



Règlement général sur les données personnelles (GDPR) au niveau européen et ses incidences sur la Fr

publié le 15/09/2016, vu 3631 fois, Auteur : [Murielle Cahen](#)

L'Union Européenne a adopté un règlement sur les données personnelles dit GDPR le 16 avril 2016. En plus d'uniformiser le droit des données personnelles, il en étend la protection.

Le règlement GDPR est entré en vigueur le 24 mai 2016 et remplace la directive 95/46/CE qui était jusqu'alors le droit applicable en matière de données. Les données correspondent à tout type d'informations relatives à une personnes physique ou morale identifiée ou pouvant être identifiée : nom, numéro de compte en banque etc ...

Ces données sont essentielles, dès lors elles se doivent d'être protégées efficacement et être soumis à un régime spécifique. Le droit français s'en est d'ailleurs emparé très tôt avec la « Loi relative à l'informatique, aux fichiers et aux libertés » de 1978. Par cette loi, la CNIL (Commission Nationale de l'informatique et des libertés) est créée, et les droits fondamentaux de la protection des données sont reconnus.

Elle se fera modifier par une loi de 2004 qui est en réalité la loi de transposition de la directive 95/46/CE. Finalement, aujourd'hui, c'est le règlement GDPR qui constitue le droit positif des données. Il a pour ambition une protection toujours plus grande des utilisateurs, c'est pourquoi les organismes nationaux de protection l'ont très bien accueilli.

I. L'impact du GDPR sur les sujets de droit

A. L'impact sur les citoyens

Le GDPR est innovant pour les citoyens en ce qu'il fonde une protection des données personnelles des mineurs de moins de 16 ans. En effet, les entreprises de traitement et les réseaux sociaux doivent obtenir l'autorisation des parents pour traiter leurs données. La plupart des pays européens s'étaient déjà dotés d'une telle législation, mais le règlement permet de s'en assurer.

Le règlement instaure aussi un droit au consentement explicite et positif. Cela veut dire que chaque traitement de données d'un utilisateur devra s'accompagner de son consentement clair, non équivoque. Il ne peut être tacite et déduit du comportement de l'utilisateur.

Le pendant de ce consentement est la consécration du droit à l'oubli : les individus pourront demander le retrait, l'effacement d'une information qui leur porte préjudice. Les entreprises de traitement pourront néanmoins conserver ces données s'ils se justifient par un « motif légitime ».

Enfin, les citoyens se voient reconnaître un droit à l'information en cas de piratage ou de violation grave de leurs données, ainsi qu'un droit d'action collective à travers des associations pour contester les violations.

B. L'impact sur les entreprises et les professionnels

Les entreprises de traitement de données se voient responsabilisées par le règlement de 2016. Notamment, ces entreprises devront nommer un « Data Protection Officer », ou DPO, qui devra s'assurer de la mise en oeuvre de protections pour toutes les données, ainsi que de la conformité de ces protections aux normes européennes.

Par ailleurs, l'entreprise a une obligation d'information en cas de piratage ou de violation grave des données d'un utilisateur : il doit l'informer par notification dans les 72 heures suivant la violation.

Enfin, le règlement oblige les entreprises à réaliser des études d'impact, pour limiter au maximum l'exploitation des « données sensibles ». Ce sont les informations sur les orientations politiques, religieuses ou encore sexuelles d'un individu. Ces données répondent à un régime spécifique et ne peuvent être traitées comme les autres.

II. L'impact du GDPR sur les organismes de contrôle

A. Le renouvellement des prérogatives des « CNIL » européennes

Les autorités de protection disposent grâce au règlement GDPR d'un nouveau pouvoir de sanction administrative. Celui-ci est assez étendu et peut aller du simple avertissement à une entreprise de traitement de données à l'obligation d'effacer certaines données.

Surtout, le règlement dote les autorités de protection d'un pouvoir d'amende administrative important. Ces amendes sont comprises entre 2 et 4% du chiffre d'affaire mondial annuel de l'entreprise sanctionnée, ou entre 10 et 20 millions d'euros pour un autre organisme.

Enfin, le règlement prône la coopération entre les différentes agences nationales de protection, notamment par la création du CEPD, le Comité européen de protection des données.

B. La création d'un organisme de contrôle au niveau européen, le CEPD

Le CEPD a vocation à remplacer le « G29 » dès 2018. Il aura pour rôle notamment le conseil à la Commission Européenne par des avis, mais aussi la promotion de la coopération entre les différents Etats-membres.

Pour ce faire, toutes les autorités de protection nationales comme notre CNIL sont membres du CEPD. Elle coordonne leurs actions, mais est aussi une sorte de juridiction, d'autorité suprême, car les avis qu'elle donne aux autorités nationales sont obligatoires et donc doivent être suivis.

Sources :

- <https://www.cnil.fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels>

- <http://www.europarl.europa.eu/news/fr/news-room/20151217IPR08112/Protection-des-donn%C3%A9es-les-citoyens-aux-commandes>