VERS UNE LEGITIME DEFENSE DES ENTREPRISES FACE AU PIRATAGE DE DONNEES

publié le **17/04/2015**, vu **4322 fois**, Auteur : Murielle Cahen

La préservation d'informations sensibles est un enjeu majeur pour les entreprises. Le droit pénal appliqué à la fraude liée au numérique demeure du droit pénal. La criminalité informatique est très difficile à relever et sa découverte est souvent hasardeuse. Cette difficulté est renforcée par le caractère transfrontalier de l'activité frauduleuse. Aussi les entreprises auraient de plus en plus tendance à se protéger en amont contre cette criminalité numérique. Mais quelles sont les possibilités qui s'ouvrent à elles ?

Aux Etats-Unis, la violation de la propriété intellectuelle d'entreprises américaines coûte chaque année plusieurs centaines de milliards de dollars. La Chine serait à ce titre responsable de 50% à 80% des atteintes. Mais la Russie, l'Inde et d'autres pays qui disposent d'un environnement juridique peu élaboré en ce qui concerne les droits de propriété intellectuelle et de politiques industrielles protectionnistes, constituent tout autant des acteurs importants de ce phénomène. Outre la perte énorme de revenus pour ceux qui ont créé les inventions ou acheté des licences, ces atteintes mettent à mal les incitations à innover pour les entrepreneurs.

Ainsi, la coopération aux plans national et international n'a cessé de croitre en matière de lutte contre la cybercriminalité. La lutte contre les cybermenaces passe en effet incontestablement par des réponses coordonnées au niveau international. Ce caractère transnational impose aux Etats la mise en place d'actions concertées visant à établir des politiques de coopération européenne et internationale en matière de lutte contre la cybercriminalité. C'est dans ce cadre que la Directive 2013/40/UE relative aux attaques contre les systèmes d'information a été adoptée le 12 août 2013 par le Parlement européen et devra être transposée en droit interne avant le 4 septembre 2015. Ainsi, et ce n'est pas nouveau, le droit européen s'empare de la question du vol de données (http://www.murielle-cahen.com/publications/vol-donnees.asp). Cette directive fixe des règles minimales concernant la définition des infractions pénales et des sanctions en matière d'attaques contre les systèmes d'information. En outre, elle améliore la coopération transfrontalière entre les autorités judiciaires et la police des différents Etats membres de l'Union européenne. Des données comparables sur les infractions visées à la directive pourront être recueillies et transmises à des agences spécialisées comme Europol et l'Agence européenne chargée de la sécurité des réseaux et de l'information en fonction de leurs missions et de leurs besoins en information.

I- Quel cadre pour le vol de données ?

A) Qualification légale du vol de données

L'article L311-1 du Code pénal qualifie de vol « la soustraction frauduleuse de la chose d'autrui ». Deux éléments sont à dégager de cette définition. En premier lieu, le vol doit porter sur une chose

et en second lieu, il faut que cette chose soit soustraite. En outre, il ressort d'une jurisprudence constante que le vol doit reposer sur un élément matériel.

Ainsi, la difficulté liées au vol de données informatiques d'un point de vue juridique s'explique d'une part par le caractère immatériel des données et d'autre part, par le fait que dans la plupart des affaires, les données sont simplement copiées et non pas soustraites.

La « fraude informatique » c'est-à-dire l'ensemble des agissements intéressant l'informatique qu'on peut tenir pour répréhensibles, est multiforme.

Manipulations informatiques : manipulation des données à saisir à l'entrée du système ; manipulation de programmes ; manipulation au niveau des commandes du terminal ; manipulation des données à la sortie ; utilisation abusive de services informatiques sur place ou à distance ; intrusion informatique (http://www.murielle-cahen.com/publications/p_intrusions.asp).

Espionnage par ordinateur : vol de logiciel ; vol d'information ou utilisation abusive d'informations.

Sabotage de l'ordinateur : destruction ou altération des données ; actes de vandalisme.

Délits économiques usuels, c'est-à-dire détournement de fonds en utilisant des moyens informatiques.

