Collecte massive des données aux États-Unis

Alors que la Chambre des représentants avait adopté le 13 mai dernier la proposition de loi « USA Freedom Act », le Sénat vient de la rejeter. Ce projet de réforme, en réponse au scandale suscité par les révélations d'Edward Snowden, devait permettre une meilleure protection de la vie privée des citoyens américains, en modifiant un article controversé du Patriot Act, et interdire à l'Agence de sécurité nationale (NSA) de collecter en masse des données aux États-Unis, notamment téléphoniques.

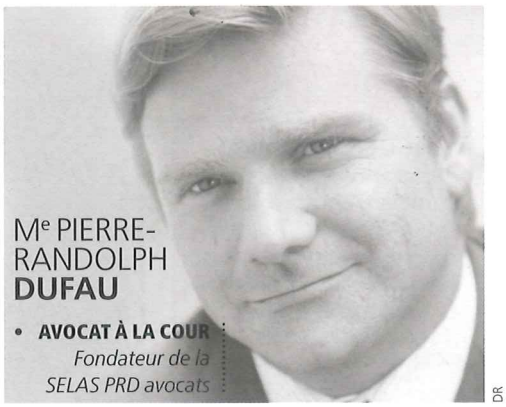
Une stratégie pour un marché unique numérique en Europe

Le 6 mai 2015, la Commission européenne a dévoilé ses projets pour la création d'un marché unique numérique, donnant ainsi corps à l'une de ses grandes priorités. Cette stratégie comporte 16 initiatives reposant sur trois piliers : améliorer l'accès aux biens et services numériques dans toute l'Europe pour les consommateurs et les entreprises, créer un environnement propice et des conditions de concurrence équitables pour le développement des réseaux et services numériques innovants et enfin maximiser le potentiel de croissance de l'économie numérique.

La CNIL annonce son programme des contrôles en 2015

Pour l'année 2015, la CNIL annonce un objectif d'environ 550 contrôles à réaliser comprenant 200 contrôles en ligne et 350 vérifications sur place, sur audition ou sur pièces, étant précisé qu'elle accordera une importance particulière aux contrôles des dispositifs de vidéosurveillance.

Cyberattaques : l'entreprise victime ou coupable ?



Me PIERRE-RANDOLPH **DUFAU**

- **AVOCAT À LA COUR**
  Fondateur de la SELAS PRD avocats

DR

LES FAITS

En avril 2015, TV5 Monde a été la cible d'une cyberattaque massive entraînant la paralysie de la chaîne, du site Internet et des réseaux sociaux de la société. Si les attaques informatiques visant les grands groupes sont médiatisées, Symantec soulignait dans son rapport annuel 2014 que 77 % d'entre elles concernaient en France les PME.

Ces failles informatiques d'origines internes ou externes doivent être appréhendées car elles s'accompagnent de sévères répercussions en termes de sécurité, de pertes économiques et de dégradation de l'image de l'entreprise. Or, la majorité d'entre elles ignorent qu'elles sont tenues, en application de l'article 34 de la Loi Informatique et Libertés, d'une obligation de moyen de mettre en œuvre les mesures conformes aux règles de l'art pour protéger leur système d'information. Au-delà du risque civil, des sanctions administratives et même pénales peuvent être prononcées allant jusqu'à 5 ans de prison et 300 000 € d'amende. Ainsi, de victime, l'entreprise qui n'aurait pas pris toutes les « précautions utiles » pour préserver « la sécurité des données » peut, indépendamment de son dommage, se voir reconnaître responsable, comme Orange qui a été sanctionnée par la CNIL à la suite d'une faille de sécurité concernant les données de près de 1,3 million de ses clients en août 2014.

LA PRÉVENTION POUR LIMITER LES RISQUES

La mise en place d'une politique de cybersécurité adaptée aux besoins de l'entreprise comportant des mesures techniques de sécurité informatique ainsi qu'une politique de gestion des incidents, dont la mise en œuvre est préconisée par la norme ISO 27035, est indispensable. Il convient également de concevoir la sécurité des données dans les relations avec les prestataires, en insérant des clauses spécifiques dans les contrats qui les lient précisant clairement le partage de responsabilité entre les deux parties. Dans ce cadre, un état des lieux du patrimoine informationnel détenu par l'entreprise s'impose afin d'assurer aux données sensibles la sécurité adéquate, ainsi que la réalisation d'audits techniques et de correctifs réguliers du système d'information (typologie et quantité de données, protections, vulnérabilités, etc.). Par ailleurs, une communication en interne sensibilisant les salariés sur ces risques est essentielle. Le recours à une charte informatique précise annexée au règlement intérieur de l'entreprise fixant les droits, devoirs et obligations des salariés est un outil efficace. À cet égard, l'ANSSI vient de publier, en coopération avec la CGPME, un guide de recommandation de bonnes pratiques simples qu'il convient de mettre en œuvre. Au-delà de ces mesures de prévention, il est conseillé de bien soigner les contrats d'assurance afin d'anticiper sur ces causes de pertes d'exploitation. Enfin, rappelons que depuis l'ordonnance du 24 août 2011, les opérateurs de communications électroniques sont tenus à une obligation de notification de la faille de sécurité, sans délai, à la CNIL et aux personnes concernées, prévue par l'article 34 bis de la Loi Informatique et Libertés, dont le défaut est sanctionné pénalement. À noter que le projet de réforme de règlement européen prévoit d'étendre cette obligation à toutes les entreprises, comme c'est le cas aux États-Unis.

CE QU'IL FAUT RETENIR

Le cyber-risque constitue une menace réelle que les entreprises doivent appréhender et anticiper pour ne pas voir, à titre de double peine, leur responsabilité engagée.