REVUE LAMY

RLDA

COLLECTION LAMY

DROIT DES AFFAIRES

Dossier spécial

LA LUTTE CONTRE LA CYBERCRIMINALITÉ, UN ENJEU JURIDIQUE ET ÉCONOMIQUE MAJEUR POUR LES ENTREPRISES : SOLUTIONS ET PROPOSITIONS

Par Emmanuel DAOUD, Clarisse LE CORRE, Elsa CHAUVIÈRE, Mélanie TROUVÉ, Émilie BAILLY, Anne SOUVIRA, Myriam QUÉMÉNER, Aurélia MARIE, Gaston VEDEL, Carole GHASSEMI et Karin ROUBAUDI

87

MENSUEL

Novembre 2013

Éclairages

10 SAS : confirmation de l'absence d'obligation de non-concurrence à la charge de l'associé
Par Irina PARACHKÉVOVA

26 L'ordonnance du 25 juillet 2013 modifiant le cadre juridique de la gestion d'actifs et la notion de fonds d'investissement alternatif (FIA)
Par Isabelle RIASSETTO

41 Qualification pénale du détournement du temps de travail par le salarié : une extension de la notion de « *bien* » en matière d'abus de confiance
Par Sylvain BEAUMONT et Cécile MAUGÈRE

Repères

54 Le droit de l'Union comme instrument de contestation interne des règlementations commerciales restrictives : libéralisation des échanges entre les États membres ou libéralisation de l'économie ?
Par Éric CARPANO

Wolters Kluwer France

DOSSIER SPÉCIAL

La lutte contre la cybercriminalité, un enjeu juridique et économique majeur pour les entreprises : solutions et propositions

SOMMAIRE

Introduction 75
Par Emmanuel DAOUD et Clarisse LE CORRE

Libertés fondamentales et protection des données personnelles 79
Par Emmanuel DAOUD, Elsa ÇHAUVIÈRE et Mélanie TROUVÉ

L'entreprise et la protection des données personnelles 85
Par Émilie BAILLY et Clarisse LE CORRE

La « cybersécurité » des entreprises 93
Par Anne SOUVIRA

La coopération entre les organes de lutte contre la cybercriminalité. pour une stratégie globale de « cybersécurité » française 98
Par Myriam QUÉMÉNER

Contrefaçon de marques et e-réputation sur les réseaux sociaux : les nouveaux défis des titulaires de marques 104
Par Aurélia MARIE, Gaston VEDEL et Carole GHASSEMI

E-réputation : quels risques pour les entreprises et les particuliers ? 111
Par Karin ROUBAUDI

Introduction

Par Emmanuel DAOUD
Avocat
Cabinet Vigo

Et Clarisse LE CORRE
Avocat
Cabinet Vigo

→RLDA 4841

Selon une étude IDC sponsorisée par EMC (Digital Universe Study, IDC, déc. 2012), les données numériques créées dans le monde seraient passées de 1,2 zettaoctets par an en 2010 à 1,8 zettaoctets en 2011, puis 2,8 zettaoctets en 2012 et devraient s'élever à 40 zettaoctets en 2020 (1 zetaoctet = 1 000 milliards de Go), soit 5,247 Go par personne sur la planète. Cette explosion des données du monde numérique est récente : 90 % de ces dernières n'existaient pas il y a deux ans (Rapport d'activité CNIL, 2012, p. 85). Les données numériques créées quotidiennement proviennent de toutes parts : messages sur les réseaux sociaux et sites internet participatifs, blogs, images numériques, vidéos et fichiers audio publiés ou stockés sur le web, transactions financières en ligne, signaux GPS de téléphones mobiles et tablettes numériques, données de géolocalisation, sauvegarde de fichiers de tous types de formats ou encore messageries électroniques (l'on estime à 294 milliards le nombre de courriels échangés dans le monde chaque jour,

68 % des courriels étant des spams : « Global State of Information Security Survey 2013, Tendances et enjeux de la sécurité de l'information », Étude PwC, 30 janv. 2013). Désormais appelées Big Data, ces données représentent un volume tel qu'elles ne peuvent être appréhendées par des outils classiques de gestion de bases de données et de gestion de l'information.

La cybercriminalité désigne les infractions pénales commises par le biais des réseaux informatiques et de l'information électronique.

L'explosion des données du monde numérique, dont la valeur patrimoniale ne cesse de s'accroître, pose des défis de nature idéologique, sociologique, économique, politique, géopolitique et bien évidemment juridique, pour la société contemporaine. L'ensemble des individus, acteurs économiques et États sont concernés par une telle expansion, non sans conséquences sur la sphère d'influence de chacun et les rapports de puissance entre les États mais aussi entre les États et les multinationales du numérique. Si le phénomène Big Data est, jusqu'à présent, propre aux pays développés, les pays émergents supplanteront ces derniers dans leur rôle de principaux producteurs de données numériques d'ici 2020, échéance à laquelle la Chine devrait générer à elle seule 22 % des données numériques mondiales (Digital Universe Study, IDC, déc. 2012 : la part des données du monde numérique générées par les pays émergents est passée de 23 % en 2010 à 36 % en 2012, et devraient s'élever à 62 % en 2020).

Face au Big Data et donc au volume croissant des données numériques, la collecte, le traitement, le partage, l'analyse, le stockage et la valorisation de ces données doivent être redéfinis et adaptés. De nouveaux modes de gestion ont ainsi fait leur apparition, tels que le cloud computing (utilisation de serveurs distants), lequel devrait concerner 40 % des données à échéance 2020. Le développement exponentiel de l'univers numérique, par l'augmentation du nombre de données à protéger, la complexification des actifs à sécuriser et l'interconnexion des systèmes qu'il sous-tend, présente par ailleurs une incidence directe sur la sécurité de l'information (« Global State of Information Security Survey 2013, Tendances et enjeux de la sécurité de l'information », préc.). La sécurisation des données constitue désormais un enjeu majeur. Il s'agit de sensibiliser les esprits à ces nouvelles problématiques, de faire face aux failles de sécurité de l'information, au manque d'adhésion des consommateurs et des entreprises aux bonnes pratiques sécuritaires et à cette nouvelle forme de criminalité, appelée « *cybercriminalité* ».

La cybercriminalité désigne les infractions pénales commises par le biais des réseaux informatiques et de l'information électronique. Elle recouvre dès lors des agissements très vastes, qu'il s'agisse d'atteintes aux biens (escroquerie, achat/vente de contrefaçons, fraude aux moyens de paiement, espionnage de sociétés, piratage d'ordinateur ou de site internet, vol de données sensibles et d'informations personnelles telles que les données bancaires, téléchargement illégal, intrusion non autorisée dans un système informatique, etc.) ou aux personnes (diffusion d'images pédophiles, incitation au suicide, à la haine raciale, au terrorisme, atteinte à la vie privée, etc.) – agissements qui se diversifient et se complexifient au fur et à mesure des innovations technologiques.

La cybercriminalité est une forme de criminalité atypique. Les auteurs de « *cyber-infractions* » sont variés (hacker isolé, réseaux organisés, salarié peu scrupuleux, cellules de renseignement, etc.) et guidés par des motivations diverses (lutte contre le terrorisme, vol de données sensibles à des fins lucratives, acte à portée idéologique ou symbolique, volonté de déstabilisation d'entités étatiques ou de multinationales, simple « *défi* » entre hackers, etc.). La cybercriminalité se caractérise par un rapport gains/risques nettement supérieur aux infractions traditionnelles, du fait de l'appréhension plus complexe des comportements répréhensibles (défaut de barrières géographiques, opacité des techniques utilisées et anonymat facilité par l'utilisation de serveurs proxies, de réseaux privés virtuels (VPN) ou du réseau TOR). Elle se distingue par ailleurs par une certaine occultation, de la part des auteurs de telles infractions, du caractère délictuel de leurs actes (La fraude en entreprise : tendances et risques émergents, 6e éd., Global Economic Crime Survey 2011, Étude PwC). L'action virtuelle est en effet perçue avec moins de gravité, au profit d'une présentation symbolique voire ludique des cyber-attaques, pourtant très éloignée de la réalité des conséquences économiques et réputationnelles pour les cibles de telles pratiques.

Quatrième catégorie de fraude la plus rencontrée par les entreprises, la cybercriminalité est devenue une préoccupation majeure des États et des opérateurs économiques. 60 milliards de dollars sont ainsi dépensés chaque année dans le domaine de la cybersécurité (logiciels de sécurité, services de sécurité, équipements, réseaux d'entreprises), avec une progression anticipée de 10 % par an durant les 3 à 5 prochaines années (Étude PwC, préc.).

Ce constat impose de mettre en œuvre une politique de « *cybersécurité* », reposant non seulement sur des dispositifs de contrôle et de prévention de la matérialisation des risques, mais également sur une action répressive adaptée assurant l'incrimination de tels comportements, en passant par une sensibilisation des personnes physiques et morales à l'impératif de protection des données. Les récentes révélations du journal *Le Monde* sur les programmes d'espionnage électronique dans le monde de l'Agence nationale américaine de sécurité (NSA), qui dénoncent la collecte de milliards de données téléphoniques (DNR) et de données liées à l'univers numérique (DNI), ne font que souligner la nécessité d'une réponse du droit pour protéger les données personnelles, au nom de la défense des droits et libertés fondamentaux.

Si la défense de la confidentialité, de l'intégrité et de la disponibilité des systèmes informatiques, des réseaux et des données justifie la mise en œuvre d'un système répressif incriminant les atteintes portées auxdits systèmes, réseaux et données, il convient toutefois de garantir un équilibre entre les intérêts légitimes de l'action répressive et le respect des libertés et droits fondamentaux (droit de ne pas être inquiété pour ses opinions, droit à la liberté d'expression, en ce compris la liberté de rechercher d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontières, ainsi que le droit au respect de la vie privée).

Ce dossier spécial vise à appréhender les multiples facettes du phénomène de la cybercriminalité en faisant appel à différents spécialistes, faisant valoir leurs domaines d'expertise respectifs. Le cabinet d'avocats Vigo (Émilie Bailly, Emmanuel Daoud, Clarisse Le Corre, Avocats, ainsi qu'Elsa Chauvière et Mélanie Trouvé, élèves-avocats) a ainsi sollicité Myriam Quéméner, Magistrat, Anne Souvira, Commissaire Divisionnaire, Aurélia Marie,

spécialiste en propriété intellectuelle et droit des marques, et Karin Roubaudi, conseil en communication et gestion de crise, afin d'étudier les nombreuses problématiques reliées à la cybercriminalité ainsi que les réponses techniques, juridiques et opérationnelles mises en œuvre par les acteurs en présence. Nous les remercions pour leur précieux concours.

* * *

L'objectif de « *cybersécurité* » repose notamment sur l'impératif de protection des données personnelles, droit fondamental visé à l'article 8 de la Charte des droits fondamentaux de l'Union européenne et à l'article 16 du Traité sur le fonctionnement de l'Union européenne, ainsi qu'à l'article 8 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, et dont le respect est garanti, en droit interne français, par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Le droit à la protection des données personnelles est étroitement lié au droit au respect de la vie privée et, plus généralement, aux droits et libertés fondamentaux. L'article premier, paragraphe 1, de la directive 95/46/CE dispose ainsi que les États membres « *assurent* [...] *la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée à l'égard du traitement des données à caractère personnel* » (Dir. PE et Cons. CE n° 95/46, 24 oct. 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE 23 nov. 1995, n° L 281).

> *Les entreprises présentent de ce fait un rôle ambigu, à la fois victimes potentielles de cyber-attaques et responsables de la sécurité des données personnelles traitées en leur sein.*

Toutefois, le droit à la protection des données personnelles « *n'apparaît pas une prérogative absolue et doit être pris en considération par rapport à sa fonction dans la société* » (CJUE, 9 nov. 2010, aff. C-92/09 et C-93/09, Volker und Markus Schecke GbR et Hartmut Eifert, Rec. CJUE 2010, I, p. 11063). Partant, et conformément à l'article 52, paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne, des limitations peuvent être imposées à l'exercice du droit à la protection des données personnelles, sous réserve qu'elles soient prévues par la loi, respectent le contenu essentiel des droits et libertés et soient, dans le respect du principe de proportionnalité, « *nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union européenne ou au besoin de protection des droits et libertés d'autrui* ».

L'étude du phénomène de la cybercriminalité nécessite dès lors de s'interroger préalablement sur le sens et la portée du droit à la protection des données personnelles, ainsi que sur les limitations de principe pouvant être imposées à l'exercice de ce droit (Daoud E., Chauvière E., Trouvé M., Libertés fondamentales et protection des données personnelles, RLDA 2013/87, n° 4842).

* * *

L'impératif de protection des données personnelles est particulièrement prégnant pour les entreprises, dont l'activité quotidienne implique nécessairement le traitement de données à caractère personnel.

Messagerie électronique, intranet, consultation d'internet, bases de données, stockage de données sensibles *via* le *cloud computing*, l'utilisation des nouvelles technologies de l'information constitue de toute évidence un outil compétitif fondamental pour les entreprises. Cette mutation du mode de fonctionnement de l'entreprise « *la rend plus performante, mais aussi plus vulnérable, ce qui l'oblige à repenser sa politique de sécurité* » (Achilleas P., J.-Cl .Libertés, Fasc. 820 : Internet et libertés, § 83).

