Le vol d'informations n'existe pas... Quelles voies juridiques pour la protection de l'information ?

Marie Barel
marie.barel(@)orange-ftgroup.com

Orange Business Services / Consulting Services
Silicomp-AQL, 4 rue de la Châtaigneraie, CS 51766,
35517 Cesson-Sevigné Cedex, France

Résumé Face à la crise, l'intelligence économique est une stratégie à développer[1] et la maîtrise de l'information une nécessité impérieuse. Alors que, contrairement aux idées reçues, le vol d'informations n'est pas une qualification juridique reconnue par le code pénal français, il convient de comprendre comment le droit protège le patrimoine informationnel de l'entreprise. Or, sauf le cas particulier de certaines données (données à caractère personnel, données couvertes par un secret, ...) pour lesquelles le législateur a organisé une protection particulière, il incombe en définitive aux responsables de mettre en œuvre au sein de l'entreprise des solutions, réponses notamment contractuelles ou normatives, susceptibles de répondre efficacement à la problématique de la protection de l'information.

Le sujet de la présente communication doit faire l'objet d'un article plus détaillé à paraître dans la revue MISC.

1 Introduction

L'information, qui constitue une composante clé de la compétitivité des entreprises, est considérée aujourd'hui comme un actif[2] stratégique [4,5] Il convient dès lors de la protéger, non plus seulement au travers de la sécurité du système qui l'héberge ou la stocke, mais bien en tant qu'élément pivot[3]. Pourtant, malgré la valeur économique attachée au patrimoine informationnel de l'entreprise, il apparaît à l'analyse que ni

[1] Voir en ce sens le discours prononcé par Michèle Alliot-Marie en ouverture de la FIC 2009 [1] : « La protection des entreprises contre l'ingérence et l'espionnage industriel est un enjeu de sécurité nationale. C'est particulièrement vrai à l'heure de la crise économique et financière. Voilà pourquoi j'appelle chacun à la vigilance et à une politique volontariste d'intelligence économique, défensive pour lutter contre les ingérences étrangères, active pour appuyer les secteurs sensibles ou stratégiques. »

[2] On entend par actif tout ce qui a de la valeur pour l'organisme concerné.

[3] À cet égard, on constate de plus en plus souvent dans les organisations, aux côtés de la fonction désormais « traditionnelle » de RSSI (en anglais, ISSO – *Information Systems Security Officer*), chargé de la sécurité des systèmes, la désignation de responsables de la sécurité des informations (en anglais, CISO – *Chief Information Security Officer*).

le législateur ni la juridiction suprême[4] n'ont reconnu à ce jour l'infraction de « vol d'informations ». Dès lors, force est de s'interroger sur les autres protections offertes par le droit et en particulier les réponses contractuelles ou normatives permettant de lutter contre la « fuite » (un euphémisme dans le cas considéré) de données sensibles de l'entreprise.

2 Protection légale de l'information

2.1 À propos des qualifications de vol et de recel d'informations

L'article 311-1 du code pénal définit le vol comme étant « *la soustraction frauduleuse de la chose d'autrui* » dont l'exposé conduira à présenter plus en détail les différents éléments constitutifs de l'infraction et à s'interroger en particulier sur le point de savoir si une information est une chose au sens du code pénal, susceptible d'appropriation...

À cet égard, il apparaîtra notamment à l'analyse que l'extension de la définition de vol à un actif ou une « chose » immatérielle telle que l'information contenue dans les systèmes informatiques des entreprises, conduirait en fait à « torturer » et malmener un texte qui ne saurait l'admettre en définitive, et ce malgré quelques décisions audacieuses [3] qui se sont exonérées de certains principes généraux du droit pénal[5]. Ainsi, malgré un infléchissement de la jurisprudence (dont plusieurs décisions seront présentées[6]), et comme le souligne les auteurs du Lamy *Droit de l'informatique et des réseaux*, si l'idée de « vol d'informations » et quelques idées voisines (« vol informatique », « vol d'usage », « vol de temps machine », ...) ont pu être avancées, « *ceci n'implique pas qu'elles soient recevables et les plus sûrs pénalistes le disent d'ailleurs très nettement* » (Devèze J., Le vol de « biens informatiques », JCP éd. G 1985, I, n° 3210 ; Pradel J. et Feuillard C., Les infractions commises au moyen de l'ordinateur, Revue de droit pénal et de criminologie 1985, p. 307)[7].