Il faut par ailleurs faire une opposition fondamentale selon que les « biens informatiques » sont *l'objet* de la fraude (sabotage de l'ordinateur par exemple) ou qu'ils sont *le moyen* de la fraude (l'ordinateur servant, par exemple, à réaliser une escroquerie). Mis en avant par MM. Devèze et Gassin, ce clivage a son importance.

Ainsi, dans un arrêt de la Cour de cassation du 4 mars 2008, le vol de données a été caractérisé suivant une double condition : le fait non seulement du détournement du support sur lequel se trouvaient les données mais en plus, du caractère secret des informations concernées. En outre, cet arrêt insistait longuement sur la nécessaire matérialité du vol. Néanmoins, ce raisonnement laissait d'ores et déjà entrevoir la réflexion selon laquelle le vol pourrait être caractérisé dès lors que les opérations effectuées allaient à l'encontre de la volonté du propriétaire des données. Le caractère secret des informations manifeste l'expression de la propriété physique sur des données immatérielles, répondant ainsi aux critères posés par le Code pénal.

B) Quelle réponse des entreprises face au vol de données ?

Entreprise sensible ou pas, chacun possède des informations stratégiques qui peuvent entraîner des conséquences plus ou moins graves en cas de divulgation, modification, ou perte de celles-ci. Elles sont donc vitales pour la structure. Une information stratégique est une information qui, quel que soit son contenu ou sa forme, pourraient avoir des conséquences graves sur la vie de l'entreprise, de ses employés, de ses clients, partenaires ou fournisseurs.

L'Article 122-5 al. 1 du Code pénal énonce que *« n'est pas pénalement responsable la personne qui, devant une atteinte injustifiée envers elle-même ou autrui, accomplit, dans le même temps, un acte commandé par la nécessité de la légitime défense d'elle-même ou d'autrui, sauf s'il y a disproportion entre les moyens de défense employés et la gravité de l'atteinte ».* Pourrait-on appliquer cet article à la personne morale de l'entreprise en cas d'attaque informatique ? Cette question reste en suspend mais les autorités s'en saisissent de plus en plus en développant un cadre législatif autour de ce phénomène.

Ainsi, un rapport de 55 propositions sur la cybercriminalité remis en juin 2014 permet de mettre en relief trois objectifs : une volonté de mieux appréhender le phénomène, de mieux prévenir les

infractions et de mieux les réprimer. Ce rapport propose d'aborder une définition de la cybercriminalité en proposant que celle-ci regroupe *« toutes les infractions tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement internet ».* Il aborde ainsi l'implication des professionnels, la mise en place d'une agence de régulation et le développement de peines spécifiques.

Par ailleurs, des services spécialisés se sont développés au niveau national. L'explosion du nombre des cyberattaques, a contraint la France à adopter une véritable politique de défense afin de protéger ses systèmes d'information.

• **l'Agence nationale de sécurité des systèmes d'information** (ANSSI), créée en juillet 2009 et chargée de proposer des règles en matière de protection des systèmes d'information de l'Etat ;

• **l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication** (OCLCTIC), chargé de lutter contre toutes les infractions liées aux nouvelles technologies de l'information et de la communication ;

• **la Bridage d'enquêtes sur les fraudes aux technologiques de l'information** (BEFTI), qui intervient principalement sur des problématiques de propriété intellectuelle notamment en cas d'atteinte aux systèmes d'information;

• **le Service technique de recherches judiciaires et documentation** (STRJD) qui a pour fonction de centraliser et exploiter les informations judiciaires qui lui sont transmises par l'ensemble des unités de la gendarmerie nationale notamment sur les infractions relatives à la transmission de données à caractère illicite sur Internet.