Les risques pesant sur les entreprises en la matière sont nombreux. Failles de sécurité, fuite de l'information, vol et divulgation de données sensibles, fraudes externes ou internes aux systèmes d'information, piratage ou encore espionnage, autant d'éléments pouvant engager la responsabilité administrative, civile et pénale des entreprises, outre le risque réputationnel que représente tout manquement à la sécurité des données des personnes physiques (salariés, clients, consommateurs, prospects, partenaires, etc.).

Les entreprises présentent de ce fait un rôle ambigu, à la fois victimes potentielles de cyber-attaques et responsables de la sécurité des données personnelles traitées en leur sein. Ce dernier leur impose de mettre en œuvre une politique de gestion des risques tant internes qu'externes en matière de données personnelles, conciliant cette exigence sécuritaire aux intérêts légitimes de l'entreprise et aux droits fondamentaux de protection des données personnelles et de respect de la vie privée, à la faveur d'une nouvelle culture d'entreprise intégrant l'impératif de protection des données et sensibilisant tous les acteurs de l'entreprise aux rôles et responsabilités de chacun (Bailly E., Le Corre C., L'entreprise et la protection des données personnelles, RLDA 2013/87, n° 4843).

Au-delà de la question de la protection des données personnelles, il s'agit pour les opérateurs économiques d'instaurer une politique de cybersécurité de nature à faire face à la diversité des risques en matière de cybercriminalité qui, on l'a vu, relèvent tant d'atteintes aux biens que d'atteintes aux personnes et, de ce fait, vont bien au-delà du piratage de données sensibles de l'entreprise.

Une telle politique de cybersécurité implique des solutions techniques, juridiques et de gouvernance, afin de préserver l'intégrité, la confidentialité et la disponibilité des systèmes d'information et des données patrimoniales ou sensibles qu'ils recèlent (Souvira A., La cybersécurité des entreprises, RLDA 2013/87, n° 4844).

L'implication des entreprises dans la sécurisation des systèmes d'information est d'autant plus nécessaire que celles-ci présentent un niveau de maturité nettement insuffisant en matière de gestion de la cybercriminalité, privilégiant une approche réactive plutôt que proactive – une entreprise sur quatre dans le monde déclare aujourd'hui ne disposer d'aucun dispositif de prévention et de détection des risques de cybercriminalité (La fraude en entreprise : tendances et risques émergents, 6e éd. Global Economic Crime Survey 2011, Étude PwC).

* * *

Les menaces contre les systèmes d'information touchent également les puissances étatiques, pour lesquelles les conséquences des cyberattaques peuvent être dévastatrices : « *appropriation de données personnelles, espionnage du patrimoine scientifique,*

économique et commercial d'entreprises victimes de leurs concurrents ou de puissances étrangères, arrêt de services nécessaires au bon fonctionnement de l'économie ou de la vie quotidienne, compromission d'informations de souveraineté » (Rapp. ANSSI, Défense et sécurité des systèmes d'information : Stratégie de la France, févr. 2011).

La cybercriminalité est rapidement devenue une préoccupation majeure des États. Néanmoins, le caractère protéiforme et transfrontalier de la cybercriminalité rend indispensable « *l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable* » (Convention sur la cybercriminalité, Conseil de l'Europe, Budapest, 23 nov. 2001).

Les nombreuses initiatives nationales, internationales et européennes récentes (pour ne citer que quelques exemples : création en janvier 2013 d'un groupe de travail interministériel sur la lutte contre la cybercriminalité ; création, le 11 janvier 2013, du Centre européen de lutte contre la cybercriminalité, Forum international de la cybersécurité en janvier 2013 à Lille ; adoption par le Parlement et le Conseil européen, le 25 janvier 2012, d'une proposition de règlement visant à modifier le cadre juridique de la protection des données à caractère personnel ; publication le 7 février 2013 de la stratégie de l'Union européenne en matière de cybersécurité et d'une proposition de directive relative à la sécurité des réseaux et des systèmes d'information) traduisent toutes le souci de pallier le caractère parcellaire du cadre juridique actuel en menant une politique pénale commune, et d'intensifier la coopération entre les structures – publiques comme privées, nationales comme supranationales – de lutte contre la cybercriminalité (Quéméner M., La coopération entre les organes de lutte contre la cybercriminalité, RLDA 2013/87, n° 4845).

* * *

Les profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques étendent le spectre de la cybercriminalité et apportent chaque jour de nouveaux défis, face auxquels les réponses restent à définir.

C'est le cas des atteintes portées aux titulaires de marques, multipliées et diversifiées par le développement des réseaux d'échanges d'informations, qui ne se limitent désormais plus à des actes de contrefaçon traditionnels. *Username squatting*, *page squatting* ou encore atteinte à l'e-réputation des marques, le droit peine à appréhender ces nouveaux risques pesant sur les titulaires de marques, s'agissant tant de la qualification juridique de ces derniers que de l'identification des auteurs de telles pratiques. S'impose alors une redéfinition des actions – juridiques ou non – pouvant être mises en œuvre par les titulaires de marques à l'encontre de ces nouvelles formes d'atteintes (Marie A., Contrefaçon de marques et e-réputation sur les réseaux sociaux : les nouveaux défis des titulaires de marques, RLDA 2013/87, n° 4846).

La protection de l'e-réputation apparaît à ce titre comme un nouvel enjeu du cyberespace. En effet, le développement des réseaux de communication et d'échanges d'informations accentue la visibilité des contenus et opinions de chacun. Réseaux sociaux, forums de discussion, blogs, sites web constituent autant de moyens de partager, commenter, enrichir et relayer sur la place publique virtuelle des informations relatives aux personnes physiques et morales, qui se construisent ainsi – ou se voient imposer – une e-réputation.

La gestion de cette dernière est désormais indispensable pour l'entreprise, pour qui l'image et la notoriété numériques représentent un avantage concurrentiel déterminant, mais également pour les particuliers (consultation, par l'employeur, du compte Facebook ou Twitter du candidat à l'embauche ou de son salarié, etc.). Enjeu majeur de communication pour les opérateurs économiques, il est à présent impératif de composer avec l'e-réputation, notamment par la mise en place d'une stratégie d'influence visant à mieux maîtriser la diffusion d'informations sur la place virtuelle publique (Roubaudi K., E-réputation : quels risques pour les entreprises et les particuliers ?, RLDA 2013/87, n° 4847). ■

Libertés fondamentales et protection des données personnelles

Les données personnelles appartiennent à la sphère privée de l'individu et bénéficient ainsi d'une protection au titre du droit au respect de la vie privée. Mais leurs spécificités et la multiplication des atteintes dont celles-ci font l'objet ont conduit à définir un régime protecteur autonome des données personnelles.

Par Emmanuel DAOUD
Avocat

Et Mélanie TROUVÉ
Élève-avocat

Elsa CHAUVIÈRE
Élève-avocat

→RLDA 4842

En vertu des définitions fournies par la Commission nationale de l'informatique et des libertés (CNIL) et la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « Loi de 1978 ») l'instituant, une donnée personnelle est une information qui permet de nous identifier ou de nous reconnaître, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à notre identité physique, physiologique, psychique, économique, culturelle ou sociale. Il peut s'agir d'un nom, d'un prénom, d'une date de naissance, d'une adresse postale, électronique ou IP, d'un numéro de téléphone, de carte de paiement, de plaque d'immatriculation d'un véhicule, de sécurité sociale, d'empreinte digitale, d'ADN, de photos... (<www.cnil.fr>).

La notion de donnée personnelle est venue remplacer celle de donnée nominative initialement utilisée dans la Loi de 1978. Elle doit être appréhendée de manière large, nonobstant son usage, son sens, son contenu ou sa forme.

Aux termes du célèbre avis rendu par le Conseil d'État le 13 août 1947, les libertés fondamentales recouvrent en réalité deux catégories de libertés différentes. Il s'agit d'une part, des libertés dans leur assertion classique dite « *libertés individuelles* », c'est-à-dire des libertés dont chaque individu peut jouir isolément, en lui-même à l'instar de la liberté d'aller et venir. Il s'agit, d'autre part, « *des grandes libertés qui, n'étant pas limitées à l'individu seul, se manifestent au dehors et comportent l'action de coparticipants ou l'appel au public* » telles que la liberté d'expression (CE, avis, 13 août 1947, repris par Gilles Lebreton dans son ouvrage « Libertés publiques et droits de l'Homme », éd. Armand Colin, Paris, 4e éd. ,1999, 521, p. 15).

Certains droits et libertés, dépourvus de fondement formel, ont fait leur entrée dans le bloc de constitutionnalité grâce à leur rattachement à la liberté individuelle. C'est notamment le cas du droit au respect de la vie privée (Cons. const., 12 janv. 1977, n° 76-75 DC, Fouille de véhicules). La protection des données personnelles a été rendue nécessaire par la consécration du droit au respect de la vie privée.

Les données personnelles sont protégées juridiquement au moyen d'un ensemble de textes nationaux et communautaires. Cette protection s'inscrit dans le prolongement de la reconnaissance du droit au respect de la vie privée (I). Cependant, cette protection comporte des limites liées aux impératifs de sécurité et à la nécessité de respecter la liberté individuelle de chacun (II).

I.– LA PROTECTION JURIDIQUE DES DONNÉES PERSONNELLES, ÉMANATION DU DROIT AU RESPECT DE LA VIE PRIVÉE

Les données personnelles, en tant que composantes de la vie privée (B), bénéficient d'un cadre juridique protecteur (A).

A.– Le cadre juridique de protection des données personnelles

Le régime juridique de protection des données personnelles résulte tant du droit national que du droit de l'Union. Au sein de l'espace européen, l'objectif de protection des données personnelles a reçu un accueil très variable selon les États. Toutefois, la mise en œuvre des directives a permis de combler les écarts entre les législations nationales sans en effacer les caractéristiques pour autant. L'avènement d'internet a sensiblement accru le besoin de protection des données personnelles, le cadre juridique applicable en la matière imposant une constante redéfinition pour tenir compte des avancées technologiques.

Le droit interne

En France, le texte fondateur en matière de protection des données personnelles est la Loi de 1978. Ce texte, évoluant au gré des avancées technologiques et du droit de l'Union, a posé les bases de la protection des droits et libertés des personnes eu égard aux risques d'abus potentiel générés par le traitement automatisé de leurs données personnelles. Ce texte instituant la CNIL crée un certain nombre de sanctions administratives pouvant être prononcées par la Commission à l'égard du responsable de traitement ne respectant pas les dispositions de la Loi (Chapitre VII « Sanctions prononcées par la CNIL »). La Loi comporte également un volet pénal (Chapitre VIII « Dispositions pénales ») instituant notamment les infractions aux dispositions de la Loi, codifiées aux articles 226-16 à 226-24 du code pénal. L'instauration de ces sanctions de nature répressive souligne le souci du législateur de veiller à ce que l'informatique ne porte pas atteinte aux droits et libertés tel que l'article premier de la Loi de 1978 l'exige. Cet arsenal pénal est avant tout dissuasif. Les poursuites étaient relativement rares jusqu'à une date récente et les litiges se soldent pour la plupart par un règlement amiable à l'initiative de la CNIL.

Le rôle protecteur de la CNIL dépend de la nature des données. Une protection renforcée est mise en place concernant les traitements de données représentant un risque particulier d'atteinte aux droits et libertés, c'est-à-dire des données faisant apparaître les origines ethniques, raciales, les opinions politiques, philosophiques, religieuses, l'appartenance syndicale, l'état de santé ou l'orientation sexuelle. Le traitement et la collecte de ces données sont, par principe, interdits, mais permis par exception, sur obtention d'une autorisation préalable de la CNIL. Pour les données jugées moins sensibles, un régime de droit commun s'applique, aux termes duquel il convient de procéder à une simple déclaration auprès de la CNIL, s'engageant par l'accomplissement de cette démarche à satisfaire aux exigences légales. Il existe toutefois des exonérations à cette formalité déclarative, notamment lorsque l'entreprise ou l'organisme effectuant un traitement de données personnelles, a créé la fonction de correspondant à la protection des données (L. n° 78-17, 6 janv. 1978, art. 22, III).

En tout état de cause, en vertu de la Loi de 1978, les traitements de données personnelles doivent être effectués avec loyauté, proportionnalité et en vue d'une certaine finalité. Les juridictions ont notamment considéré comme déloyal, le fait d'avoir recours à la corruption d'agents SNCF afin qu'ils transmettent à une société d'assurance des renseignements obtenus dans l'exercice de leur activité (TGI Paris, 16 déc. 1994, Lamy Droit informatique et réseaux, 2005, n° 577).

Le droit communautaire

La Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces donnée (ci-après « la Directive »), fait également partie des textes références en matière de protection de données personnelles. Cette Directive sous-tend la conception selon laquelle le bon fonctionnement du marché intérieur nécessite la libre circulation, son seulement des personnes, des marchandises, des services et des capitaux, mais également celle des données personnelles. La Directive instaure un cadre réglementaire visant à établir un équilibre entre une protection élevée de la vie privée des personnes et la libre circulation des données personnelles au sein de l'Union européenne. Elle a été transposée en droit national par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

La Directive est à l'origine de la création d'un groupe de travail européen rassemblant les représentants des vingt-neuf autorités indépendantes de protection de données personnelles, le G29. Cette instance a un rôle essentiel en matière d'harmonisation des positions dans le cadre des négociations avec les pays situés hors de l'Union européenne, notamment les États-Unis. Le G29 a ainsi pris position publiquement à l'occasion des affaires PNR (relative à un accord permettant le transfert de données des passagers aériens européens au ministère de la sécurité intérieure des USA), SWIFT (relative à un accord passé par la Commission européenne en vertu duquel elle acceptait de transférer les données bancaires européennes au Trésor Américain) ou plus récemment PRISM (révélant un important programme de surveillance électronique des agences américaines de renseignements ; Rapport d'information Sénat n° 441 par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques, 27 mai 2009).

