ALERION.LEXPRESS

FLASH DU CABINET ALERION

JANVIER 2017

PROTECTION DES DONNÉES

Nouvelles lois : nouveaux défis, nouvelles opportunités

L'année 2016 a été marquée par des changements majeurs dans la réglementation sur la protection des données personnelles, tant en Europe qu'en France. Le nouveau règlement général sur la protection des données (« **RGPD** ») a été adopté en avril 2016[1] par le Parlement européen et entrera en vigueur le 25 mai 2018. Le *Privacy Shield*, encadrant les transferts de données entre l'Europe et les États-Unis a été lancé en juillet 2016 et la directive sur la sécurité des réseaux et des systèmes d'information[2] doit être transposée par les États membres au plus tard le 9 mai 2018.

Plus récemment, le Parlement a adopté la loi « pour une République numérique »[3] qui favorise l'ouverture des données publiques, tout en anticipant sur certaines dispositions du RGPD, dont celles sur le droit à l'oubli et le renforcement des pouvoirs de sanction de la CNIL.

Au même moment, le gouvernement a adopté un décret controversé, dit « TES » pour « titres électroniques sécurisés », autorisant la création d'une base de données nationale des passeports et cartes d'identité, comprenant leurs données biométriques (empreintes digitales)[4]. Même si cette base de données n'est – pour le moment - établie qu'à des fins d'authentification par les autorités (confirmer l'identité d'un individu au moyen de ses données biométriques et non pas l'inverse), la CNIL et l'opinion publique craignent la mise en place d'un système d'identification automatique : toute personne qui aura accès, légalement ou illégalement, à cette base de données pourrait identifier un citoyen français à partir de ses empreintes… Une cible parfaite pour les cybercriminels !

A ce titre, on a pu observer au cours des dernières années que la prolifération des objets connectés et des réseaux sociaux, associée à l'augmentation constante des cyberattaques, contraignaient les entreprises à mettre en œuvre des systèmes et des procédures plus complexes et plus robustes, pour protéger les données personnelles des utilisateurs. Au même moment, un nombre croissant de données sont désormais considérées comme des données personnelles, dont les adresses IP[5]. Cette protection accrue des données contraste avec les nouvelles obligations de mise à disposition du public d'une quantité croissante de données par l'administration.

Dans les mois qui viennent, les entreprises et les administrations vont être confrontées à l'obligation de mettre en œuvre et de respecter de nouvelles lois et règlements exigeant une transparence accrue, une confidentialité renforcée, ainsi qu'un contrôle étendu. Si établir et maintenir un équilibre entre ces nouveaux droits et obligations représente un véritable défi, c'est également l'opportunité de constituer un avantage concurrentiel, en se concentrant sur la confidentialité des données, pour garantir la sécurité des produits et services et renforcer ainsi la confiance des clients. Le rôle joué par les autorités de protection des données personnelles sera essentiel pour assurer cet équilibre, au moyen notamment des pouvoirs élargis qui leur ont été accordés par le RGPD[6].

Il est donc important que les entreprises appréhendent et maitrisent ce nouveau paysage réglementaire pour être prêtes avant leurs concurrents.

1. L'Open Data en France

La loi « pour une République numérique » vise notamment à garantir un accès libre et gratuit aux documents et bases de données de l'administration dont la publication représente un intérêt économique, social, ou liés à la santé et l'environnement, ainsi qu'à la diffusion des connaissances scientifiques et ce, afin que chaque opérateur puisse développer des services à partir de ces données librement accessibles.

La loi prévoit toutefois des exceptions importantes : sécurité nationale, données sensibles, droits de propriété intellectuelle, etc.

Cette ouverture bienvenue présente toutefois deux enjeux liés aux nouveaux droits et obligations introduits par la loi elle-même : la nécessaire anonymisation de

REGULATORY & COMPLIANCE
FRÉDÉRIC SAFFROY ASSOCIÉ
LOULLIG BRETEL OF COUNSEL
SOPHIE GUERRIERI AVOCAT SENIOR
LIRIA MARTINEZ SALMON AVOCAT

toutes les données publiques et le difficile équilibre avec le droit à l'oubli et la mort numérique.

2. Le droit à l'oubli et la mort numérique

La loi « pour une République numérique », anticipant le RGPD sur le premier sujet, a établi deux nouveaux droits : le droit à l'oubli et la mort numérique.

Le droit à l'oubli ne concerne que les données des mineurs. Une fois adultes, ils peuvent demander que les données personnelles collectées avant leur majorité soient effacées. Cependant, la mise en œuvre et l'efficacité de ce nouveau droit peuvent se révéler complexes en raison des exceptions liées à l'intérêt général : archivage, recherches scientifiques et historiques, statistiques, liberté d'opinion et d'information, etc.