[4] En France, la Haute juridiction, la plus élevée de l'ordre judiciaire français, est la Cour de cassation. À l'inverse des autres juridictions judiciaires françaises, il n'y a qu'une seule Cour de cassation pour toute la France, ce qui permet d'assurer l'unité d'application et d'interprétation du droit sur tout le territoire français.

[5] À savoir, le principe d'interprétation stricte de la loi pénale d'une part, et le principe de légalité des délits et des peines d'autre part...

[6] On présentera notamment les arrêts Logabax (Crim., 8 janvier 1979), Bourquin (Crim., 12 janvier 1989) et Antoniolli (Crim. 1er mars 1989)...

[7] On verra par ailleurs, au travers de différents éléments de droit comparé, que cette situation juridique est commune à de nombreux pays. Plusieurs Etats, dont la Chine pour le cas le plus récent (sur le projet de loi débattu en seconde lecture en décembre 2008, voir par exemple : http://www.dailytrust.com/index.

En définitive, on soulignera que, en l'absence de reconnaissance par le droit de l'infraction de vol d'informations (et quand bien même une évolution comparable à celle connue en matière de vol d'électricité reste possible), le recours à la qualification de recel est parfois utilisée sur le terrain pénal. Infraction autonome, à la fois « fourre-tout » et générique, le « recel d'informations » a en effet déjà été sanctionné (sur le fondement de l'alinéa 2 de l'article 321-1du code pénal[8]) par les tribunaux s'agissant par exemple d'un cas[9] de recel de fichiers informatiques obtenus après un accès frauduleux aux systèmes d'information [2]...

2.2 La protection offerte à certaines catégories de données

Ayant conclu précédemment que le recours au texte concernant le vol ne peut être *classiquement* fondé et efficace que dans le cas en principe où le support matériel de l'information a fait l'objet d'une atteinte, il convient néanmoins de rappeler la protection particulière offerte par le droit pénal portant sur certaines catégories de données.

Ainsi en matière de données à caractère personnel (telles que définies à l'article 2 de la Loi dite « Informatique et Libertés » du 6 janvier 1978), il faut notamment rappeler que le code pénal contient pas moins de douze délits sanctionnant les « atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques » (articles 226-16 et suivants). Parmi ces atteintes figurent les infractions liées à une collecte déloyale ou un détournement de finalité des données visées, qui les protègent ainsi en principe contre toute utilisation non consentie par les personnes concernées ou non déclarée par le responsable de traitement. De plus l'obligation de sécurité et de confidentialité des données qui s'impose au responsable de traitement en vertu de l'article 34 de la loi précitée oblige notamment à définir une politique d'habilitation et de gestion des droits d'accès permettant de garantir que seules les catégories de destinataires « autorisés » ont accès aux informations traitées.

Concernant les données couvertes par un secret : à défaut de l'infraction même de violation du « secret d'entreprise » (qui reste elle aussi, comme le « vol d'infor-

`php?option=com_content&task=view&id=1749&Itemid=11)`, ont néanmoins prévu (ou préparent), dans le cadre de leur législation nationale relative à la criminalité informatique, des dispositions permettant d'appréhender tantôt le vol (*theft*), tantôt l'accès à, la capture (au sens de la copie), ou bien encore l'utilisation non autorisés des informations contenues sur les systèmes informatiques...