Enfin, la Charte des droits fondamentaux de l'Union européenne vise également à assurer la protection des données personnelles. Rappelons que cette Charte est devenue juridiquement contraignante depuis l'entrée en vigueur du Traité de Lisbonne. Elle s'adresse non seulement aux institutions de l'Union mais également aux juridictions nationales des États membres lorsqu'ils mettent en œuvre le droit de l'Union. Son article 8 « *Protection des données à caractère personnel* » prévoit ainsi que : « *1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante* ». Les termes de la Charte constituent également une référence pour la CNIL lorsqu'elle contrôle la légalité d'un système de traitement de données personnelles.

B.– La protection des données personnelles, un prolongement du droit au respect de la vie privée

L'avènement du droit à la protection de la vie privée

Les sociétés démocratiques modernes ont constitué un terrain favorable à la protection de la vie privée. Pour l'expliquer, Alexis de

Tocqueville avait recours au concept d'individualisme qu'il décrivait comme « *un sentiment réfléchi et paisible qui dispose chaque citoyen à s'isoler de la masse de ses semblables et à se retirer à l'écart avec sa famille et des amis* » (De la démocratie en Amérique, t. 2, Partie 2, chap. II). En cela, la notion de vie privée est indissociable de celle d'individu.

> *La licéité des traitements de données personnelles dépend de l'équilibre trouvé entre les intérêts du responsable de traitement et le respect de la vie privée des individus concernés.*

La reconnaissance et la protection de la vie privée sont apparues nécessaires dès le milieu du XX[e] siècle, dans un mouvement global de promotion des droits fondamentaux et des libertés publiques.

Ainsi, le droit à la protection de la vie privée *lato sensu*, impliquant donc la protection de la famille, du domicile, de la correspondance, a été consacré au niveau international par l'article 12 de la Déclaration universelle des droits de l'Homme du 10 décembre 1948, à l'article 17.1 du Pacte international relatif aux droits civils et politiques du 16 novembre 1966, ainsi qu'à l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950.

En France, le droit à la protection de la vie privée est apparu dans le droit positif en 1970 aux articles 9 du code civil et 368 du code pénal alors en vigueur (L. n° 70-643, 17 juill. 1970 tendant à renforcer la garantie des droits individuels des citoyens).

La protection des données personnelles rendue nécessaire par la consécration du droit au respect de la vie privée

C'est dans ces conditions favorables à la protection de la vie privée qu'a pu émerger une prise de conscience quant aux enjeux inhérents au traitement de données personnelles et aux risques du fichage généralisé de la population, risques mis en évidence par les politiques discriminatoires nazies notamment (Missika J.-L. et Faivret J. P., « informatique et libertés », Les temps modernes, août-sept 1977, n° 374).

En France, un projet du gouvernement connu sous le nom de SAFARI, a été révélé par le journal *Le Monde* le 21 mars 1974 dans un article intitulé « *Safari ou la chasse aux français* ». Ce projet permettait l'identification de chaque citoyen par un numéro et l'interconnexion de tous les fichiers de l'administration.

La Loi de 1978 s'inscrit dans cette perspective. Aux termes de cette dernière, le législateur a cherché à rassurer la société civile, en proclamant que « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

Le Conseil constitutionnel s'appuie fréquemment sur la notion de vie privée pour contrôler la constitutionnalité de dispositions relatives à la création de fichiers contenant des informations à caractère personnel. Ainsi, ce fut notamment le cas pour les fichiers STIC et JUDEX (Cons. const., 13 mars 2003, n° 2003-467 DC, relative à la loi pour la sécurité intérieure) ainsi que des dossiers médicaux personnels (Cons. const., 12 août 2004, n° 2004-504 DC, sur la loi relative à l'assurance maladie). Le Conseil invite ainsi au respect des « *dispositions protectrices de la liberté individuelle prévues par la législation relative à l'informatique, aux fichiers et aux libertés* » (ex. : Cons. const., 18 janv. 1995, n° 94-352 DC, considé. 10, Vidéosurveillance).

La licéité des traitements de données personnelles dépend de l'équilibre trouvé entre les intérêts du responsable de traitement et le respect de la vie privée des individus concernés. À titre d'illustration, la CNIL a considéré, dans une délibération de 2004 que les aéroports parisiens pouvaient licitement mettre en place un dispositif de reconnaissance d'empreintes digitales des employés afin de contrôler les déplacements dans les zones de sûreté (CNIL, 8 avr. 2004, délib. n° 04-017, JCP E, 2004, p. 2023). À l'inverse, les juridictions ont pu considérer qu'une filiale de la SNCF ne peut légalement instaurer un système de contrôle de temps de présence de ses employés aboutissant à la constitution d'une base de données d'empreintes digitales du personnel (TGI Paris, 19 avr. 2005, D. 2005, p. 2650).

Au sein de l'Union européenne, la Directive de 1995 lie également la question de la protection des données à la nécessité de respecter la vie privée des individus. Elle affirme que « *l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire* ». Ce texte, souligne la nécessité de protéger les données personnelles en tant que démembrement de la vie privée et place le droit au respect de la vie privée aux côtés des droits fondamentaux garantis au niveau communautaire.

Pour la Cour EDH, le lien entre l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales et la protection des données personnelles est indéniable. En effet, elle a considéré dès 1987 que « *la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8* » (CEDH, 26 mars 1987, aff. 9248/81, Leander c/ Suède ; CEDH, 25 mars 1998, aff. 23224/94, Kopp c/ Suisse ; CEDH, 16 févr. 2000, aff. 27798/95, Amann c/ Suisse). Face à l'avènement des technologies et techniques scientifiques modernes, la jurisprudence de la Cour a permis de replacer la question de la vie privée au cœur des débats. Elle a notamment retenu en matière pénale que « *la protection offerte par l'article 8 serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part* » (CEDH, 4 déc. 2008, aff. 30562/04, 30566/04, § 112, S. et Marper c/ Royaume-Uni). La Cour ne fait pas de distinction en fonction du caractère public ou privé des données. Elle considère que même « *les données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics* » (CEDH, 4 mai 2000, aff. 28341/95, § 43, Roratu c/ Roumanie).

Ainsi, la protection des données personnelles a été consacrée par le truchement du droit au respect de la vie privée de chacun. Pour autant, le droit à la protection des données personnelles s'autonomise

et doit être concilié avec la prise en compte d'intérêts concurrents. En somme, l'exercice du droit à la protection des données personnelles doit faire face à de réelles limites.

II.– LES LIMITES DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES

Le droit à la protection des données personnelles qui vient d'être exposé est menacé de deux manières qu'il convient de distinguer ci-après.

Tout d'abord, internet et les données qu'il contient offrent aux institutions de très nombreuses opportunités de traçage des individus dans une mesure qui échappe très largement au contrôle, voire parfois à la connaissance, de ces derniers. Dans un contexte de demande accrue de sécurité, ces capacités risquent d'être surexploitées, notamment dans le cadre de la lutte contre le terrorisme (A). Se développe également une nouvelle forme de traçage susceptible d'affecter le droit au respect de la vie privée des individus. Celle-ci naît d'une exposition consciente et volontaire de pans entiers de leur vie privée par ceux qui, précisément, sont les titulaires du droit à son respect (B).

A.– Les données personnelles face à l'exigence de sécurité : une recherche d'équilibre entre exploitation et protection

Les données personnelles ont cette particularité d'être à la fois des moyens pour un État de garantir la sécurité de ses ressortissants et des composantes du droit à la protection de la vie privée.

Les données personnelles comme outils de protection du droit à la sécurité

Le droit à la sécurité fût érigé en droit fondamental dans l'ordre juridique français par la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

La jurisprudence de la CEDH reconnaît l'obligation des États d'assurer la sécurité de leurs ressortissants et la valeur inestimable des données personnelles à cette fin. Les juges de Strasbourg admettent ainsi que « *les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, de sorte que l'État doit être capable, pour combattre efficacement ces menaces, de surveiller en secret les éléments subversifs opérant sur son territoire* » (CEDH, 6 sept. 1978, aff. 5029/71, § 42, Klass et a. c/ Allemagne).

Ils estiment également que « *la lutte contre la criminalité, et notamment contre le crime organisé et le terrorisme, qui constitue l'un des défis auxquels les sociétés européennes doivent faire face à l'heure actuelle, dépend dans une large mesure de l'utilisation des techniques scientifiques modernes d'enquête et d'identification* » (CEDH, 4 déc. 2008, aff. 30562/04, 30566/04, §105, S. et Marper c/ Royaume-Uni).

L'identification des auteurs d'actes terroristes étant le premier défi auquel sont confrontés les États, l'accès à certaines données immatérielles devient un enjeu stratégique majeur. La lutte contre le terrorisme implique notamment une politique de collecte des données personnelles perçue comme un outil indispensable de la protection du droit à la sécurité.

L'identification des auteurs d'actes terroristes étant le premier défi auquel sont confrontés les États, l'accès à certaines données immatérielles devient un enjeu stratégique majeur.

Comment concilier la protection des données personnelles et le droit à la sécurité ?

Le contrôle de la protection des données personnelles par la Cour européenne des droits de l'Homme et le Conseil constitutionnel

Rappelant le risque « *de saper, voire détruire la démocratie au motif de la défendre* », la CEDH affirme avec fermeté que « *les États ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée* » (Klass et a. c/ Allemagne, préc., § 9). Dans cette espèce, la Cour concluait qu'une surveillance secrète des communications et des correspondances doit être soumise à un contrôle effectif, laissant le soin aux États d'éluder la difficile question de la compatibilité entre contrôle effectif dans une société démocratique et secret défense.

En France, le Conseil constitutionnel a appliqué cette injonction, posant les critères de l'équilibre entre exploitation et protection des données personnelles. Sa décision du 22 mars 2012 sur la loi relative à la protection de l'identité en est une bonne illustration. Par cette décision, le Conseil constitutionnel censure la loi du 6 mars 2012 qui prévoyait la création d'un fichier biométrique des détenteurs d'une carte nationale d'identité. Il estime en effet que la création d'un tel fichier constitue une atteinte disproportionnée au droit au respect de la vie privée, protégé par l'article 2 de la Déclaration des droits de l'Homme et du citoyen. Pour arriver à une telle conclusion, le Conseil commence par rappeler que « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* » (consid. 8). S'attachant ensuite à étudier les modalités du traitement mis en place, le Conseil relève deux éléments clefs. Le premier est l'étendue des individus concernés par la collecte prévue, en l'occurrence la quasi-totalité de la population française. Le second élément est le type de données collectées. Il souligne alors le caractère « *particulièrement sensible* » des relevés d'empreintes digitales (consid. 10). Enfin, les juges relèvent que si l'objectif affiché de la Loi était la lutte contre l'usurpation d'identité, elle prévoyait également la consultation et l'interrogation du fichier à des fins de police administrative ou judiciaire. Ces éléments permettent ainsi au Conseil de conclure, au moyen d'un raisonnement très proche de celui de la CEDH, à une atteinte disproportionnée au droit au respect de la vie privée, eu égard aux objectifs réellement poursuivis par le législateur.

À l'inverse, dans une décision du 19 janvier 2006, le Conseil constitutionnel, procédant à la même analyse, a abouti à un arbitrage en faveur de l'exigence de sécurité. La question se posait de la constitutionnalité de l'article 8 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. La disposition prévoyait la mise en œuvre de dispositifs de photographie automatique des véhicules et de leurs occupants sur certains axes routiers et l'enregistrement provisoire de ces photographies. Les juges de la rue Montpensier

concluent qu'au regard, tant des finalités de la Loi que des garanties strictes qu'elle fixe, « *les dispositions contestées sont propres à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée* » (Cons. const.,19 janv. 2006, n° 2005-532 DC, consid. 20-21).

Si les éléments de nature à assurer un juste équilibre entre exploitation et protection des données personnelles semblent bien établis d'un point de vue juridique, cet équilibre est sans cesse remis en question par des considérations d'ordre politique et diplomatique.

> *Le développement de l'Internet et notamment des réseaux sociaux amène les individus à exposer davantage et de plus en plus tôt leur vie privée.*

Les freins à une protection juridique efficace

Aujourd'hui les arbitrages étatiques ont plutôt tendance à se positionner en défaveur de la vie privée, au profit de l'exigence de sécurité. Cette tendance peut s'expliquer de deux manières. Le développement du terrorisme et la peur des attentats qui peuvent l'accompagner accroissent indiscutablement la demande de sécurité des citoyens. Mais ce phénomène s'explique également, comme le souligne un rapport d'information du Sénat en date de 2009, par le caractère souvent indolore et invisible des procédés utilisés. Installer une caméra dans chaque lieu public ne produit pas le même effet que d'affecter un policier à chaque coin de rue (Rapport d'information du Sénat n° 441, préc.).

En outre, le caractère international, à la fois de la lutte contre le terrorisme et des flux de données dématérialisées participe très largement de la fragilité de la protection juridique de ces données. Une telle protection ne peut, dans ce contexte, exister que dès lors qu'il existe des normes, ou à tout le moins des standards, acceptés et respectés par tous les États, la réciprocité des obligations devenant un élément essentiel à la mise en place d'une protection effective.

