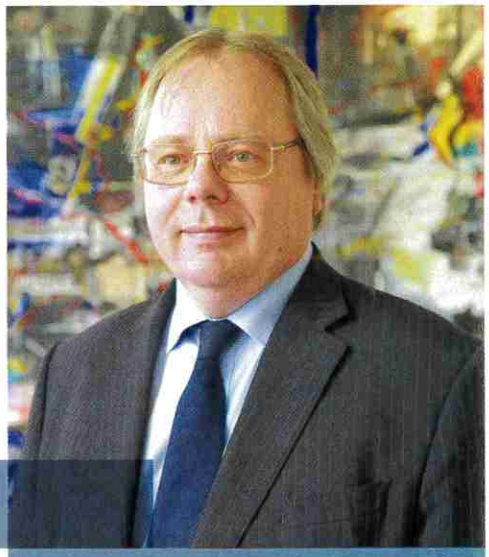
Par Frédéric Forster, avocat, directeur du pôle Télécoms du cabinet Alain Bensoussan Avocats Lexing

LE BIG DATA EST-IL LE NOUVEL OR NOIR DES ENTREPRISES ?

Alors que le développement des objets connectés génère des volumes de données inédits, le big data est en passe de devenir le nouvel eldorado des entreprises. À condition pour celles-ci d'en respecter les règles du jeu.



Avocat à la Cour d'appel de Paris, Frédéric Forster dirige le pôle Télécoms du cabinet Alain Bensoussan Avocats Lexing depuis 2006. Il était précédemment directeur juridique du groupe SFR. Il est également vice-président du réseau international d'avocats Lexing.

Les individus n'ont jamais été autant connectés et les objets connectés jamais aussi nombreux, générant un flux continu de données démultiplié par l'apparition de nouveaux modes de collecte et de conservation des données dans le cloud. L'explosion phénoménale du big data qui en résulte ouvre une véritable mine d'or à tous les acteurs qui accèdent aux données ainsi collectées et stockées. Sans compter le recours à de nouveaux outils – au premier rang desquels les algorithmes prédictifs – par des intervenants commercialisant sur le marché des prestations de mise en relation des données ainsi collectées[1] à des fins marketing essentiellement. L'avantage compétitif qui en résulte pour les entreprises capables d'exploiter et développer ces données tiendra surtout dans l'anticipation des comportements et besoins futurs des clients.

Quels risques ?

Dans un tel contexte, la protection du patrimoine informationnel des entreprises n'a jamais été autant au cœur de leurs préoccupations. En effet, pour celles-ci, les dangers majeurs résident dans des risques d'atteinte à leur réputation et à leur valorisation, au moyen de violations de leurs données capables d'impacter, par ricochet, leurs partenaires et clients dont les données auront été dérobées et divulguées ; dans des risques de condamnations civiles et même pénales, si notamment, elles se trouvaient associées via leur réseau informatique à toutes sortes d'actions illégales. À l'arrivée, le préjudice de l'entreprise peut s'avérer extrêmement important en termes d'image, de C.A., de perte de compétitivité.

Quelle protection ?

L'arsenal juridique récent tient en de multiples règles dont les deux dernières en date sont issues de deux textes européens : la directive NIS et le Règlement général sur la protection des données.

La directive européenne relative à la sécurité des systèmes d'information du 6 juillet 2016, dite directive NIS[2], que les États membres doivent transposer avant le 9 mai 2018, a pour objectif la mise en place, pour les opérateurs d'importance vitale (OIV)[3], de règles contraignantes notamment sur le plan de la gestion et la notification des failles de sécurité, qui impliquent pour l'entreprise : de s'organiser pour identifier et gérer ces éventuelles failles ; une gouvernance particulière : renforcement de pouvoirs du RSSI, révision des chartes d'usage de l'Internet, audit de la solidité et de la robustesse des outils logiciels utilisés. La concentration des données par les acteurs du big data constitue évidemment un point d'attractivité très fort pour tous ceux qui voudraient mettre la main sur ces données. En conséquence, la préoccupation sécuritaire doit être au cœur de la démarche, et c'est précisément ce que vise cette directive, pour une catégorie certes particulière d'acteurs, en harmonisant les conditions dans lesquelles les moyens de sécurité doivent être déployés et celles dans lesquelles les failles de sécurité devront être révélées et gérées.

Le Règlement général sur la protection des données, adopté le 27 avril 2016, marque, quant à lui, un tournant majeur dans la régulation des données personnelles. Son adoption signifie aussi le début d'un compte à rebours jusqu'à son entrée en vigueur effective. En effet, les entreprises ont jusqu'au 25 mai 2018 pour repenser la gouvernance en place en matière de protection des données personnelles et déployer de nouvelles actions pour se mettre en conformité dans les délais imposés. L'enjeu est primordial pour les entreprises : les sanctions susceptibles d'être prononcées atteignent des niveaux très élevés : jusqu'à 2 % ou 4 % du C. A. mondial ! Une chose est sûre : le nouveau Règlement va profondément modifier les règles applicables à l'environnement digital des entreprises, dont celles-ci doivent très vite prendre la mesure. ■

Les dangers majeurs encourus par le patrimoine informationnel résident dans des risques d'atteinte à la réputation et à la valorisation des enteprises par la violation de leurs données qui impacterait, par ricochet, celles de leurs partenaires et clients.

[1] *Ainsi, certaines start-up proposent des market places où les propriétaires de données les monétisent en direct auprès de clients demandeurs (v. B. Bonnell, « Redonnez-nous nos données ! » Les Échos, 14 février 2017)*

[2] *NIS :* network and information security

[3] *Les secteurs considérés d'importance vitale sont essentiellement ceux en rapport avec les activités régaliennes de l'Etat (armée, santé et police) ainsi que ceux relatifs à l'énergie, aux transports ou encore aux communications électroniques.*