

**PRINTEMPS 2016 - N°28****Transparence, qualité de l'information, protection des données privées : l'action de l'Union européenne**

Par Bruno GENCARELLI, chef d'unité « Protection des personnelles » à la Commission

En 2012, la Commission européenne a présenté un projet de réforme de la protection des données personnelles. Que s'est-il passé depuis lors ? Pour Bruno Gencarelli, l'un des porteurs du projet et négociateur de l'accord de 2015 conclu avec les Etats-Unis, le droit de la protection des données personnelles et plus largement de la vie privée a désormais atteint sa maturité.

Le droit de la protection des données personnelles, et plus largement de la vie privée, a fait l'objet d'une constitutionnalisation à travers la Charte des droits fondamentaux, dont l'article 8 est désormais contraignant. Il a également trouvé une base juridique spécifique dans le Traité européen, qui permet à l'Union européenne de légiférer en la matière, et du reste un très important paquet législatif est actuellement en cours de négociation. Enfin, le droit de la protection des données personnelles fait l'objet d'une jurisprudence abondante et particulièrement protectrice à la Cour de justice, que ce soit à propos du rôle des autorités de contrôle indépendantes (les CNIL), du droit des individus et en particulier du droit à l'oubli, ou encore de la prise en compte de la protection des données dans les domaines sensibles comme la prévention et la répression des infractions pénales.

**La matière première de l'économie numérique**

Ces évolutions juridiques n'ont fait qu'accompagner l'ampleur prise par la collecte, le traitement et le partage des données à caractère personnel, qui sont devenues la véritable matière première de l'économie numérique. Ces données irriguent la recherche et constituent désormais un aspect essentiel de très nombreuses activités.

**Une nouvelle pertinence pour la protection des données personnelles**

La question de la protection des données met en évidence un paradoxe.

Alors qu'on parle d'étanchéité pour des données dites sensibles ou ultra-sensibles les données de santé, on s'aperçoit que les données en question peuvent être agrégées et combinées avec d'autres : les frontières tombent. On observe également que des notions comme le principe de finalité sont brouillées : il devient difficile d'anticiper quel usage sera fait des informations recueillies.

L'émergence du *Big data* a ainsi paradoxalement pour effet de conférer une nouvelle pertinence à la notion de protection des données privées, alors que cette notion pouvait paraître dépassée et, si j'ai bien compris, réservée aux « vieux cons »

**Vers de nouvelles avancées législatives ?**

La nécessité de protéger la vie privée est déjà prise en compte dans le droit national, depuis la loi Informatique et liberté de 1978, et dans le droit européen, depuis la directive de 1995.

Nous nous efforçons maintenant d'obtenir de nouvelles avancées. Le consentement à la communication des données devrait être explicite. La qualité de l'information fournie pourrait être meilleure, et les pages en petits caractères, que personne ne lit, pourraient être remplacées par des icônes ou par des symboles graphiques. Les finalités du traitement des données devraient être spécifiées. Le droit applicable devrait être clairement déterminé : dès qu'il y a ciblage d'un utilisateur européen et/ou fourniture d'un service, le droit européen devrait s'appliquer, indépendamment de la localisation de la société. La question des transferts internationaux devrait également être clarifiée, sachant que, le plus souvent, les données recueillies traversent l'Atlantique. Nous travaillons aussi sur les questions de discrimination, notamment à propos des profils de santé qui pourraient constituer une barrière à l'embauche.

La réforme du cadre législatif en matière de protection des données est en voie d'adoption. Elle en est actuellement à la phase des *trilogues*, c'est-à-dire de la négociation finale entre les trois institutions,

Parlement, Conseil et Commission. Le nouveau cadre législatif comportera trois grands axes.

### **Rationalisation et simplification**

Le premier concerne la rationalisation et la simplification du cadre réglementaire en matière de protection des données. L'adoption d'un règlement au lieu d'une directive permettra de mettre fin à la fragmentation des droits nationaux, dans une matière qui est par définition transfrontalière.

La simplification se traduira par la suppression de nombreuses obligations de notification d'autorisations préalables, qui se sont avérées peu efficaces en matière de protection des données. On passera d'un système *ex ante* à un système *ex post*, avec des mécanismes internes de contrôle (évaluation d'impact, obligation de documentation...) et des mécanismes externes, comportant notamment la possibilité de sanctions financières crédibles.

Cette démarche de simplification et d'harmonisation, qui traverse l'ensemble du texte, se heurte à certaines limites, notamment dans le domaine qui nous intéresse aujourd'hui, celui de la santé. C'est un effet un domaine où les compétences de l'Union européenne sont limitées et où les États membres sont soucieux de préserver certains particularismes nationaux.

Notre proposition prévoyait, par exemple, l'adoption de mesures communes de réduction des risques, comme le recours à la pseudonymisation, mais les résistances des États membres se sont avérées relativement fortes en la matière.

### **Renforcement des droits des individus**

Le deuxième axe est le renforcement et la mise à jour des droits des individus. À partir du socle que constituent le droit national, le droit européen de 1995 et les droits tels que l'accès à l'information et à sa rectification, nous proposons d'introduire des droits nouveaux tels que le droit à la portabilité des données. Un individu devrait pouvoir faire déplacer ses données d'un fournisseur de services à un autre, ce qui lui permettrait de choisir celui qui lui apporte davantage de garanties en matière de protection et de sécurité des données. La concurrence serait ainsi renforcée et les barrières à l'entrée abaissées.

### **La mise en œuvre du droit**

Le troisième axe est celui de la mise en œuvre du droit. En 2014, on a constaté une augmentation de 50 % des incidents de sécurité. Compte tenu de la valeur des données personnelles, les conséquences de ces incidents sont de plus en plus sérieuses, et ce risque concerne aussi bien le secteur privé que le secteur public.

Or, il ne peut pas y avoir de règle de droit crédible s'il n'existe pas de sanction crédible attachée à sa violation. C'est pourquoi nous proposons de permettre aux CNIL européennes d'imposer des sanctions financières proportionnelles au poids des entreprises en cause, c'est-à-dire calculées par rapport à leur chiffre d'affaires.

Au-delà de ce système de sanction, nous proposons un véritable changement de gouvernance en matière de protection des données. Aujourd'hui, chaque CNIL agit sur son propre territoire, alors que les affaires dont nous parlons sont transfrontalières et ont un impact pour l'ensemble des citoyens européens ou pour une grande partie d'entre nous.

C'est pourquoi nous proposons la création d'un guichet unique pour les recours. L'instruction des dossiers serait assurée par l'une des autorités nationales qui devrait décider des mesures à prendre avec les autres autorités concernées. Il ne s'agirait pas de créer une super autorité européenne mais bien un système reposant sur la mise en réseau des CNIL européennes et sur leur collaboration.

<< [Retour au sommaire](#)

 [Télécharger le PDF de l'article](#)

## **PRES@JE.COM**

Une publication de l'Institut PRESAJE  
**(Prospective, Recherche et Etudes Sociétales Appliquées à la Justice et à l'Economie)**

30 rue Claude Lorrain 75016 Paris

Tél. 01 46 51 12 21 - E-mail : [contact@presaje.com](mailto:contact@presaje.com) - [www.presaje.com](http://www.presaje.com)

Directeur de la publication : Michel Rouger

Pour ne plus recevoir d'e-mails de la part de Presaje, [cliquez ici](#)

[>> CONSULTER LES PRECEDENTS NUMEROS](#)