Les discussions actuellement en cours au sein des institutions européennes, visant à réformer la directive phare en la matière qui date de 1995 (Dir. PE et Cons. CE n° 95/46/CE, préc.), ont cette ambition, dans un cadre territorial qui se limite néanmoins aux États de l'Union européenne. Les nombreuses tentatives avortées de réformation et la difficulté, tant juridique que matérielle, à imposer ces standards Outre-Atlantique (dont l'opinion publique mondiale a eu l'éclatante illustration avec le programme PRISM, cet été) laissent penser que la balance n'a pas fini de pencher vers l'exploitation, au détriment de la protection.

B.– Les données à caractère personnel face à l'exposition de soi sur l'Internet : un besoin de régulation

Le développement de l'Internet et notamment des réseaux sociaux amène les individus à exposer davantage et de plus en plus tôt leur vie privée, comme le souligne la CNIL dans ses publications sur le sujet (Les perspectives pour 2012-2013 : la régulation des données personnelles au service d'une véritable « éthique du numérique », <www.cnil.fr>, 10 juill. 2012).

Ces réseaux ne sont pas et n'ont pas vocation à être une zone de non-droit. La difficulté juridique posée ici est celle de la protection des données personnelles, non pas contre des captations externes comme c'est le cas dans le cadre de la lutte contre le terrorisme, mais, en amont, contre leur diffusion par leurs propres propriétaires. Dans l'un comme dans l'autre des cas, le risque premier est celui du détournement des données à des fins étrangères à celles pour lesquelles elles ont été diffusées.

La position « responsabilisante » de la Cour européenne des droits de l'Homme

Quelle garantie de protection pour des données à caractère personnel diffusées volontairement par leur détenteur ? Pour la CEDH, « *la révélation antérieure par l'intéressé lui-même, des informations litigieuses est un élément essentiel de l'analyse de l'immixtion reprochée (...) dans certains aspects de la vie privée (...). En effet, les informations, une fois portées à la connaissance du public par l'intéressé lui-même, cessent d'être secrètes et deviennent librement disponibles (...). Selon la Cour, les révélations* [par l'intéressé] *une fois rendues publiques, affaiblissent le degré de protection à laquelle ce dernier pouvait prétendre au titre de sa vie privée, s'agissant désormais de faits notoires et d'actualité (...). De l'avis de la Cour, c'est pourtant là un critère déterminant dans l'appréciation de l'équilibre à ménager entre le droit de la requérante à la liberté d'expression et celui* [de la personne en cause] *au respect de sa vie privée. Dans la mesure où la requérante a repris, sans les déformer, une partie des informations librement divulguées et rendues publiques* [par l'intéressé] *la Cour est d'avis que celui-ci ne conservait plus une « espérance légitime » de voir sa vie privée effectivement protégée* » (CEDH, 23 juill. 2009, aff. 12268/03, Hachette Filipacchi c/ France).

La Cour, sans aller jusqu'à exclure d'office le caractère privé de toute donnée volontairement diffusée, estime que cette circonstance est de nature à affaiblir significativement la protection des données personnelles. Elle opte ainsi pour une position « *reponsabilisante* » pour les utilisateurs de l'Internet. Libres du choix de ce qu'ils diffusent, ces derniers réduisent ainsi plus ou moins significativement la sphère de leur vie privée, au sens juridique, au sens de ce qui bénéficie d'une protection.

Si cette position est légitime, notamment parce qu'elle s'attache à garantir le libre exercice par les internautes de leurs libertés d'expression et de communication, elle est discutable sur deux points. Tout d'abord, il est manifeste que le fonctionnement et le principe même des réseaux sociaux encouragent leurs utilisateurs à dévoiler un grand nombre d'informations sur leur vie privée. Au point que le caractère purement volontaire de la démarche de diffusion des utilisateurs est entamé. Par ailleurs, la difficulté essentielle ici n'est pas tant celle de la diffusion ou non d'une donnée que celle de la perte de contrôle de celle-ci par son propriétaire une fois qu'elle est en ligne. Les utilisateurs ont besoin, pour être pleinement responsables de la protection de leurs données, d'outils leur permettant de maîtriser réellement leur diffusion.

La nécessaire dynamique de régulation

La CNIL s'est ainsi donnée pour mission de fournir « *des clés pour un usage maîtrisé et responsable du numérique* », mission qui « *passe notamment par une éducation numérique partagée et portée par différents acteurs* » (Les perspectives pour 2012-2013 : la régulation des données personnelles au service d'une véritable « éthique du numérique », préc.).

C'est également le sens d'une recommandation du Conseil de l'Europe de 2012 qui reconnaît le rôle des réseaux sociaux comme « *moyens de promotion des droits de l'homme et catalyseur en faveur de la démocratie* ». Elle invite néanmoins les États membres à adopter des mesures pour « *aider les individus dans leur utilisation des réseaux sociaux* » et « *garantir le droit au respect de la vie privée des utilisateurs* » face aux nombreux traitements de leurs données à caractère personnel (Recomm. CM/Rec(2012) du Comité des ministres aux États membres sur la protection des droits de l'homme dans le cadre des réseaux sociaux, 4 avr. 2012).

Dans le même ordre d'idées, une Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche a été adoptée dans le cadre de l'UE le 13 octobre 2010. Sont contenues dans cette Charte des « *Bonnes pratiques à adopter par les sites collaboratifs (réseaux sociaux, blogs, forums, sites de publication de contenu, messagerie) et les moteurs de recherche pour ce qui concerne les données publiées intentionnellement. L'objectif est de mieux garantir le respect de la vie privée pour les internautes en leur permettant d'exercer simplement un meilleur contrôle sur les données qu'ils ont publiées* ». Sa portée est cependant très limitée, d'autant que ni Facebook, ni Google n'ont souscrit cet engagement.

La refonte actuellement en discussion des règles européennes de protection des données personnelles sur l'Internet a pour objectif d'introduire un réel « *droit à l'oubli* » et de « *renforcer l'information des personnes sur le traitement de leurs données en rendant celui-ci plus lisible et plus accessible* » (Recomm. CM/Rec(2012) du Comité des ministres aux États membres sur la protection des droits de l'homme dans le cadre des réseaux sociaux, 4 avr. 2012). L'enjeu de cette réforme est ni plus ni moins de passer d'un dispositif de « *soft law* » (encouragements à l'autorégulation tant des opérateurs des réseaux que leurs utilisateurs) à celui de « *hard law* » visant à garantir l'effectivité du droit à la protection des données personnelles y compris lorsque les utilisateurs ont fait un usage immodéré des droits qui sont les leurs. ■

L'entreprise et la protection des données personnelles

Les entreprises sont à la fois victimes potentielles de cyber-attaques et responsables des traitements de données personnelles engendrés par leurs activités. Cette situation particulière leur impose de mettre en œuvre une politique de gestion des risques tant internes qu'externes en matière de données personnelles, conciliant l'exigence sécuritaire aux intérêts légitimes de l'entreprise et aux droits fondamentaux de protection des données personnelles et de respect de la vie privée, à la faveur d'une nouvelle culture d'entreprise intégrant l'impératif de protection des données et sensibilisant tous les acteurs de l'entreprise aux rôles et responsabilités de chacun.

Par Emilie BAILLY

Avocat
Cabinet Vigo

Et Clarisse LE CORRE

Avocat
Cabinet Vigo

→RLDA 4843

Les traitements de données à caractère personnel sont omniprésents pour les opérateurs économiques, *via* des réseaux internes et externes (*cloud computing*, big data, réseaux d'entreprise/intranet, bases de données, internet, etc.), et ce pour des finalités tant diverses qu'essentielles à l'entreprise (recrutement, géolocalisation, vidéosurveillance, contrôle de l'accès physique aux locaux, contrôle des horaires, messagerie électronique, transactions économiques et financières, transferts de données à l'étranger, etc.). Ces traitements visent tous les interlocuteurs de l'entreprise, internes comme externes à celle-ci – salariés, clients, consommateurs, prospects, concurrents, partenaires et autres tiers–.

Les entreprises sont, par conséquent, soumises aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, loi dite « *Informatique et Libertés* », et doivent composer avec l'impératif de protection des données personnelles.

Or, selon une enquête de l'IFOP pour MAKAZI GROUP, spécialiste du data marketing, seuls 14 % des 300 chefs d'entreprise interrogés estiment être parfaitement au fait de la législation en vigueur dans ce domaine. Si 47 % pensent la connaître « *assez bien* », près de deux sur cinq reconnaissent qu'ils la connaissent mal, voire très mal (<http://www.01net.com/editorial/603686/donnees-personnelles-39pour-cent-des-dirigeants-francais-connaissent-mal-la-legislation/> [dernière consultation : 10 oct. 2013]), méconnaissance de la règlementation qui est susceptible d'engager la responsabilité administrative, civile et pénale des personnes morales, en dépit de leur bonne foi.

La conformité à la règlementation applicable est d'autant plus difficile, notamment pour les TPE/PME, que les régimes de protection européens des données personnelles sont particulièrement évolutifs et fragmentés, ce qui place les opérateurs économiques dans une situation d'insécurité juridique préoccupante (Proposition de règlement du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, 7 févr. 2013, COM(2013) 48 final, 2013/0027 (COD), disponible à : <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf> [dernière consultation :10 nov. 2013], p. 2).

> *Seuls 14 % des 300 chefs d'entreprise interrogés estiment être parfaitement au fait de la législation en vigueur dans ce domaine.*

Au-delà du risque interne qui résulte de la non-conformité à la loi « *Informatique et Libertés* », l'entreprise doit se prémunir contre le risque externe d'éventuelles intrusions frauduleuses dans ses systèmes informatiques susceptibles de provoquer la perte, le détournement ou encore l'altération des traitements de données à caractère personnel. Car si l'usage des nouvelles technologies constitue un outil pour l'accroissement de la compétitivité de l'entreprise, il la rend également plus vulnérable, « *ce qui l'oblige à repenser sa politique de sécurité pour parer notamment à des attaques venues de l'extérieur ou à la fuite d'information* » (Achilleas P., J.-CL. Libertés, Fasc. 820 : Internet et libertés, § 83).

Plus de six entreprises françaises sur dix ont subi au moins un accident de sécurité en 2011. Elles n'étaient qu'une sur trois en 2010. De fait, seuls 55 % des entreprises ont confiance en leur sécurité (« Global State of Information, Security Survey 2013, Tendances et enjeux de la sécurité de l'information », Étude réalisée par le cabinet PwC, publiée le 30 janv. 2013). Les attaques malveillantes et criminelles constituent la première cause de

la violation des données en France (42 % des cas). 31 % des violations de données résultent de négligences humaines (erreurs qui incluent notamment un mauvais traitement des données par les employés, un défaut de contrôle, le non-respect de la règlementation), 27 % résultant quant à elles d'erreurs système. En moyenne, 22 242 données sont compromises par incident (« Cost of Data Breach :France », Étude réalisée par Ponemon Institute, sponsorisée par Symantec, publiée le 5 juin 2013).

56 % des entreprises françaises victimes de fraude indiquent qu'elles ont été commises par un fraudeur interne.

Les conséquences de ces failles de sécurité sont lourdes pour les entreprises. Des conséquences commerciales, d'une part. La France est le pays où les conséquences commerciales des violations de données sont les plus lourdes, avec un taux d'attrition des clients de 4,4 %, et un coût relevant des pertes d'activité ou de contrats (perte de clients, difficulté à acquérir des nouveaux clients, dégradation de l'image) établi à 1,19 millions d'euros en 2012. Des conséquences financières, d'autre part, puisque le coût lié aux violations de données a augmenté de 11 % en France pour s'établir à 2,86 millions d'euros, contre 2,55 millions d'euros en 2011. Le coût moyen par donnée compromise s'élève à 127 euros en 2012, contre 122 euros en 2011, soit une augmentation de 4,1 % (« Cost of Data Breach :France », préc.).

L'enjeu de la mise en œuvre d'une politique de sécurité efficiente par les opérateurs économiques est d'autant plus conséquent que les données personnelles collectées et traitées par ceux-ci ont une valeur patrimoniale qui attise les convoitises. Le *Financial Times* a d'ailleurs récemment mis en ligne un simulateur permettant d'évaluer le prix de nos données personnelles (<http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz2h9t2kGZ5> [dernière consultation : 17 oct. 2013]).

Les données à caractère personnel peuvent constituer une part non négligeable du patrimoine d'une entreprise. Il existe dès lors un véritable « *marché* » des données personnelles, lesquelles se monnaient entre les différents acteurs de la vie économique – la FNAC a acquis récemment, dans le cadre de la liquidation de VIRGIN, le fichier-clients du distributeur culturel comportant près de 1,6 millions de noms, pour la somme de 54 000 euros. Corollaire de cette valorisation économique des données personnelles, il s'est créé un « *marché noir* » des données personnelles obtenues grâce à des activités illicites sur les réseaux informatiques, notamment des intrusions frauduleuses dans les systèmes informatiques d'entreprises insuffisamment protégées.

L'entreprise constitue aujourd'hui un levier fondamental de l'effectivité de la politique de protection des données personnelles. Il est dès lors indispensable que l'entreprise compose avec le nouveau rôle qui est le sien, ce qui implique une gestion des risques tant internes (I) qu'externes (II) à l'entreprise en matière de protection des données à caractère personnel. La présente étude vise à appréhender, outre le cadre juridique existant et les obligations qui en découlent pour les entreprises, la politique sécuritaire des entreprises en matière de collecte, traitement et conservation des données à caractère personnel.

