Protéger l'innovation et le patrimoine informationnel : une entreprise avertie en vaut deux

Depuis la directive européenne « Attaques contre les systèmes d'information » de 2013, censée être transposée par les Ving-huit depuis le 4 septembre 2015, les entreprises – et leurs-traitants – doivent redoubler de vigilance contre la cybercriminalité aux risques démultipliés. L'arsenal français est renforcé.

Par Christiane Féral-Schuhl*, avocate associée, cabinet Féral-Schuhl/Sainte-Marie

L'innovation à l'ère numérique peut revêtir plusieurs formes : un nouveau brevet, un concept commercial, un logiciel, des informations stratégiques, des bases de données, de la musique, des films, ... Certaines de ces données bénéficient d'une protection légale : le droit d'auteur pour les logiciels, les vidéos, les œuvres multimédia... ; le droit des marques pour les noms de domaine, les logos... ; la loi informatique et libertés pour les données personnelles, le droit des brevets pour les inventions, ...

Preuve de la titularité des droits

La protection est parfois assujettie à des formalités légales : l'enregistrement des brevets, des dépôts de marques, des noms de domaine ou encore les formalités auprès de la Cnil (1). Parfois, la protection est acquise de plein droit mais il faudra justifier de certaines conditions en cas de contestation : l'*« originalité »* pour l'œuvre logicielle ou encore l'*« investissement financier, matériel ou humain substantiel »* pour les bases de données (2). Il faudra en tout état de cause établir la preuve de la titularité des droits, ce qui peut exiger des précautions telles que le dépôt des codes sources pour lui donner date certaine, ou encore un contrat pour encadrer les conditions de cession des données concernées.

Mais la protection n'est pas systématique, comme l'illustre si bien le long débat législatif sur le secret des affaires qui n'a pas encore permis de trouver de solution (3), ouvrant la voie au détournement de données stratégiques pour l'entreprise. S'il est désormais acquis que la valeur de l'entreprise réside en grande partie dans son patrimoine informationnel, la question de la protection de ces données est d'autant plus cruciale que l'entreprise, pour être compétitive, doit vivre à l'heure du *big data*, de l'*open data*, du *cloud*, du logiciel libre *(open source)*, des API (4) et des objets connectés. Comment, dans cet environnement, lutter contre la malveillance ou tout simplement la négligence ?

Une enquête réalisée par le cabinet d'étude britannique Vanson Bourne pour EMC, réalisée entre août et septembre 2014 sur des décideurs informatiques au sein d'entreprises employant plus de 250 personnes (pour un total de 3.300 personnes dans 24 pays), a révélé que 64 % des entreprises concernées avaient déclaré avoir été victime(s) de pertes de données ou d'interruptions d'activité dans le cours de l'année 2014. Ce qui correspond à une moyenne de trois jours ouvrés d'interruption non planifiée. Ces entreprises auraient subi un préjudice de 1,7 milliards de dollars.

Si les entreprises sont confrontées à des risques en provenance de l'extérieur (piratage, vol de données, fraude, virus, *phishing*, usurpation d'identité, ...), il faut constater que les défaillances sont le plus souvent le résultat de négligences internes : non respect des règles de sécurité, notamment dans la gestion des badges d'accès ou des codes, divulgations non autorisées de données, erreurs de manipulations, ..., manque de formation, d'information, de sensibilisation, etc.

L'exemple de la recherche et du développement – secteur d'investissement et d'innovation par nature – en est une bonne illustration. En effet, les travaux menés par les chercheurs le sont parfois en mode collaboratif sur des réseaux non sécurisés, voire non conservés dans les serveurs de l'entreprise, exposant à la perte des investissements. De même, la publication ou l'utilisation d'API ouvrent des fenêtres sur les systèmes d'information des entreprises et organisations, et engendrent des risques liés à la sécurité, notamment d'atteintes aux données (intrusion, captation, ...).

Directive contre la cybercriminalité

Le chef d'entreprise a l'obligation d'assurer la sécurité de l'entreprise. Cette obligation devrait être renforcée dans les années à venir avec la directive européenne *« Attaques contre les systèmes d'information »* du 12 août 2013.

Cette directive visant à combattre la cybercriminalité (5), qui devait être transposée par les Vingt-huit avant le 4 septembre 2015 (6), encourage les Etats membres à prévoir *« dans le cadre de leur droit national, des mesures pertinentes permettant d'engager la responsabilité des personnes morales, lorsque celles-ci n'ont de toute évidence pas assuré un niveau de protection*

Notes

(1) - Commission nationale de l'informatique et des libertés (Cnil).

(2) - Art. L. 341-1 du Code de la propriété intellectuelle (CPI).

(3) - La pénalisation de la divulgation de secrets d'affaires avait été introduite par amendement lors des discussions à l'Assemblée nationale sur le projet de loi pour la croissance et l'activité (loi dite « Macron »). Finalement l'amendement a été retiré le 30 janvier 2015, quelques jours à peine après son dépôt, à la grande satisfaction des journalistes.

(4) - *Application Programming Interface* (API).

suffisant contre les cyberattaques » (considérant 26). Mais au-delà de cette obligation générale, le chef d'entreprise peut être tenu, pour certaines catégories de données, à des obligations légales spécifiques. Tel est le cas pour les données à caractère personnel pour lesquelles il est tenu de *« prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »* (7). Le manquement à cette disposition légale est sanctionné de cinq ans de prison et de 300.000 euros d'amende (8).