[8] L'alinéa 2 stipule : « *Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit.* »

[9] TGI de Paris, 1er juin 2007. Les faits sanctionnés étaient fondés sur l'alinéa 2 de l'art. 321-1 du code pénal, qui opère une extension de l'infraction de recel telle définie au premier alinéa et dispose que : « *constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit* ».

mations » envisagé précédemment, une catégorie juridique à imaginer), il est loisible ici d'évoquer en premier lieu la protection offerte aux informations couvertes par le secret industriel ou « secret de fabrique », qui permet, depuis le nouveau dispositif de 1992[10], de sanctionner plus facilement « l'espionnage » au niveau de l'entreprise[11], alors même que l'auteur de l'infraction n'est pas tenu au secret professionnel[12]. Dans ce registre, on rappellera une affaire remontant à quelques années déjà, en 2002, dans laquelle un pirate informatique avait dérobé à Dassault Aviation des secrets industriels et militaires pour les revendre ensuite par le biais d'Internet à environ 250 personnes à travers le monde (le préjudice causé alors avait été estimé à plus de 361 millions de dollars)... Certains de ces secrets concernant en l'occurrence des systèmes d'armement et donc des données intéressant le secret de la défense nationale[13], on rappellera que sont dans ce cas spécifiquement protégés, outre les « renseignements, procédés, objets, documents », les « *données informatisées ou fichiers* »[14] qui sont classifiés de défense, c'est-à-dire qui font l'objet de mesures de protection destinées à restreindre leur diffusion... Dans ce cadre particulier, comme dans celui des autres données soumises à des réglementations spécifiques (Sarbanes-Oxley, Bâle II, Loi sur la Sécurité Financière, Solvency II, ...), des mesures de sécurité pour la gestion de ces données, allant par exemple de l'authentification forte au chiffrement et la mise en place de systèmes de contrôle interne, sont alors imposées[15]. Sur le plan technique par ailleurs, on voit apparaître également de nouvelles solutions à la problématique de gestion de l'information qui s'appuient sur le concept de labellisation électronique [6]

[10] Cf. article L. 621-1 du Code de la propriété intellectuelle et article L. 152-7 du code du travail.

[11] L'auteur de la révélation du secret, dès lors qu'il connaissait l'utilité et le caractère secret des informations divulguées, risque une peine de deux ans d'emprisonnement et une amende de 30.000 euros, tout comme celui qui aurait tenté de les divulguer. Le tiers complice de la divulgation, qui cherche à obtenir d'un employé la divulgation des dispositifs techniques de fonctionnement ou de fabrication d'un produit ou système, encoure les mêmes peines.

[12] Secret qui est protégé quant à lui sur le fondement des articles 226-13 et 226-14 du code pénal et pour lequel le « nouveau code pénal » de 1992 (Badinter), abandonnera la liste à la Prévert des personnes astreintes à ce secret et s'écartera de la notion de secret confié tels qu'ils figuraient dans l'ancien article 378 du code pénal...

[13] Textes de référence : articles 413-9 à 413-12 du code pénal ; article R. 413-6 du code pénal ; décret n° 98_608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale ; Instruction Générale Interministérielle (IGI) n° 1300/SGDN/PSE/SSD/DR.

[14] Il en va de même s'agissant de l'infraction de livraison d'informations à une puissance étrangère (article 411-6 du code pénal), lorsque l'exploitation, la divulgation ou la réunion des informations livrées ou rendues accessibles est de nature à porter atteinte aux intérêts fondamentaux de la Nation.

[15] Pour le cas du secret de la défense nationale, voir notamment : IGI n° 900/SGDN/PSE/SSD/DR portant sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées. IGI n° 910 relative aux systèmes traitant des informations classifiées de défense de niveau Confidentiel Défense.

et dont les enjeux sont à la fois la protection des données au sens de l'intégrité et de l'authenticité et la traçabilité.

Dans tous les cas, on peut en définitive identifier deux piliers principaux de la protection de l'information : d'une part, une démarche de classification de l'information[16], à la fois tournée vers l'interne (avec une politique et des procédures formalisées, communiquées à l'ensemble des acteurs) et vers l'externe (adressant la problématique de la gestion des tiers, ceux-ci étant de plus en plus impliqués dans la sécurité et la maîtrise de l'information) et ; d'autre part, la traçabilité des actions sur les systèmes et les données : d'abord, parce que la majorité des « vols d'informations » sont le fait d'employés « indélicats » et donc des attaques d'origine interne[17], ensuite, parce que l'un des premiers défis des responsables de la sécurité des informations réside en fait dans la détection même de la violation des données[18].