I.– L'IMPÉRATIF DE PROTECTION DES DONNÉES PERSONNELLES DANS L'ENTREPRISE : LA GESTION DU « *RISQUE INTERNE* » À L'ENTREPRISE

56 % des entreprises françaises victimes de fraude indiquent qu'elles ont été commises par un fraudeur interne. Le cyber-fraudeur serait ainsi « *un employé dans 85 % des cas, qui dispose de moins de cinq ans d'ancienneté au sein de l'entreprise dans 51 % des cas et est âgé de moins de 40 ans dans 65 % des cas* » (La fraude en entreprise : tendances et risques émergents », 6e éd., Global Economic Crime Survey 2011, Étude réalisée par le cabinet PwC, 2011).

En matière de protection des données personnelles, la gestion du risque interne, c'est-à-dire du risque résultant de l'organisation et du fonctionnement de l'entreprise, suppose une parfaite connaissance de la loi « *Informatique et Libertés* » et surtout la sensibilisation des salariés aux problématiques liées à la protection des données personnelles, précisant notamment les rôles et les responsabilités de chacun (A).

La maîtrise du risque interne justifie par ailleurs la mise en place de dispositifs de surveillance des salariés et le recours accru aux nouvelles technologies pour endiguer notamment le développement des fraudes aux systèmes d'information en interne. Les dispositifs de surveillance des salariés sont toutefois très encadrés et doivent être pertinents, proportionnés et s'opérer dans le respect de la vie privée des salariés et des données personnelles ainsi collectées (B).

A.– La sensibilisation, à tous les niveaux de l'entreprise, aux problématiques liées à la protection des données à caractère personnel

1. *L'émergence d'une culture d'entreprise intégrant l'impératif de protection des données personnelles*

Les entreprises ont mis en place un ensemble de dispositifs techniques, normatifs et organisationnels, de façon à diffuser les bonnes pratiques en leur sein, assurer leur conformité à la règlementation applicable en matière de protection des données personnelles et, ainsi, réduire le coût et l'impact de la violation des données.

Cette réactivité des entreprises se traduit par des mesures organisationnelles et process visant à prévenir la violation des systèmes d'information : élaboration ou renforcement de la politique de sécurité des systèmes d'information, programme de lutte et d'identification des incidents de sécurité, création d'une cellule de crise en interne pour gérer les violations de données, formation et information des salariés, communication interne et externe sur la politique de sécurité de l'entreprise, autant d'éléments qui mettent en exergue le rôle dorénavant prépondérant des RSSI / DSI au sein de l'entreprise, mais également celui du correspondant informatique et libertés (CIL), dont l'action peut prendre plusieurs formes – conseil, recommandations, sensibilisation, médiation et alerte en cas de disfonctionnement.

Il s'agit aussi pour l'entreprise de mieux gérer les violations de données lorsqu'elles se réalisent (définition en amont des mesures techniques et organisationnelles à mettre en œuvre, reporting immédiat, modalités de la communication au public sur l'incident, etc.).

Il s'opère par ailleurs un développement des chartes de protection des données personnelles, chartes informatiques et codes éthiques relatifs à la sécurité des données personnelles et au respect de la vie privée des salariés et des consommateurs. Ces derniers formalisent les bonnes pratiques afin de les uniformiser, les diffuser dans l'entreprise, et augmenter leur applicabilité par les collaborateurs concernés, permettant « *non seulement de présenter au personnel une ligne de conduite claire et précise en la matière, mais aussi de communiquer de manière positive sur ces bonnes pratiques auprès des clients et du public* ». De même, les entreprises développent en partenariat avec la CNIL des « *règles d'entreprise contraignantes* » ou BCR (Binding Corporate Rules), codes de conduite internes qui définissent la politique d'un groupe en matière de transfert de données hors de l'Union européenne, visant à assurer un niveau de protection suffisant aux données transférées vers un pays tiers.

Il résulte de cette évolution des pratiques que la protection des données personnelles fait aujourd'hui partie intégrante de la culture d'entreprise, constituant dorénavant un facteur avec lequel les acteurs économiques doivent impérativement composer.

La sécurité des données est un enjeu stratégique et social pour les entreprises (La protection des données : un enjeu stratégique et social, Questions à Isabelle Falque-Pierrotin, Présidente de la CNIL, Hebdo édition affaires n° 309, 20 sept. 2012) et s'intègre progressivement au volet social de la responsabilité sociale de ces dernières (RSE). Les principes directeurs de l'OCDE à l'intention des entreprises multinationales, par lesquels l'OCDE émet des recommandations pour une conduite responsable des entreprises dans le contexte international, visent désormais expressément la sécurité des données à caractère personnel collectées, conservées, traitées ou diffusées par les entreprises (Principes directeurs de l'OCDE à l'intention des entreprises multinationales, révisés par réunion ministérielle de l'OCDE le 25 mai 2011). Il en va de même pour la norme internationale d'application volontaire ISO 26000:2010, ainsi que la norme ISO/IEC 27002:2013 relative à la gestion de la sécurité de l'information au sein de tout organisme.

Comme le souligne Isabelle Falque-Pierrotin, Présidente de la CNIL, ce développement a pour origine « *une vision utilitariste dans laquelle l'éthique n'a que peu de place : il s'agit de donner à l'entreprise un avantage concurrentiel, en suscitant la motivation des salariés ou en prévenant les atteintes à la réputation de l'entreprise* » (La protection des données : un enjeu stratégique et social, préc.). Il n'en demeure pas moins que l'impératif de protection des données personnelles figure aujourd'hui au rang des préoccupations éthiques de l'entreprise et impose aux opérateurs économiques davantage de transparence envers leurs salariés, clients et partenaires, dans la collecte et le traitement de leurs données personnelles.

2. *La consécration du rôle moteur des entreprises en matière de protection des données personnelles par le projet de réforme du cadre juridique européen*

La proposition de règlement d'application directe dans l'ensemble des États membres de l'Union européenne, appelé à remplacer la Directive européenne de 1995 (Proposition de règlement du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, 7 févr. 2013, COM(2013) 48 final, 2013/0027 (COD)) et dont le texte définitif devrait être adopté en 2014 pour une entrée en vigueur deux ans plus tard, prévoit la fin des formalités administratives pesant jusqu'alors sur les entreprises et, dans le même temps, le développement de la gouvernance des normes internes des entreprises.

L'article 22 du projet de règlement stipule que « *le responsable du traitement adopte des règles internes et met en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du présent règlement* ». Cela implique que l'entreprise, au même titre que tout responsable de traitements de données, devra pouvoir justifier de la conformité des traitements au règlement européen et mettre en œuvre des mesures telles que :

- la tenue d'une documentation permettant de conserver la trace de tous les traitements effectués et leurs caractéristiques ;

- la mise en œuvre d'obligations en matière de sécurité des données ;

- la réalisation d'analyses d'impact des traitements de données jugées à risque ;

- l'adoption de règles contraignantes internes visant notamment à encadrer les transferts transfrontaliers de données ;

- la désignation d'un délégué à la protection des données (équivalent du CIL dans le dispositif français, dont la désignation est aujourd'hui facultative) ;

- l'élaboration de codes de bonne conduite, facultative mais encouragée par le projet de règlement.

Le projet de règlement européen n'a pas d'incidence sur les sanctions pénales applicables aux manquements aux règles en matière de protection des données personnelles. Il en va différemment pour les sanctions administratives susceptibles d'être prononcées, dans la mesure où l'article 79 du projet de règlement prévoit des amendes allant de 0,5 % à 2 % du chiffre d'affaires mondial pour les personnes morales et de 250 000 euros à 1 million d'euros pour les personnes physiques, soit une augmentation considérable du montant susceptible d'être prononcé (pour mémoire, les entreprises peuvent aujourd'hui être condamnées, en application de l'article 47 de la loi « *Informatique et Libertés* », à des sanctions pécuniaires pouvant atteindre au maximum 150 000 euros – 300 000 euros en cas de récidive). Il sera précisé que le montant de l'amende administrative est fixé en tenant compte de la nature, de la gravité et de la durée de la violation, du fait que l'infraction ait été commise délibérément ou par négligence, du degré de responsabilité du mis en cause et des éventuelles violations commises antérieurement, des mesures et procédures techniques et d'organisation mises en œuvre ainsi que du degré de coopération avec l'autorité de contrôle en vue de remédier à la violation.

Ainsi, le projet de règlement européen met fin à la possibilité pour l'entreprise de se retrancher derrière l'accomplissement des formalités administratives pour tenter de s'exonérer de sa responsabilité et confère aux opérateurs économiques un rôle fondamental et proactif en matière de protection des données personnelles, notamment pour mieux sécuriser les flux transfrontaliers de données et prévenir de façon effective la cybercriminalité.

Si ce projet de refonte du cadre juridique européen s'inscrit dans la continuité du développement de la gouvernance des normes internes d'entreprise, il est indispensable pour les opérateurs économiques d'anticiper les obligations qui devraient très rapidement s'imposer à elles en matière de protection des données personnelles. Ces obligations auront, de toute évidence, un impact sur la gestion des risques internes à l'entreprise, notamment en matière de surveillance et de gestion de l'activité des salariés.

B.– La surveillance des salariés

Le salarié bénéficie du principe général du droit au respect de sa vie privée, en application de l'article 9 du code civil et de l'article 8 de la Convention européenne des droits de l'Homme. La Cour européenne des droits de l'Homme retient ainsi qu' « *aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de vie privée* » (CEDH, 4 mai 2000, aff. 28341/95, Rotaru c/ Roumanie, D. 2001., p. 1988, obs. Lepage A.), la Cour de cassation considérant au même titre que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée* » (Cass. soc., 2 oct. 2001, n° 99-42.942, Sté Nikon France, Bull. civ. V, n° 291).

> *En définitive, la protection des systèmes informatiques et des données personnelles qu'ils contiennent contre d'éventuels agissements déloyaux d'employés constitue un intérêt légitime de l'entreprise.*

Des aménagements à ce principe général sont possibles pour répondre aux intérêts légitimes de l'entreprise, le Code du travail précisant que « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* » (C. trav., art. L. 1121-1).

En d'autres termes, l'utilisation de procédés de surveillance susceptibles de porter atteinte aux droits et libertés des personnes, notamment au droit au respect de la vie privée, doit reposer sur un motif légitime (1) et respecter une condition de proportionnalité (2), outre le formalisme imposé par le Code du travail (3).

1. *L'intérêt légitime de l'entreprise*

La notion d'intérêt légitime de l'entreprise n'est définie par aucun texte légal. Toutefois, il est communément admis que l'intérêt légitime de l'entreprise est caractérisé lorsque l'employeur, à des fins disciplinaires, effectue une surveillance de ses employés, pour des motifs tombant dans l'une des deux catégories suivantes :

- la sécurité des biens ou des personnes (vol, vandalisme, agression ou harcèlement, etc.) ;

- des motifs économiques (exécution du travail des salariés et leur rendement).

En définitive, la protection des systèmes informatiques et des données personnelles qu'ils contiennent contre d'éventuels agissements déloyaux d'employés constitue un intérêt légitime de l'entreprise.

L'employeur dispose de divers moyens techniques pour surveiller l'activité des salariés : cybersurveillance (contrôle des connexions internet et de la messagerie électronique), géolocalisation, vidéosurveillance, autocommutateur téléphonique, contrôle d'accès par badgeage ou biométrie, système d'alertes professionnelles, etc.

Ces dispositifs sont autant de traitements de données personnelles, dès lors qu'ils enregistrent de nombreuses informations sur les salariés visés. À ce titre, ces derniers sont soumis à la réglementation relative à la protection des données personnelles (conditions de validité de la collecte et du traitement de données à caractère personnel, formalités administratives préalables, obligation d'information des personnes sur l'existence du traitement et les droits y afférents, obligation de sécurité et de confidentialité des données, etc.).

Ils doivent notamment se conformer au principe de proportionnalité, lequel impose que les données collectées soient « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* » (L. n° 78-17, 6 janv. 1978, art. 6, loi dite « *Informatique et Libertés* »). En d'autres termes, l'employeur ne peut pas, au nom de la protection des systèmes informatiques de l'entreprise et des données personnelles qu'ils contiennent, porter atteinte au droit à la protection des données personnelles et au respect de la vie privée dont les salariés peuvent eux-aussi se prévaloir.

2. *Le principe de proportionnalité*

La loi « *Informatique et Libertés* » et le Code du travail imposent à l'employeur de ne traiter, dans les dispositifs de surveillance des salariés, que les informations pertinentes et nécessaires au regard des objectifs poursuivis. L'impératif de sécurité doit ainsi s'accorder aux droits fondamentaux : il s'agit de trouver un équilibre entre la protection des intérêts de l'entreprise et la protection de la vie privée des salariés.

Faisant application du critère de proportionnalité, la CNIL est ainsi revenue sur la possibilité pour les entreprises de mettre en œuvre des dispositifs biométriques reposant sur le contour de la main aux fins de gestion des horaires des salariés, aux motifs que « (...) *son recours implique d'utiliser une partie de son corps, ce qui en soi est disproportionné au regard de la finalité de gestion des horaires* » – le recours à la biométrie est toutefois toujours autorisé s'agissant du contrôle d'accès des salariés et visiteurs ainsi que de la restauration sur les lieux de travail .