Obligations des entreprises

L'entreprise, elle, doit également veiller au respect de cette obligation par ses sous-traitants (9), au risque d'être sanctionnée. Ainsi, une société distribuant des produits optiques a été condamnée par la Cnil à une sanction de 50.000 euros pour avoir, entre autres, manqué à son obligation d'assurer la sécurité et la confidentialité gérées par un de ses sous-traitants. La Cnil relève que *« le contrat entre la société et son sous-traitant ne comportait aucune clause relative à la sécurité et à la confidentialité des données »* (10).

Sur ce point également, le prochain règlement européen sur la protection des données à caractère personnel (« Privacy »), devrait renforcer les obligations en prévoyant une obligation de notification des failles de sécurité à toutes les personnes concernées, ainsi qu'une obligation d'informer l'autorité de contrôle de toute violation *« sans retard injustifié et, si possible, 24 heures au plus tard après en avoir pris connaissance »*. Au-delà du délai de 24 heures, l'entreprise devra nécessairement justifier son silence.

Par ailleurs, les opérateurs d'importance vitale (OIV) sont tenus de respecter des règles de sécurité spécifiques (11). Leur non-respect les expose à des sanctions pénales (12). Les OIV ont également l'obligation d'informer sans délai le Premier ministre de tout incident affectant le fonctionnement ou la sécurité des systèmes d'information (13).

Enfin, on rappellera que le Référentiel général de sécurité (RGS) – afin d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens – s'impose aux administrations et aux prestataires qui les assistent dans leur démarche de sécurisation de leurs systèmes d'information (arrêté du 13 juin 2014 portant approbation du RGS et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques). Plus généralement, on rappellera que l'arsenal français est complet avec plusieurs infractions répertoriées dans le Code pénal. Le vol (14) de données est cependant rarement reconnu par la jurisprudence puisque les éléments constitutifs de l'infraction ne sont pas réunis : dans la mesure où la donnée n'est pas une « chose », il n'y a pas de *« soustraction frauduleuse de la chose d'autrui »*.

En revanche, le recel (15) peut être invoqué à la condition que les données atteintes soient fixées sur un support physique. Même si le recel d'informations sans support matériel a pu être admis dans des arrêts anciens, la jurisprudence actuelle ne suit pas cette tendance. De même, l'abus de confiance (16) est souvent utilisé à l'encontre de salariés ayant détourné des fichiers informatiques à des fins personnelles, en contradiction avec, notamment, la Charte informatique de l'entreprise. Enfin, l'usurpation d'identité numérique (17), utilisée depuis peu, a conduit récemment à la condamnation d'une personne s'étant fait passer pour l'ancien associé d'une entreprise afin de créer des adresses courrielles et des profils sur les réseaux sociaux. De même, c'est sur ce fondement qu'a été sanctionnée la personne ayant créé un faux site web permettant aux internautes de publier au nom d'une personne publiques des communiqués au contenu diffamatoire.

Infractions et Cheval de Troie

Enfin, les atteintes aux STAD (18) répertorient toute une série d'infractions : le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un STAD, le fait d'entraver ou fausser le fonctionnement d'un STAD, le fait d'introduire frauduleusement des données dans un STAD, extraire, détenir, reproduire, transmettre, supprimer ou modifier frauduleusement les données qu'il contient, ou encore le fait de – sans motif légitime – importer, détenir, offrir, céder ou mettre à disposition un équipement, instrument, programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 232-1 à 323-3 du Code pénal, comme par exemple le Cheval de Troie.

Il convient de signaler que dans un arrêt récent (19), la Cour d'appel de Paris a relaxé un internaute ayant accédé à un système de traitement automatisé de données (STAD) dont la sécurité défaillante avait permis l'accès aux données, mais l'a condamné pour maintien frauduleux, ayant constaté qu'il avait réalisé des opérations de chargement alors qu'il existait un contrôle d'accès dont il n'avait pu ignorer l'existence

On rappellera que la voie pénale n'exclut pas une action civile pour obtenir des dommages intérêts. @

* Christiane Féral-Schuhl,
ancien bâtonnier du Barreau de Paris.

Notes

(5) - Directive européenne 2013/40/UE du 12 août 2013 relative aux attaques contre les systèmes d'information, publiée au Journal officiel de l'Union européenne L 218 du 14 août 2013.

(6) - A cette date, la directive n'a toujours pas été transposée.

(7) - Article 34 de la loi française « Informatique et Libertés ».

(8) - Article 226-17 du Code pénal.

(9) - Délibération de la Cnil datée du 7 août 2014.

(10) - Délibération de la Cnil datée du 5 novembre 2015.

(11) - Article L.1332-6 du Code de la Défense, créé par la loi de Programmation militaire (LPM).

(12) - Code de la Défense, art. L. 1332-6-1 et L. 1332-7 ; Code pénal, art. 131-38.

(13) - Code de la Défense, art. L. 1332-6-2.

(14) - Article 311-1 du Code pénal.

(15) - Article 321-1 du Code pénal.

(16) - Article 313-1 du Code pénal.

(17) - Article 226-4-1 du Code pénal.

(18) - Article 323-1 et s. du Code pénal.

(19) - CA Paris, 5 février 2014, n°13/04833