3 Réponses contractuelles ou normatives à la protection de l'information

La sécurisation du patrimoine informationnel passe, on le voit, bien entendu par une combinaison de solutions à la fois techniques et organisationnelles (sécurité des accès au Système d'Information, classification et labellisation des documents, chiffrement des supports, traçabilité des actions sur les systèmes et les données, DRM et autres techniques de « *data loss prevention* »), auxquelles les réponses contractuelles et normatives viennent également s'ajouter dans le rang des mesures préventives.

Sur le registre du contrat d'abord, on rappellera l'intérêt de la signature d'accords de secret ou de confidentialité (NDA) permettant en particulier de définir, d'une part, le périmètre des données sensibles protégées et, d'autre part, les règles de classification et de gestion des documents ou données échangées dans le cadre de cet accord (voir *supra*, démarche de classification tournée vers l'externe) . Les engagements individuels de confidentialité quant à eux, ont d'abord un effet psychologique et

[16] Cette démarche, à la fois essentielle et complexe, respectera en outre quelques bonnes pratiques, afin d'éviter les écueils classiques. Voir notamment à cet égard, le rapport du Cigref [5], pp. 17- 21...

[17] Ainsi, en février 2009, une enquête menée conjointement par le Ponemon Institute et Symantec auprès d'employés ayant quitté leur société en 2008, révèle que 59% d'entre eux admettent dérober des données confidentielles appartenant à l'entreprise qu'ils quittent. Pour plus détails sur les résultats de cette étude, voir : http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20090223_01

[18] Ainsi, d'après différentes recherches effectuées par le Ponemon Institute en 2006 et 2007, 41% des personnes interrogées pensent que leur société ne remarquerait même pas les violations de sécurité ayant entraîné une perte de données confidentielles. De plus, près d'un informaticien sur deux (42%) (sur un panel de 1000 professionnels) considère que sa propre entreprise ne fait que peu de chose pour réduire les risques et détecter des vols ou des pertes de données confidentielles.

une visée pédagogique, qui permettent en général une meilleure sensibilisation des personnels.

Par ailleurs, les pertes et vols de données confidentielles étant, comme nous l'avons déjà souligné, le fait majoritairement de salariés de l'entreprise, deux autres outils juridiques existent qui permettent de fonder d'éventuelles poursuites :

- l'obligation de loyauté[19] d'une part, qui consiste, de manière générale, à ne pas nuire à la réputation et au bon fonctionnement de la société et qui déclenche une obligation de discrétion relativement aux informations dont un salarié a connaissance par ses fonctions et dont la divulgation serait préjudiciable à l'entreprise ;
- la Charte relative à l'utilisation du Système d'Information d'autre part, qui comprend toujours plusieurs dispositions de nature à responsabiliser les Utilisateurs quant au respect de la confidentialité des données (qu'elles soient celles de l'entreprise ou de tiers), interdit des actions qui conduiraient à une fuite d'informations confidentielles et définit des règles de sécurité à respecter...

Sur le fondement de ces différents moyens, l'entreprise pourra ainsi décider de l'opportunité de mettre en œuvre tantôt la voie disciplinaire : licenciement justifié par la perte de confiance et sur le fondement de la violation de l'obligation de loyauté ou de la violation des règles de sécurité définies dans la Charte, tantôt la voie judiciaire : demande de dommages intérêts destinée à réparer le préjudice causé du fait de la perte des données confidentielles (par exemple, perte d'image ou pertes financières) ; suivant l'utilisation faite des données détournées, action en concurrence déloyale (détournement à son profit du fichier clients) ou en diffamation et dénigrement (discrédit sur les produits ou services, le travail de l'entreprise ou la personne d'un concurrent) ; action au pénal : pour abus de confiance (c'est sur ce fondement que la jeune stagiaire chinoise employée chez l'équipementier Valeo a été condamnée en décembre 2007[20] après une plainte déposée en 2005 pour vol de fichiers informatiques confidentiels), pour accès frauduleux au système d'information (en cas par exemple de dépassement de l'habilitation donnée ou des droits d'accès octroyés) ou bien encore en contrefaçon (pour le « vol »de bases de données ou de logiciels)...

Ainsi, on le voit, les entreprises victimes sont en réalité loin d'être démunies et les angles d'attaque sont multiples pour pouvoir, même indirectement, appréhender le

[19] La base légale de cette obligation se trouve dans les articles 1135 du code civil et 1222-1 du code du travail.