L'essentiel des contrôles et sanctions de la CNIL portent d'ailleurs sur la vidéosurveillance, la géolocalisation et la biométrie. La CNIL a ainsi prononcé une amende de 10 000 euros à l'encontre d'une société pour avoir, en dépit de la mise en demeure de mise en conformité adressée par la CNIL, manqué à l'obligation de proportionnalité du dispositif de vidéosurveillance (la société ayant placé au moins un de ses salariés sous une surveillance permanente et constante, situation qui a perduré en dépit de la mise en demeure pour mise en conformité adressée par la CNIL), à l'obligation d'information des salariés visés par le traitement, ainsi qu'à l'obligation d'assurer la sécurité des données (la CNIL relève notamment « *la brièveté des mots de passe* [permettant l'accès aux ordinateurs et aux données personnelles contenues dans ces derniers], *leur déductibilité, leur simplicité et l'absence de renouvellement* » : CNIL, Délib. formation restreinte n° 2013-139, 30 mai 2013, SAS Professional service consulting). Une sanction pécuniaire d'un montant de 10 000 euros a également été prononcée à l'encontre d'une société ayant refusé de

communiquer à l'un de ses salariés les données dont il demandait communication (données collectées par le système de géolocalisation mis en place sur son véhicule de service), ce refus constituant un manquement à l'obligation de garantir le droit d'accès (CNIL, Délib. formation restreinte n° 2013-213, 22 juin 2013, Sté Équipements Nord Picardie).

De même, la CNIL s'est récemment inquiétée de l'emploi par certaines entreprises de logiciels espions particulièrement intrusifs, les « *keyloggers* », capables d'enregistrer toutes les actions effectuées par les salariés sur leur poste informatique sans que ceux-ci s'en aperçoivent. La CNIL a ainsi rappelé que de telles pratiques, qui permettent une surveillance constante et permanente sur l'activité professionnelle des salariés concernés mais aussi sur leur activité personnelle résiduelle, sont totalement disproportionnées et ne se justifient que par un « *fort impératif de sécurité* », par exemple dans les domaines d'activité sensibles ou à très haute valeur ajoutée, pour lutter contre l'espionnage industriel (Flche pratique CNIL, Keylogger : des dispositifs de cybersurveillance particulièrement intrusifs, 20 mars 2013).

Enfin, la mise en place de dispositifs de surveillance des salariés doit être accompagnée d'une information spécifique, par l'employeur, des personnes concernées.

3. *Le formalisme imposé par le Code du travail*

La mise en œuvre de dispositifs de surveillance des salariés par l'entreprise doit faire l'objet d'une information préalable de ces derniers.

Le Code du travail prévoit qu'aucune information concernant personnellement un candidat à un emploi ou un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance (C. trav., art. L. 1221-9 et L.1222-4). De même, le comité d'entreprise doit être (i) informé de tous traitements automatisés de gestion du personnel, préalablement à leur introduction dans l'entreprise, et toute modification de ceux-ci, et (ii) informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés (C. trav., art. L. 2323-32).

> *Bien qu'étroitement encadrée par le législateur, la surveillance des salariés contribue à la maîtrise du risque interne à l'entreprise en matière de protection des données personnelles.*

La jurisprudence retient ainsi que l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés durant le temps du travail, seul l'emploi de procédés clandestins de surveillance étant jugé illicite (Cass. soc., 14 mars 2000, n° 98-42.090, Bull. civ. V, n° 101). L'employeur ne peut mettre en œuvre un dispositif de contrôle des salariés qui n'a pas été préalablement porté à la connaissance de ces derniers (Cass. soc., 22 mai 1995, n° 93-44.078, Bull. civ. V, n° 164 ; Cass. soc., 15 mai 2001, n° 99-42.219, Bull. civ. V, n° 167), et ce même s'il ne pouvait être sérieusement allégué que le salarié ignorait l'existence du dispositif de contrôle (Cass. soc., 7 juin 2006, n° 04-43.866, Bull. civ. V, n° 206).

Bien qu'étroitement encadrée par le législateur, la surveillance des salariés contribue à la maîtrise du risque interne à l'entreprise en matière de protection des données personnelles. Le cadre juridique qui vient d'être décrit constitue dès lors un socle pour l'entreprise dans la définition de mesures de prévention des atteintes internes aux données personnelles traitées par cette dernière.

Outre les menaces internes, l'entreprise doit se prémunir contre un risque externe d'atteinte aux données personnelles, prévention qui constitue par ailleurs une obligation légale, dont le non-respect est susceptible d'engager sa responsabilité.

II.– L'IMPÉRATIF DE PROTECTION DES DONNÉES PERSONNELLES DANS L'ENTREPRISE : LA GESTION DU « *RISQUE EXTERNE* » À L'ENTREPRISE

Malgré l'amélioration des politiques de sécurité des systèmes et réseaux d'informations, les entreprises sont régulièrement victimes de vols de données, qui sont ensuite revendues à d'autres, concurrents ou non. Le deuxième opérateur mobile en Allemagne, Vodafone GmbH, a ainsi récemment été victime d'un piratage de grande ampleur, permettant à un ou plusieurs cybercriminels de voler les noms, adresses, dates de naissance, sexes et coordonnées bancaires de près de deux millions d'abonnés.

Dans une position arrêtée en première lecture le 4 juillet 2013, le Parlement européen indique que « *des cyberattaques à grande échelle sont susceptibles de provoquer des dommages économiques notables, tant du fait de l'interruption des systèmes d'information et des communications qu'en raison de la perte ou de l'altération d'informations confidentielles importantes d'un point de vue commercial ou d'autres données. Il y a lieu en particulier de veiller à sensibiliser les petites et moyennes entreprises innovantes aux menaces liées à ces attaques et à leur vulnérabilité à cet égard, en raison de leur dépendance accrue à l'égard du bon fonctionnement et de la disponibilité des systèmes d'information et de leurs ressources limitées en matière de sécurité de l'information* » (Proposition du Parlement européen arrêtée en première lecture le 4 juill. 2013 en vue de l'adoption de la directive 2013/40/UE du Parlement européen et du Conseil relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil).

Le constat d'un tel risque externe à l'entreprise conduit à faire peser sur les opérateurs économiques une obligation de protection des systèmes d'informations et des données (A). Le droit pénal vient par ailleurs apporter un ensemble de réponses en cas de réalisation d'attaques à l'intégrité des données personnelles, par la définition de qualifications pénales (B).

A.– L'obligation de protection des données personnelles par l'entreprise

1. *Le cadre légal de l'obligation de protection des données personnelles par l'entreprise*

L'obligation de sécurisation des données résulte de l'article 226-17 du code pénal (l'article 226-17 du code pénal dispose que « *le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* »), lequel renvoie à l'article 34 de la loi « *Informatique et Libertés* », qui prévoit l'obligation à la charge de tout responsable de traitement 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 ».

Ainsi, le fait de ne pas prendre toutes les « *précautions utiles* » pour protéger un traitement comportant des données personnelles est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

L'obligation de sécurisation des données personnelles ainsi définie demeure imprécise, s'agissant notamment de la définition des « *précautions utiles* » à adopter par le responsable de traitement. En définitive, il s'agit pour les entreprises de mettre en œuvre des mesures appropriées et efficaces en vue de garantir la protection des données personnelles, et d'être en mesure de justifier la mise en œuvre de ces dernières.

Pour aider les entreprises à assurer leur conformité aux dispositions susvisées et prévenir les failles de sécurité, la CNIL a publié en 2010 un guide présentant les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement de données à caractère personnel (Guide CNIL, La sécurité des données personnelles, éd. 2010), en matière d'authentification des utilisateurs (mot de passe individuel, complexe et secret), de gestion des habilitations et de sensibilisation des utilisateurs, de sécurité des postes de travail (verrouillage automatique des postes de travail inactifs), de sécurisation de l'informatique mobile, de maintenance, de sécurité des locaux (vérification des habilitations et des accès par badge nominatif, digicode, contrôle des prestations de gardiennage, etc.), de sécurité du réseau informatique interne (gestion des accès et habilitations informatiques), de sécurité des serveurs et des applications (sauvegardes régulières), d'archivage et de sous-traitance.

Deux guides complémentaires ont été publiés par la CNIL en 2012 pour améliorer la maîtrise des traitements complexes, proposant une méthode pour identifier et traiter les risques ainsi qu'un ensemble détaillé de mesures et de bonnes pratiques (Guide CNIL, Gestion des risques vie privée, Parties I « La méthode » et II « Catalogue de mesures », éd. 2012). La CNIL formule notamment des recommandations en termes de modalités de sauvegarde des données, de protection des archives, de contrôle de l'intégrité des données, de traçabilité de l'activité sur le système informatique, de gestion des atteintes à la sécurité, de contrôle des accès logiques et physiques, de lutte contre les codes malveillants et de réduction des causes de vulnérabilité des réseaux et systèmes informatiques.

2. *Les enjeux du respect de la protection des données personnelles par l'entreprise*

Les enjeux de la sécurisation des systèmes d'information de l'entreprise sont considérables. Toute violation de l'intégrité de ces derniers emporte des risques lourds pour l'entreprise – entrave au bon fonctionnement de l'entreprise, atteinte aux éléments constitutifs du patrimoine de l'entreprise (vols de fichiers, vols d'informations, contrefaçons, concurrences déloyales et parasitismes économiques), violation des secrets de l'entreprise (espionnage industriel), conséquences commerciales et financières.

L'entreprise qui laisse courir en son sein des risques d'atteinte à la protection des données personnelles et à la sécurité de ses systèmes d'informations s'expose à des sanctions administratives publiques ou non publiques – avertissement ou sanction pécuniaire (sur l'année 2012, 13 sanctions ont été prononcées dont 9 avertissements et 4 sanctions pécuniaires oscillant entre 1 000 et 10 000 euros. Les manquements retenus par la CNIL ont été, pour l'essentiel, la collecte déloyale de données, le défaut des formalités préalables, le défaut de sécurité et de confidentialité des bases de données, le défaut d'information de la personne visée par le traitement, le non-respect du droit d'accès, ainsi que le non-respect du principe de proportionnalité du dispositif : Rapport d'activité CNIL, 2012, p. 58) – ainsi que des sanctions pénales (C. pén., art. 226-16 à 226-24) et civiles, la responsabilité civile de l'entreprise pouvant être engagée par tout tiers (salarié, client, partenaire) justifiant d'atteinte à la protection de ses données personnelles lui causant un préjudice et dont il est sollicité réparation (Griguer M., Protection des données personnelles : conformité et bonnes pratiques des entreprises, Cah. dr. entr. n° 1, janv. 2013, prat. 5).

Plus encore, les manquements à la protection des données comportent des risques substantiels d'atteinte à l'image et la réputation de l'entreprise, dont les conséquences économiques peuvent se révéler désastreuses notamment pour les sociétés cotées, les failles de sécurité étant de ce fait considérées comme des « *risques systémiques* » pour les entreprises (Griguer M., préc.). Pour mémoire, la cyber-attaque de la multinationale Sony, au cours du mois d'avril 2011, qui a exposé les données personnelles (notamment les coordonnées bancaires et les identifiants) des 77 millions d'utilisateurs du PlayStation Network, a entraîné une chute du cours de bourse immédiate de près de 5 %, à laquelle s'est ajouté le coût de la maintenance, de la sécurisation du réseau et des compensations pour les consommateurs, ainsi qu'une sanction pécuniaire de 250 000 livres prononcée en janvier 2013 par l'Information Commissioner's Office (ICO), l'équivalent britannique de la CNIL.

B.– Les réponses du droit pénal en cas de réalisation du risque d'atteinte à l'intégrité des données personnelles

Les entreprises sont ciblées par les cybercriminels en raison des nombreuses données parfois sensibles que contiennent leurs systèmes. Le vol ou la manipulation de données suppose le plus souvent, le « *piratage d'un système* », c'est-à-dire l'accès illégal à ce dernier (1).

La dénomination sociale, le logo, la marque ou l'enseigne des opérateurs économiques peuvent également être usurpés afin de tromper des clients ou prospects et obtenir de ces derniers la communication d'informations personnelles (2).

1. *Les réponses du droit pénal en cas d'atteinte aux systèmes informatiques des entreprises*

Les systèmes informatiques centralisent et agrègent de nombreuses données et constituent de ce fait une cible tentante pour qui s'intéresse à ces informations parfois insuffisamment protégées qui, on l'a vu, sont susceptibles d'être utilisées à des fins lucratives.

En France, l'accès illégal à un système informatique est une infraction pénale : la loi n° 88-19 du 5 janvier 1988 sur la fraude informatique, dite loi « *Godfrain* », permet de sanctionner toutes les intrusions non autorisées dans un système informatique. Les sanctions prévues varient en fonction du degré d'incidence de l'intrusion sur le système en cause :

- l'article 323-1 du code pénal sanctionne les intrusions dans un système de traitement automatisé de données de trois

ans d'emprisonnement et de 30 000 euros d'amende. L'alinéa 2 du même article prévoit une aggravation de peine lorsque l'accès frauduleux au système a entrainé la suppression ou la modification des données ou l'altération du fonctionnement du système. L'accès frauduleux est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données tout en sachant qu'elle est dépourvue d'autorisation ;

- l'article 323-2 du code pénal incrimine le fait de fausser ou d'entraver le fonctionnement du système informatique, passible de cinq ans d'emprisonnement et de 75 000 euros d'amende. Peu importe qu'il y ait eu accès, autorisé ou non, au système informatique de la victime ; il s'agit ici de réprimer des dégâts causés volontairement aux données et au système ;

- l'article 323-3 du code pénal vise la modification frauduleuse de données. Il sanctionne l'introduction, la suppression ou la modification frauduleuse de données de cinq ans d'emprisonnement et de 75 000 euros d'amende.

Les peines d'emprisonnement et d'amende des infractions prévues aux articles 323-1, 323-2 et 323-3 du code pénal susvisés ont été aggravées par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Cette dernière a par ailleurs inséré un nouvel article 323-3-1 dans le code pénal permettant de réprimer le trafic de moyens destinés à commettre des infractions en matière informatique, en sanctionnant l'importation, la détention, l'offre, la cession et la mise à disposition des moyens techniques, matériels ou logiciels permettant de telles attaques.

