionnels avec qui vous avez contracté ne vous ait prévenu de la communication de vos informations à ces tiers précisément ?

Pour remédier à ce problème de maîtrise des données, le règlement prévoit un chapitre entier sur les droits de la personne concernée, ce que ne faisait pas la directive de 1995, laquelle se contentait de placer les droits de la personne concernée dans un chapitre intitulé *« Conditions générales de licéité des traitements de données à caractère personnel »*.

Le renforcement des droits de la personne concernée se fait en accentuant les droits préexistants de celle-ci, par exemple en prévoyant une meilleure transparence quant à la communication des informations relatives au traitement des données à caractère personnel, ou encore en rallongeant la liste des informations à fournir à la personne concernée.

Quatre principaux nouveaux outils

Mais surtout, le règlement européen lui octroie de nouveaux droits :

- Un droit à l'information lors de l'apparition de failles de sécurité.

Ainsi, le droit à la notification d'une violation de ses données à caractère personnel semble aujourd'hui indispensable, alors que l'on ne compte plus le nombre d'entreprises victimes de failles de sécurité relatives aux informations sur leur clientèle : noms, adresses, numéros de

Notes

(1) - Lire l'interview de Viviane Reding, alors vice-présidente de la Commission européenne, en charge de la Justice, des Droits fondamentaux et de la Citoyenneté, dans *EM@ n°53, p. 1 et 2.*

(2) - Agence nationale de la sécurité et des systèmes d'information (ANSSI).

(3) - Le « Safe Harbor » autorisait le transfert des données personnelles des citoyens européens vers les Etats-Unis sous certaines conditions.

(4) - Lire *« US Safe Harbor : la CJUE accable la Commission européenne »*, par Christophe Clarenc, *EM@132, p. 6 et 7.*

téléphone ou encore données bancaires se retrouvent alors publics.

• Un droit d'opposition à une mesure fondée sur le profilage.

Au-delà des failles de sécurité dont peuvent être victimes les entreprises, les internautes doivent, aussi, à leur échelle, faire preuve de vigilance. En effet, au travers des historiques de navigations, des blogs, des réseaux sociaux ou des moteurs de recherche, ils dévoilent, sans souvent en avoir pleinement conscience, des pans entiers de leur vie privée. Or ces informations se révèlent souvent précieuses puisqu'elles pourront être valorisées, alimentant ainsi une véritable économie des données. En ce sens, le « profilage », destiné à évaluer et analyser certains aspects personnels afin d'orienter les publicités selon les intérêts ou de prévenir certains comportements illicites peut être source d'erreurs ou d'abus. C'est dans cet objectif que le Règlement prévoit une obligation d'information spécifique en matière de profilage ainsi que la possibilité de s'y opposer.

• Un droit à l'« effacement » numérique.

Comme le souligne la CNIL dans son rapport d'activité 2013, « la circulation d'informations concernant une personne peut avoir de graves conséquences sur sa vie privée et professionnelle, parfois plusieurs années après les faits ». Aussi, le Règlement européen vient consacrer un « droit à l'effacement » qui permettra à la personne concernée, selon des motifs limitativement énumérés, d'obtenir l'effacement de données personnelles la concernant et la cessation de la diffusion de ces données. La consécration de ce nouveau droit par le Règlement achève ainsi une évolution nécessaire au regard de la protection de la vie privée des citoyens européens.

• Un droit à la portabilité de ses données.

Ces nouveaux droits sont primordiaux en ce qu'ils permettent à la personne concernée d'exercer un contrôle *ex post* sur ses données. La personne concernée a le droit de se voir communiquer ses données personnelles par le responsable de traitement, sous un format « structuré, couramment utilisé et lisible par machine » afin de faciliter leur transfert vers un autre prestataire de services si elle le souhaite et sans que le responsable de traitement ne puisse s'y opposer. L'objectif ici est d'éviter à la personne concernée de se lancer dans une fastidieuse récupération manuelle de ses données qui pourrait l'inciter à renoncer à changer de prestataire.

« Education » et « *hygiène informatique* »

Ces nouveaux outils doivent cependant s'accompagner d'une part, d'une « éducation » à la protection des données, et d'autre part, de la promotion d'une certaine « *hygiène informatique* », selon l'expression consacrée par l'ANSSI (2), qui permettra à la personne concernée de fixer elle-même les frontières de sa vie privée.

Le règlement européen tient aussi compte de l'invalidation du « Safe Harbor » (3) (décision CJUE du 6 octobre 2015 (4). et ses conséquences en consacrant son chapitre V au transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales L'invalidation de cette décision a conduit la Commission européenne et le gouvernement américain à conclure un accord visant à assurer un niveau de protection suffisant aux données transférées de l'UE vers les Etats-Unis appelé « Privacy Shield ».

Articulation avec le « Privacy Shield »

Le G29 réunissant les « Cnil » européennes, qui avait publié son avis le 13 avril 2016 sur le niveau de protection des données personnelles assuré par le « Privacy Shield » (5), a cependant rappelé qu'il devrait tenir compte du règlement européen sur les données personnelles – lequel n'avait pas encore été adopté au moment de la publication du « Privacy Shield ». L'article 45 du règlement énonce les critères à prendre en compte par la Commission européenne lors de l'évaluation du caractère adéquat du niveau de protection des pays tiers à l'Union. Au nombre de ces critères, on trouve *« le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel (...) ».*

Outre le renforcement de la sécurité juridique, on notera que le règlement vise à : réduire la charge administrative des responsables de traitement de données, faire peser davantage de responsabilité sur les sous-traitants, renforcer l'exercice effectif par les personnes physiques de leur droit à la protection des données les concernant au sein de l'UE (notamment leur droit à l'effacement et leur droit d'exiger que leur consentement préalable, clair et explicite soit requis avant l'utilisation de leurs données personnelles), améliorer l'efficacité de la surveillance et du contrôle de l'application des règles en la matière (6).

Le règlement aura d'autant plus d'impact qu'il s'appliquera, dès le 25 mai 2018, de manière uniforme dans l'ensemble des pays de l'UE, sans devoir être transposé en droit national (7). Son champ d'application s'étendra au-delà des frontières des Vingt-huit puisque, désormais, des entreprises ayant leur siège social en dehors de l'UE pourront se voir appliquer le règlement dès lors que les données qu'elles traitent concernent des résidents de l'UE, ce que ne prévoyait pas la directive. @

**** Ancien bâtonnier du Barreau de Paris.***

Notes

(5) - Lire *« Les "Cnil" européennes tirent exagérément sur le nouveau bouclier « Privacy Shield »*, par Julie Brill et Winston Maxwell, *EM@145, p. 8 et 9.*

(6) - Notamment par des amendes administratives pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial d'une entreprise en cas de violation de ces dispositions.

(7) - Sous réserve d'éventuelles dérogations ou règles supplémentaires qui pourront être mises en œuvre sous certaines conditions par les Etats membres.