[20] http://www.spyworld-actu.com/IMG/_article_PDF/article_6417.pdf

« vol d'informations » visé ici... Dès lors on peut conclure, selon la formule de Paris Bove[21], qu' « information mal acquise ne profite jamais » !

4 Conclusion

À supposer d'abord qu'ils soient détectés (voir nos remarques plus haut à ce sujet), dans tous les cas, le type d'incidents visé (« vol d'information » ou fuite/perte de données confidentielles) fait l'objet d'un « chiffre noir » important, en raison à la fois de la volonté d'éviter la perte d'image d'une part et de l'absence d'obligation de report d'incident d'autre part[22]. Or, le risque d'intelligence économique (voire d'espionnage industriel) est globalement et largement sous-estimé au sein des entreprises et organismes français qui se trouvent souvent mal préparés, avec la difficulté même de pouvoir identifier quelles informations sensibles ou confidentielles se trouvaient sur un portable en cas par exemple de perte ou de vol de ce dernier. En définitive, au-delà des insuffisances réelles ou supposées de la législation et du cadre juridique français sur le sujet, c'est bien une approche de sécurité globale et la sensibilisation des acteurs (*awareness*) qui font davantage défaut ici et augmentent le degré d'exposition au risque visé. Et l'on peut dès lors affirmer que, à l'ère où la frénésie d'échanges d'information conduit souvent à une interpénétration (favorable aux techniques de social engineering) des domaines privés et professionnels[23], les investissements en sécurité doivent être à la mesure de l'importance du facteur humain en matière protection de l'information.

Références

1. Mme Michèle Alliot-Marie. Discours d'ouverture de la fic, 2009. http://crimenumerique.files.wordpress.com/2009/03/20090324fic2009-mam.pdf.

[21] Bruxelles, Revue de droit pénal et de criminologie – Jurisclasseur [octobre 1999]

[22] On relèvera néanmoins ici avec intérêt que, concernant le domaine de la protection des données à caractère personnel, le projet de révision de la directive Européenne 2002/21/CE *relative à un cadre règlementaire commun pour les réseaux et services de communications électroniques* (directive cadre « E-privacy ») prévoit une nouvelle disposition suivant laquelle tout opérateur de réseau ou de services de communication électronique au public devra avertir son autorité de contrôle nationale (en France, la CNIL) des incidents de sécurité ou de la perte de l'intégrité des données à caractère personnel de leurs abonnés, ayant eu un impact significatif. Lire le texte du projet en débat (page 61) : http://www.europarl.europa.eu/document/activities/cont/20080720080728ATT35127/20080728ATT35127EN.pdf

[23] À cet égard, le rapport du Cigref [5] souligne bien, parmi les enjeux actuels de la protection de l'information, « *la tendance à la convergence des usages domestiques et professionnels des SI. Wifi, messageries instantanées, réseaux sociaux, blogs, wikis ... sont d'utilisation courantes dans la sphère privée mais souvent incompatibles avec les usages et les besoins dans l'entreprise* »...

2. A. Caprioli. Le « recel »d'informations et des correspondances sanctionné. *revue Communication – Commerce Electronique, n° 3, comm. 46, n° 6*, Mars 2008.
3. Mohamed Chawki. Vol d'informations : quel cadre juridique aujourd'hui ? *Droit-TIC*, juillet 2006. http://www.droit-tic.com/pdf/vol_information.pdf.
4. Protection du patrimoine informationnel. *Publications Cigref*, 2007. http://cigref.typepad.fr/cigref_publications/RapportsContainer/Parus2007/Protection_patrimoine_informationnel_CIGREF_FEDISA_2007_web.pdf.
5. La protection de l'information : enjeux, gouvernance et bonnes pratiques. *Publications Cigref*, 2008. http://cigref.typepad.fr/cigref_publications/2008/10/2008---protecti.html.
6. André Follic and Aurélien Magniez. Sécurisation des données de bout en bout. *XIII^e Symposium de l'Architecture Cap Gemini*, 2008. http://architectes.capgemini.com/images/secuboutenbout.pdf.