La tentative de commission des délits susvisés est punie des mêmes peines, en application de l'article 323-7 du code pénal. L'article 323-4 du même code permet en outre de réprimer les associations de malfaiteurs, dès leurs premiers efforts accomplis en vue de l'intrusion dans un système de traitement automatisé de données. Enfin, le recel d'informations obtenues suite à une intrusion frauduleuse dans un système de traitement automatisé de données est puni par l'article 321-1 du code pénal de cinq ans d'emprisonnement et de 375 000 euros d'amende.

2. *Les réponses du droit pénal en cas d'usurpation d'identité d'entreprises dans le cadre d'un hameçonnage (« phishing ») ou de pratiques analogues*

Parmi les techniques préférées des cybercriminels figure le hameçonnage, qui consiste à tromper l'internaute *via* un courriel semblant émaner d'une entreprise de confiance (banque, site de commerce ou de paiement en ligne, réseau social, etc.) et renvoyant vers un site web pour l'inviter à révéler ses identifiants personnels (un faux site à en-tête d'une banque, par exemple). Les données personnelles sont ensuite dérobées et mises sur le « *marché noir* » des données personnelles précédemment évoqué.

La Caisse d'allocations familiales (CAF) a ainsi été victime d'une campagne de hameçonnage, aux termes de laquelle un courriel frauduleux invitait son destinataire à cliquer sur un lien pour se rendre sur le site de l'organisme afin qu'il puisse percevoir des droits dont il était censé bénéficier. Le lien figurant dans le courriel redirigeait la personne visée vers un site web localisé en Hongrie imitant le site web de la CAF et encourageait l'utilisateur à s'identifier et à entrer ses coordonnées bancaires.

D'après la note d'orientation n° 4 du Comité de la Convention Cybercriminalité (T-CY), une usurpation d'identité se décompose en trois étapes :

• phase 1 : l'obtention des renseignements personnels par des moyens divers tels que le vol physique, l'utilisation de moteurs de recherche, des attaques de l'intérieur ou de l'extérieur (accès illicite aux systèmes informatiques, Trojans, « keyloggers », logiciels espions et autres programmes malveillants), par le recours au hameçonnage ou à d'autres techniques d'ingénierie sociale ;

• phase 2 : la possession et la cession des renseignements personnels (par ex., la vente de ces informations à des tiers) ;

• phase 3 : l'utilisation des renseignements personnels pour se livrer à des activités frauduleuses ou commettre d'autres infractions, par exemple en prenant l'identité d'une autre personne pour exploiter des comptes en banque ou des cartes de crédit, ouvrir de nouveaux comptes, contracter des prêts et crédits, commander des biens et services ou diffuser des programmes malveillants.

Ainsi, l'usurpation d'identité (y compris le hameçonnage et les conduites analogues) sert généralement à la préparation de nouveaux agissements criminels, tels que la fraude informatique.

En France, la loi dite *LOPPSI II* (L. n° 2011-267, 14 mars 2011, d'orientation et de programmation pour la performance de la sécurité intérieure, JO 15 mars) a introduit dans le Code pénal un délit spécifique d'usurpation d'identité s'étendant aux réseaux numériques. Le nouvel article 226-4-1 du code pénal sanctionne ainsi « *le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération* ».

Cette incrimination comble un vide juridique en permettant de répondre à des actes malveillants qui ne pouvaient, jusque-là, tomber sous le coup d'aucune qualification pénale. Le délit d'usurpation numérique ainsi défini ne vise pas seulement le nom de la victime (personne physique ou morale), mais son identité et plus largement n'importe quelle donnée « *permettant de l'identifier* ». Les informations relatives à l'identité d'une personne morale susceptibles d'être considérées comme des données « *identifiantes* » sont nombreuses : dénomination sociale, nom commercial, sigle, marque, logo, enseigne, nom de domaine, adresse IP, adresse e-mail interne, etc.

***

La cadre juridique de la protection des données à caractère personnel est en profonde mutation, avec pour objectif la définition d'« *une politique plus globale et plus cohérente à l'égard du droit fondamental à la protection des données à caractère personnel* » (Proposition de règlement, préc., p.2.), impératif qui se couple avec l'exigence de sécurité des réseaux et de l'information (Proposition de Directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union, 7 févr. 2013, COM(2013) 48 final, 2013/0027 (COD)).

De telles évolutions impliquent une adaptation permanente des acteurs économiques, adaptation indispensable pour prévenir les failles de sécurité mais pourtant peu évidente notamment pour les TPE/PME, pour lesquelles le risque de non-conformité est plus sensible.

De fait, l'entreprise constitue aujourd'hui un levier fondamental de l'effectivité de la politique de protection des données personnelles, rôle initialement imposé par les pouvoirs publics mais que l'entreprise a su s'approprier, en intégrant progressivement l'impératif de protection des données personnelles à la « *culture d'entreprise* », jusqu'à en faire une arme concurrentielle.

Il est dès lors indispensable que l'entreprise compose avec le nouveau rôle qui est le sien, ce qui implique une gestion des risques tant internes qu'externes à l'entreprise en matière de protection des données. Plus encore, il s'agit pour les opérateurs économiques de prendre part aux débats et défendre leurs intérêts dans la redéfinition du cadre juridique et politique de la protection des données à caractère personnel. ■

La « *cybersécurité* » des entreprises

La révolution numérique est entrée avec l'Internet dans l'entreprise avant qu'elle n'ait gagné en maturité informatique, car le business commande d'aller toujours plus vite en toute contradiction avec la sécurité du patrimoine matériel et informationnel.

Par Anne SOUVIRA

Commissaire Divisionnaire

→RLDA 4844

Quelle que soit sa taille, l'entreprise est confrontée à la cybersécurité. Jusque récemment l'analyse du risque cybernétique, aux effets peu quantifiables, menait à des arbitrages financiers défavorables. Aussi échappait à l'entreprise, inconsciente des dangers, l'enjeu de la préservation des Systèmes d'information (SI) et des données patrimoniales, ou sensibles qu'ils recèlent. Les responsables de la Sécurité des systèmes d'information (RSSI) ont alors formé une communauté d'échanges, constatant l'absence de budget pour unifier le parc matériel métiers ou pour construire la politique de sécurité des installations. Cette communauté, avec des directeurs de SI, s'est ouverte aux avocats, aux autorités (ANSSI : Agence nationale de sécurité des systèmes d'information dépendant du Secrétaire général de la Défense et de la Sécurité nationale, forces répressives, CNIL) afin d'apprécier le phénomène des cyber-menaces et d'y apporter une réponse technique et juridique (Refalo P.-L., L'effet papillon du hacker, Eyrolles, 2012).

Parallèlement, la conformité à la règlementation, aux lois françaises avant-gardistes informatiques, aux directives et projets européens, devient incontournable, quand la mondialisation économique ne la rend pas incompatible avec le droit d'autres pays (<http://www.feral-avocats.com/fr/nos-publications/articles_de_presse/557/586.html> e-discovery : comment concilier les exigences de la procédure américaine avec les règles protectrices des données à caractère personnel ?, avr. 2010). La cybersécurité peut se définir comme une politique de réduction de la surface des menaces cybercriminelles, inhérentes à l'usage des nouvelles technologies dans l'entreprise. Il faut accepter et faire accepter sa mise en œuvre tout en résolvant de façon très opérationnelle, techniquement, juridiquement dans un contexte financier contraint, une somme d'obligations légales.

L'intégrité, la confidentialité et la disponibilité des systèmes et des données, sont l'objet même des contrats, des Politiques de sécurité des système d'information (PSSI) et des Plans de continuité d'activité (PCA) auxquels s'intègrent les formations des personnels depuis le plus haut niveau, les règlements intérieurs et chartes informatiques, afin de construire une cybersécurité globale de l'entreprise et de la pérenniser. Car, comme le reprend Patrick Pailloux, le directeur de l'ANSSI, à l'image du comité d'hygiène et des conditions de travail (CHSCT), sans hygiène informatique, c'est l'ensemble du système de protection qui est jeté à bas (Publications des guides de sécurité de l'ANSSI, <http://www.ssi.gouv.fr/fr/ssi/>, <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html>).

> *Ces menaces internes ou externes, pas toujours techniques, sont très diversifiées et pour y faire face, l'entreprise n'a pas que des obligations légales, elle a aussi des droits.*

Faire de la cybersécurité, c'est optimiser son activité dans la sérénité, vu les menaces d'espionnage ou de sabotage qui pèsent sur elle. Prendre conscience des cyber-risques pour mieux les maîtriser, en intégrant les contraintes légales de protection de l'individu et de l'entreprise, tout en développant ses activités, c'est le challenge de la cybersécurité de l'entreprise (Le risque numérique : <http://www.senat.fr/compte-rendu-commissions/20130624/opecst.html>, <http://www.senat.fr/notice-rapport/2012/r12-721-notice.html>).

Ces menaces internes ou externes, pas toujours techniques, sont très diversifiées et pour y faire face, l'entreprise n'a pas que des obligations légales, elle a aussi des droits.

L'informatique et les réseaux sociaux se développent en se généralisant, le sujet de la cybersécurité doit être abordé par tous, sans anxiété particulière avec la conscience des risques de l'inter dépendance dans ce monde hyper-connecté. Aussi, être l'acteur de sa propre sécurité c'est donc assurer celle d'autrui.

C'est pourquoi seule une formation différenciée des acteurs, permettra à terme de réduire les risques encourus car à l'heure, du

« *cloud* « (*Cloud computing* : hébergement de données en nuage : dans des *data centers* non connus), du « *BYOD* » (*Bring your own device* : ou « AVEC », Apportez votre équipement personnel de communication, selon la Commission générale de terminologie et de néologie française) et de la réalité augmentée, le monde professionnel est dépendant du monde privé et réciproquement.

La cybersécurité embrasse un périmètre toujours plus vaste à mesure du développement des nouvelles technologies. Il est urgent d'acquérir la connaissance des bons usages de la technologie et, des connaissances juridiques pluridisciplinaires tant est grand le retard pris.

L'examen des principales menaces internes et externes et des conséquences de leur réalisation sur l'entreprise (I) puis des moyens de les prévenir ou d'y répondre (II), doit convaincre que pour sauvegarder son activité, ses emplois voire d'en créer, l'entreprise ne peut faire l'économie de sa cybersécurité.

I.– UNE ENTREPRISE MENACÉE DE L'INTÉRIEUR PRÊTANT LE FLANC AUX CONSÉQUENCES DÉSASTREUSES DES ATTAQUES EXTERNES

Évoquer une cybersécurité des entreprises c'est mesurer qu'elles sont soumises à des cybermenaces (CDSE, Colloque annuel, 6 déc. 2012, « Les entreprises et l'État face aux cybermenaces » ; Quéméner M., Cybermenaces, entreprises et internautes, Economica 2008) qu'elles doivent éviter, contribuant ainsi à la lutte contre la cybercriminalité. Celle-ci se manifeste par les infractions commises *via* ou contre ses réseaux et systèmes d'information. Accès frauduleux à ses réseaux et systèmes de données pour les détruire ou dérober des secrets de fabrique, utilisation frauduleuse de ses communications téléphoniques ou de son processus de paiement par ingénierie sociale (l'ingénierie sociale, ou *social engineering* en anglais, est une forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clefs. Cette pratique exploite les failles humaines et sociales de la structure cible, à laquelle est lié le système informatique visé (in wikipedia)) donnant lieu à de vrais « *faux ordres de virement* », escroqueries au faux président… entrainent de lourdes pertes financières, des licenciements montrant combien la menace externe peut être liée aux comportements internes.

Les motivations des pirates sont toujours classiques, l'espionnage à des fins économiques ou industrielles et la malveillance par des exploits (un exploit est, dans le domaine de la sécurité informatique, un élément de programme permettant à un individu ou un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système d'exploitation ou dans un logiciel que ce soit à distance, remote exploit, ou sur la machine sur laquelle cet exploit est exécuté, local exploit ; ceci, afin de prendre le contrôle d'un ordinateur ou d'un réseau (*in* Wikipédia)).

Que l'attaque cybernétique provienne de l'intérieur ou de l'extérieur, elle aura un coût pouvant aller jusqu'à la disparition de l'entreprise. Ce phénomène doit donc être pris au sérieux, compte tenu de l'accroissement des obligations légales de l'entreprise, responsable du traitement des systèmes et des données et de la sécurisation de son réseau.

A.– Les menaces internes issues de comportements inappropriés facilitent les atteintes de l'extérieur

Les menaces internes du fait des personnes dans les procédures déclenchées tant au pénal qu'au civil, sont d'abord les inquiétantes menaces involontaires (*praeter*-intentionnelles peut-être aujourd'hui), la vulnérabilité a-t-on coutume de dire se situant « *entre la chaise et le clavier* ». Elles relèvent plus de comportements inadaptés à l'usage des nouvelles technologies que de la malveillance, à but lucratif ou non, qui caractérise les menaces intentionnelles.

> *Il ne sert d'ériger de belles défenses en château fort, au coût élevé de solutions techniques, si l'édifice peut s'écrouler par celui qui, de sa chaise, aura abaissé le pont-levis de son clavier.*

Le danger de l'acte de malveillance est réel, dans un contexte conflictuel souvent prud'homal. Il va conduire, souvent facilité par un emploi au sein du SI, au sabotage des installations causant un grave préjudice tels la disparition de données, fichiers ou serveurs, peu en rapport avec la rancœur, le sentiment de défaut de reconnaissance ou autres motivations pauvrement humaines. La violation des correspondances de messageries ou la fuite de données informationnelles, financières ou personnelles, de secret de fabrique, par contrefaçons de fichiers, de base de données, de logiciel ou par abus de confiance par détournement de la chose immatérielle remise, relèvent quant à elles plus de l'espionnage.