Au titre du droit lié à la mort numérique, les personnes peuvent communiquer des instructions au responsable du traitement – ou à un tiers de confiance - sur le sort à réserver à leurs données après leur décès, y compris leur effacement. Cela concerne non seulement les réseaux sociaux, mais aussi les autres services en ligne (paiement, stockage, etc.). Comme la loi ne prévoit aucune limite à ce droit et que le responsable du traitement ne peut le restreindre dans ses conditions générales d'utilisation, nombre de données risquent d'être perdues. Les conséquences de l'exercice de ce nouveau droit risquent ainsi de heurter l'intérêt général, notamment la recherche scientifique et historique.

3. Des pouvoirs renforcés pour la CNIL

La loi « pour une République numérique » a étendu les pouvoirs de sanction de la CNIL, en l'autorisant à infliger des amendes pouvant s'élever à 3 millions d'euros (contre 150 000 € actuellement). La loi anticipe ainsi sur le RGPD qui prévoit des pénalités pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial. Dans certains cas, la CNIL sera même autorisée à imposer des amendes sans mise en demeure préalable.

La loi étend également le rôle de la CNIL, celle-ci devant désormais être consultée sur tous les projets de lois ou de règlements concernant les données personnelles. Par ailleurs, de nouvelles missions lui sont confiées :

- la promotion de l'utilisation de moyens assurant la confidentialité des données ;
- la certification des procédés d'anonymisation liés à la publicité des données publiques ;
- l'étude des questions éthiques soulevées par la constante évolution des outils numériques.

4. Contrôle d'accès biométrique aux lieux de travail

Souhaitant moderniser les normes sur l'utilisation de la biométrie pour le contrôle d'accès aux lieux de travail et en anticipation du RGPD sur le « *Privacy by design* » (protection de la vie privée dès la conception) et les études d'impact, la CNIL a adopté, en juin 2016, deux autorisations simplifiées (AU-052 et AU-053), publiées au *Journal officiel* le 27 septembre 2016[7].

Les entreprises devront présenter un rapport documenté justifiant le recours à un dispositif biométrique et précisant en quoi un système de contrôle moins invasif n'était pas adapté. La CNIL contrôlera la conformité du dispositif mis en place avec les autorisations.

La différence fondamentale entre ces deux autorisations est la conservation ou non des données biométriques dans un dispositif détenu par la personne (par ex. une carte) ou dans une base de données globale contrôlée par le responsable du traitement. La CNIL considère en effet que les risques de piratage sont limités dans le premier cas, alors que dans le second, un piratage de la base de données représenterait une menace majeure.

Il est frappant de relever qu'en créant le méga-fichier TES, le gouvernement a délibérément choisi l'architecture considérée comme la plus risquée par la CNIL…

5. CNIL et *Class Action*

La loi n°2016-1547 du 18 novembre 2016 de « *modernisation de la justice du XXIe siècle* » ouvre l'action de groupe (ou *Class Action*) au domaine de la protection des données personnelles. Elle permet à des associations et syndicats de saisir la justice civile ou administrative pour faire cesser des manquements à la loi Informatique et libertés par un responsable du traitement ou un sous-traitant. Elle ne permet toutefois pas de demander réparation du préjudice subi.

[1] Règlement de l'UE n°2016/679 du 27 avril 2016.
[2] Directive de l'UE n°2016/1148 du 6 juillet 2016.
[3] Loi n°2016-1321 du 7 octobre 2016.
[4] Décret n°2016-1460 du 28 octobre 2016.
[5] La CJUE a récemment décidé qu'une adresse IP, même si elle n'identifie pas directement son utilisateur, est une donnée personnelle s'il est possible d'accéder à des données complémentaires permettant de l'identifier ("*P. Breyer v. Deutschland*", 19 octobre 2016, C-582/14).
[6] La CNIL a sanctionné le Parti socialiste d'un avertissement public en raison d'une faille de sécurité dans son processus d'authentification qui permettait un accès libre aux données personnelles des nouveaux membres (délibération n°2016-315 du 13 octobre 2016).
[7] Délibérations n°2016-186 du 30 juin 2016 (AU-052) et n°2016-187 du 30 juin 2016 (AU-053).

REGULATORY & COMPLIANCE
FRÉDÉRIC SAFFROY ASSOCIÉ
LOULLIG BRETEL OF COUNSEL
SOPHIE GUERRIERI AVOCAT SENIOR
LIRIA MARTINEZ SALMON AVOCAT