Au cœur de l'entreprise, les bons reflexes à adopter sont, outre une préparation en amont consistant en un état des lieux des données sensibles et une information constante des équipes, la nécessité d'être réactif face à une attaque. Selon Christophe d'Arlhac, consultant et dirigeant, sont d'abord et avant tout la sensibilisation des collaborateurs, la fixation de règles pour l'utilisation du système d'information et le renforcement de la sécurité de ce système. Ainsi, en cas d'attaque, le comportement à adopter dépendra de la stratégie d'attaque. La cyberassurance s'avère être également une solution émergente. Outre le recouvrement des coûts liés à une attaque cybercriminels, disposer d'une cyberassurance permet à l'entreprise de disposer de réseaux d'experts qui permettent de réagir rapidement. Par contre elle ne s'adapte pas à tout contexte, c'est pourquoi un certain nombre de questions doivent se poser avant de souscrire une cyberassurance : les besoins de la société, le type de cyberassurance, les conditions de déclenchement de celle-ci, etc.

II – Quelles conséquences pour les entreprises ?

A) L'e-reputation à l'épreuve des piratages

La cybercriminalité fait également peser un « risque de réputation » significatif sur les entreprises. En cas d'attaque, leurs données personnelles ainsi que celles de leurs partenaires commerciaux ou clients peuvent être dérobées et divulguées. L'impact peut ainsi s'avérer préjudiciable non seulement pour la réputation mais encore pour la crédibilité de l'entreprise auprès de ses partenaires. L'e-réputation est un phénomène assez récent. Il s'agit non seulement de l'image que l'entreprise donne d'elle même sur internet mais également du ressenti qu'ont les consommateurs à son propos. Le numérique a considérablement complexifié les rapports entre les consommateurs et l'entreprise, permettant un dialogue entre les différentes parties grâce à de nouveaux supports que l'entreprise ne peut pas forcement contrôler. Bien que le web ait permis un surplus de création de valeur ajoutée non négligeable pour les entreprises, il a fait dépendre des

internautes la réputation des entreprises.

La première des urgences pour l'entreprise reste de protéger sa réputation auprès de ses clients pour préserver ses relations commerciales. Le maintient de son chiffre d'affaire prévisionnel est indispensable et cela passe par la restauration de la confiance des actionnaires et du grand public. A cette fin, le dirigeant doit faire appel d'abord à un expert IT, pour déterminer l'origine de l'attaque, la circonscrire, identifier les données impactées, réparer la faille et upgrader le système. Le dirigeant va aussi recourir aux services d'un spécialiste de la communication de crise, pour contrôler les conséquences de l'attaque sur la réputation de son entreprise (plan de communication media, training des porte-paroles, etc.), ainsi qu'à un avocat pour gérer les relations avec les régulateurs et les tiers.

B) Illustrations récentes : les affaires Orange et Sony

En février 2014, l'opérateur annonce avoir été victime d'un piratage informatique. Cette attaque de grande ampleur a mis en cause une masse extrêmement importante de données personnelles (http://www.murielle-cahen.com/publications/p_donnees.asp). Même si l'opérateur a annoncé par la suite que l'intrusion a été éphémère, et que l'intégrité des codes personnels n'a pas été menacée, des menaces de pishing ont pesé sur les clients par le biais de sollicitations douteuses qu'ils pourraient recevoir par email.

Autre affaire très récente, les dirigeants de Sony Pictures ont reconnu que le studio de cinéma a été victime d'un vol "très important de données confidentielles" au cours d'une attaque informatique sophistiquée. Par ailleurs, cinq films de Sony Pictures, y compris certains qui ne sont pas encore sur les écrans ont aussi été piratés.

Sources :

http://blogs.lentreprise.com/l-entreprise-et-les-medias/2014/02/03/piratage-de-donnees-lincroyable-silence-dorange/

http://toiledefond.net/e-reputation-des-entreprises/

http://business.lesechos.fr/directions-numeriques/cyber-attaques-se-preparer-pour-reagir-efficacement-7388.php?id=7388#

http://www.leparisien.fr/economie/les-pme-face-a-la-cybercriminalite-15-09-2014-4136531.php

http://www.it-expertise.com/comment-faire-face-a-la-cybercriminalite/

http://www.globalsecuritymag.fr/Lutte-contre-la-cybercriminalite,20131007,40067.html