REPÈRES

Alain Bensoussan (avocat) : « Données personnelles : le RGPD offre le niveau de protection le plus élevé au monde »

30-06-2017

Avocat à la Cour d'appel de Paris, spécialisé en droit des technologies avancées depuis 1978, fondateur de Lexing, premier réseau international d'avocats technologues dédié au droit des technologies avancées, Alain Bensoussan nous livre les grandes lignes de la conférence qu'il donnera sur la protection des données à l'occasion du salon APS (26-28 septembre à la porte de Versailles).

Alain Bensoussan est avocat à la Cour d'appel de Paris. Il est spécialisé en droit des technologies avancées depuis 1978. © Alain Bensoussan Avocats

http://www.infoprotection.fr/

Qu'est-ce que le RGPD ?

Le Règlement général sur la protection des données (RGPD) [en anglais : General Data Protection Regulation (GDPR), NDLR] est un règlement européen sur la protection des données personnelles. Il a fait l'objet d'un très large consensus entre les États-membres de l'Union européenne (UE). Surtout, il offre le niveau de protection le plus élevé au monde en matière de données personnelles. A la différence d'une directive européenne, les État-membres n'ont pas à transposer ce règlement dans leur droit national. Dès le 25 mai 2018, le RGPD entrera directement en vigueur dans les systèmes légaux existants, mettant à néant les textes qui lui sont contraires. Ceci dit, il existe pas moins de 57 possibilités permettant aux États d'ajouter des obligations à celles du Règlement... Cependant, les États ne peuvent pas faire moins que le RGPD.

Comment le RGPD a-t-il émergé ?

Le RGPD va harmoniser les réglementations en matière de protection des données personnelles dans l'ensemble de l'UE en vue de remplacer ou compléter les dispositions nationales qui existent dans les États-membres. L'UE ne partait pas d'une feuille blanche. Citons la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Celle-ci a été transposée par tous les pays de l'UE mais sans arriver à une harmonisation. De fait, il existe de très grandes disparités d'un pays à l'autre. C'est dans ce cadre que la Commission a eu compétence pour pondre un nouveau règlement. Le 25 mai 2018, le RGPD annulera en quelque sorte la directive.

Quels seront les principaux changements ?

Actuellement, les entreprises doivent maîtriser 28 programmes de protection plus ou moins différents dans l'UE. Le RGPD va considérablement simplifier cette situation. Cependant, il va aussi radicalement augmenter les obligations et les sanctions pour les entreprises.

Commençons par les obligations...

Les entreprises devront mettre en œuvre la protection des données dès la conception des systèmes d'information ou des applications. C'est ce qu'on appelle le « Privacy by Design » (article 25-1). Il y a ensuite la « Security by Default » : le système d'information doit garantir que les données utilisées seront limitées au système qui les met en œuvre. Enfin, avec le principe d'« Accountability »,apparaît une notion d'exigence de documentation ainsi que de renversement de la charge de la preuve.

Aujourd'hui, c'est à la Commission Informatique et Libertés (CNIL) qu'il incombe de démontrer que tel traitement de données n'est pas conforme. Demain, avec le RGPD, c'est le responsable du traitement qui devra prouver qu'il est conforme. Pour pallier cette difficulté, nous venons d'établir avec le bureau Veritas un référentiel de certification dans le cadre de la conformité au RGPD qui sera certainement très utile aux entreprises.

Qu'en est-il de la pression et des sanctions sur les entreprises ?

Elle sera très forte car l'obligation de documentation va conduire à mettre en place des mesures organisationnelles à tous les niveaux de l'entreprise qui gère des données personnelles. Le maximum de la sanction est fixé à 20 millions d'euros ou 4% du chiffre d'affaires mondial de l'entreprise. Cela devrait donner à réfléchir ! Même de grands acteurs comme Google...

Comment les entreprises doivent-elles s'y prendre ?

J'ai établi une « feuille de route » en 20 étapes. Parmi les plus importantes, il faut commencer par désigner un Data Protection Officer (DPO) - en français : un responsable de la protection des données -, puis tenir un registre des traitements et implémenter pour toutes les applications les deux principes de « Privacy by Design » et de « Security by Default ». Il faut aussi documenter tout le processus de gestion des données personnelles et mettre en œuvre le principe d'Accountability. Enfin, il faut aussi assurer la sécurité des systèmes d'information et réaliser des études d'impact pour les traitements à risque.

C'est un travail assez conséquent... Les TPE et PME seront-elles alors les plus mal loties ?

Elles n'ont pas l'obligation de désigner un Data Protection Officer ni de tenir un registre de l'ensemble des traitements qui n'est généralisé par le RGPD que pour les entreprises de plus de 250 salariés. En revanche, les obligations de « Privacy by Design » et de « Security by Default » sont maintenues.

Quelles seront les entreprises les plus touchées ?

Celles qui gèrent les données de santé, dont les assurances.

Quels vont être les principaux changements pour les citoyens européens ?

Tout d'abord, le droit à la compréhension et à la transparence. Ensuite, le droit à l'oubli ainsi que le droit à la portabilité des données pour éviter qu'Internet, et notamment l'Internet des Objets (IoT) ne soit régulé par un « dominant » comme Microsoft ou Google.

Quels vont être les impacts sur la sécurité et la sûreté ?

Il y en aura un certain nombre. Par exemple, la pré-inscription d'une personne dans un avant-système de contrôle d'accès devra être faite avec son consentement. Tous les constructeurs informatiques, tous les consultants en sécurité ont développé une offre RGPD. Même notre cabinet propose une offre en mode SaaS (Software as a Service) sur notre site.

Qu'en est-il du contrôle des données hébergées dans le cloud ?

C'est la même chose. J'ajoute que le RGPD ouvre une action spécifique qui permet aux personnes privées d'obtenir une indemnisation de leur préjudice. Notamment en saisissant l'autorité de régulation de leur pays. Une chose est sûre : il y a un marché qui s'ouvre pour les spécialistes de la protection des données personnelles !

Propos recueillis par Erick Haehnsen