On peut citer l'involontaire infection de tout le réseau d'une société à travers la France, par l'usage d'une clef USB personnelle infectée ou le courriel contenant un lien dans son texte ou dans la pièce jointe qui déclenche l'infection du poste puis se répand sournoisement. Les conséquences non recherchées sont aussi néfastes que la malveillance ou l'attaque externe. Elle doit donc être crainte et traitée tant pour les TPME que pour les grandes entreprises.

Les menaces internes du fait d'une insuffisance de gouvernance de sécurité et de moyens techniques dans un environnement budgétaire contraint.

En écho de comportements insensés parfois, le RSSI se doit d'être à la fois un facilitateur et un gendarme. Il se plaint du manque de rigueur dans l'exigence du respect et de contrôle des règles édictées ; Le déficit en règles claires et strictes des usages, en sensibilisation de sécurité basique, en formation alors que des budgets ne sont pas consommés, constitue une réelle menace. Il ne sert d'ériger de belles défenses en château fort, au coût élevé de solutions techniques, si l'édifice peut s'écrouler par celui qui, de sa chaise, aura abaissé le pont-levis de son clavier. Des expériences existent selon les entreprises (les services institutionnels interviennent en entreprise) avec les énergies des services de communication pour faire prendre conscience au personnel de son implication dans la sauvegarde de l'entreprise par un comportement rigoureux, mais l'exemple ne vient pas « *d'en haut* ».

La contrainte budgétaire mène à un investissement en sécurisation des systèmes insuffisant, à des solutions techniques de moindre qualité, à un parc informatique vulnérable faute de coûteuses mais indispensables mises à jours des correctifs de vulnérabilité des systèmes, à une infogérance-dépendance informatique non maîtrisée par le maître et responsable du SI. Un contrat de prestations à bas coût peut causer la perte irréversible de données. L'absence d'une gestion rigoureuse des accès aux systèmes ou aux données en fonction du besoin d'en connaître, d'une politique écrite de sécurité des systèmes

d'information (PSSI) et d'un plan de continuité d'activité ou de reprise, de sauvegarde ou de récupération des données, voilà l'essentiel des menaces internes de gouvernance qui facilitent la réalisation des menaces externes. De même, l'entreprise a l'obligation de sécuriser son accès internet pour protéger la propriété littéraire et artistique sur internet sauf à être passible de la contravention de négligence caractérisée (D. n° 2010-695, 25 juin 2010, instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique sur internet) ou de complicité de téléchargement d'image pédopornographique, etc., nonobstant sa responsabilité de l'article 1384 du code civil.

L'admission et la gestion du BYOD, téléphones et ordinateurs portables personnels au sein de l'entreprise est une porte ouverte sur le cœur de l'entreprise qui parfois même, participe à l'achat du matériel de l'abonnement privé utilisé à des fins personnelles ce qui rend complexe le recueil de la preuve en cas d'attaque.

L'accès Wi-Fi proposé aux visiteurs, non considéré comme « *public* », n'est pas soumis à la législation de conservation des traces et souvent ces traces de connexion se seraient révélées bien utiles si l'entreprise savait qu'elle en a la possibilité. L'obligation faite aux uns n'empêche pas les autres de s'y conformer dans le respect de la légalité (L. n° 2004-575, 21 juin 2004, dite LCEN, mod. par D. n° 2011-219, 25 févr. 2011, art 6. relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne).

La menace interne peut également porter sur des manquements techniques par l'entreprise comme la question du *cloud computing*, ou de l'hébergement des données à distance en France, en ou hors UE. Elle constitue une menace si le défi juridique sur le tri de données sensibles ou susceptibles de transfert n'a pas été relevé et traité avec l'aide ou non d'un correspondant informatique et libertés (CIL) ; la réversibilité des données est-elle certaine en cas d'hébergement dans un data center submersible ? Quelles sanctions pour avoir transféré indument des données ? Par la CNIL et par le tribunal correctionnel ?

L'occurrence de la menace interne peut avoir pour conséquences des atteintes aux systèmes de traitement automatisés de données (STAD) des collectes frauduleuses, déloyales ou illicites de données à caractère personnel et la divulgation de données patrimoniales de l'entreprise, à caractère personnel ou financier. Les atteintes aux STAD empêchant ou perturbant les communications voire modifiant ou supprimant des données essentielles au fonctionnement ou à l'activité de l'entreprise, sont d'une particulière gravité pour sa survie. C'est pourquoi la loi Godfrain (L. n° 88-19, 5 janv. 1988, sur la fraude informatique) punit sévèrement les atteintes aux STAD tout comme la loi CNIL (L. n° 78-17, 6 janv. 1978, relative à l'informatique, aux fichiers et aux libertés) les violations des données à caractère personnel afin de protéger efficacement les individus.

B.– Les menaces externes : de l'espionnage essentiellement destiné à appauvrir l'entreprise pour accroître des patrimoines peu scrupuleux

Le patrimoine matériel ou informationnel de l'entreprise est l'objet des convoitises d'États, de concurrents ou de délinquants peu scrupuleux animés par l'appât du gain, ces menaces externes invisibles pèsent gravement sur l'entreprise. Aussi sont-elles portées de plus en plus à la connaissance des autorités lorsqu'elles surviennent, mais avec modération vu des facteurs prioritaires comme sa e-reputation, le contexte social et économique du moment où sa capacité à communiquer et réagir à cette crise. La réalisation de ces menaces, aux motivations diverses, aura les mêmes conséquences sur l'économie de l'entreprise qu'une attaque interne.

L'obtention frauduleuse d'un avantage concurrentiel par de l'intelligence économique déloyale a été l'objet de l'attention des médias.

« *L'hacktivisme* » sévit en fonction du secteur d'activité de l'entreprise, de sa présumée réputation à être facile à pirater (le domaine des media par exemple) ou de l'intérêt des internautes pour le site, de la relation institutionnelle de l'entreprise avec l'État... On peut citer la défiguration de site, le remplacement de la page d'accueil par une revendication, le déni de service par saturation des serveurs pour les rendre indisponible tel Paypal qui avait coopéré avec les États-Unis dans le dossier *Wikileaks*, les attaques contre Charlie Hebdo pour la parution des caricatures et combien d'autres attaques émises de l'étranger sans aucune chance de les attribuer faute de coopération et d'entraide internationales efficaces.

La concurrence déloyale pour faire des économies de R&D est très répandue en France. Elle s'exerce par le pillage du patrimoine immatériel des propriétés intellectuelle et industrielle, par les atteintes aux droits d'auteurs et droits voisins et au producteur de logiciels et de BDD, notamment par contrefaçon de bases de données ou de logiciels (ou par vol de données), par les contrefaçons des sites, marques, logos, dessins, modèles, brevets nuisant à l'économie nationale.

L'obtention frauduleuse d'un avantage concurrentiel par de l'intelligence économique déloyale a été l'objet de l'attention des médias. Ainsi l'espionnage économique permet de se procurer des informations secrètes par les attaques sournoises persistantes (APT) (advance persistant threat APT), sur des conditions commerciales, sur un secret de fabrique ou une marque, sur les informations en violation du secret des correspondances des messageries. L'espionnage par exfiltration sournoise de données pendant des années, explique des offres ou des contrats manqués qui sont allés à la concurrence étrangère. L'État français en a été victime lors de négociations internationales (cf. l'affaire de Bercy et de son attaque ciblée à l'occasion du G20 en 2011 <http://www.lefigaro.fr/conjoncture/2011/03/07/04016-20110307ARTFIG00333-bercy-cible-d-une-vaste-affaire-de-piratage.php>, <http://www.liberation.fr/economie/2011/03/07/le-ministere-de-l-economie-et-des-finances-victime-d-une-attaque-informatique_719808>). Il faut citer les procédés déloyaux « *commerciaux* » de la cybercriminalité tels, la collecte déloyale d'un annuaire type carnet d'adresses mail, numéros de téléphone, l'extraction d'une partie substantielle d'une base de données (BDD), le référencement frauduleux, le typosquatting d'un nom de domaine proche.

L'atteinte à la réputation par le dénigrement sur internet, tel le site des « *patrons–voyous* », par la divulgation de vulnérabilités, l'entrave temporaire des systèmes informatiques par le déni de service, la défiguration de pages cachant l'attaque plus profonde, l'introduction de codes malveillants exécutant des programmes destructeurs de données, sont redoutées comme l'atteinte aux systèmes SCADA (supervisory control and data acquisition (logiciels de

pilotage des systèmes industriels)) par une mafia ou un État, par la prise de contrôle des logiciels et réseaux informatiques pilotant les processus des usines avec la manipulation de leurs données ; On pense principalement aux risques dans les transports, l'énergie et l'eau...

Aussi en échange de sa protection par des incriminations aux *quantum* élevés, pour dissuader des passages à l'acte, l'entreprise a des obligations légales aux implications techniques, juridiques et financières conséquentes et des moyens budgétaires très variables. Pourtant il lui faut mettre en place, des outils techniques et juridiques de prévention et de répression dans l'éventualité du besoin du recueil et d'administration de la preuve.

II.– LA MISE EN ŒUVRE DES MOYENS TECHNIQUES, JURIDIQUES ET DE MANAGEMENT DE LA CYBER-SÉCURITÉ EST LIÉE AU CADRE JURIDIQUE LÉGAL ET JURISPRUDENTIEL QUI PERMET LA RÉACTION ADAPTÉE

A.– C'est la mise en œuvre concomitante de solutions techniques, juridiques et de gouvernance envers les biens et les personnes qui permettra de limiter au mieux les dangers et d'y réagir

Il faut tout d'abord construire, financer et appliquer un plan de sécurité préventif et réactif dans le cadre de la politique de sécurité des systèmes d'information (PSSI) et de la continuité de l'activité ou sa reprise. Effectuer et stocker des sauvegardes de données de traces, organiser la résilience des systèmes, avoir des analystes de traces journalisées, pour recueillir les éléments d'audit ou d'enquête, indispensables pour remonter à l'origine ou reconstituer le mode opératoire et évaluer le préjudice.

Cela répond à l'obligation de sécurisation des réseaux et systèmes afin de protéger les données contenues ou transitant (L. n° 78-17, 6 janv. 1978, art. 34 et 34 *bis*, mod. et codifiée à C. pén., art. 226-17 et 226-17-1) et suppose une étude juridique et opérationnelle des risques de l'hébergement des données en nuage, obligations de déclarations, transferts de données à caractère personnel hors UE, récupération physique des données. Le responsable du traitement automatisé des données est celui qui en décide, lui donnant la finalité proportionnée au but poursuivi et sa durée. Il ne peut déléguer. Les *quantum* de peines, jusque cinq et sept ans d'emprisonnement, et les peines d'amendes doivent faire prendre conscience des enjeux relatifs aux données personnelles et sensibles. Le recours à un « *cloud souverain* » pour limiter le risque d'une perte définitive de données et permettre la reprise rapide de l'activité prend alors tout son sens notamment pour éviter que les TPME moins argentées ne sacrifient à la fausse économie des hébergeurs « *low cost* » mais surtout « *low delivery* », prestations sans mises à jour ni retour des données...

Si la menace involontaire peut être réduite, le risque zéro n'existe pas, le directeur ouvrira toujours la pièce jointe urgente sur laquelle « *on* » sollicite son avis, sur son téléphone portable, qu'il rechargera ensuite inconsidérément sur son ordinateur...de même que la comptable adjointe, promue par téléphone, unique personne de confiance par son PDG qui la somme d'effectuer, malgré les procédures qu'il a lui-même édictées, effectuera un virement bancaire.

L'analyse de risque ne semblant pas pertinente pour quantifier les conséquences financières de l'attaque, certains prônent même une assurance contre les cyber-risques, méconnaissant qu'on ne s'assure pas contre les infractions pénales que l'on peut commettre à titre de personne morale également.

Aussi la combinaison d'outils complémentaires doit être mise en œuvre, comme un contrat de travail prenant en compte le risque informatique, l'avenant au règlement intérieur dans le silence de la loi, l'établissement d'une charte informatique signée et opposable à tous, la consultation des partenaires sociaux, associés à la sensibilisation, la formation et à un management pédagogique conscient de ce risque à évaluer en permanence.

Les droits de l'entreprise pour assurer sa cybersécurité en interne c'est sa capacité légale de cyber-surveillance pour se prémunir ou réagir en urgence à la fraude interne, grave et révélée par des circonstances exceptionnelles selon la Cour de cassation.

Du contrat de travail résulte l'obligation de son exécution avec loyauté, le matériel et l'immatériel mis à disposition de l'employé sont réputés professionnels, le chef d'entreprise a alors tout droit de regard dans la sphère professionnelle sous réserve du droit au respect d'une sphère d'intimité de la vie privée au sein de l'entreprise (Cass. soc., 2 oct. 2001, n° 99-42.942, Bull. civ. V, n° 291, arrêt *Nikon*).

> ↳ *Le chef d'entreprise a alors tout droit de regard dans la sphère professionnelle sous réserve du droit au respect d'une sphère d'intimité de la vie privée au sein de l'entreprise.*

Dans cet arrêt de référence, la Cour de cassation rappelle le principe : « *Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée. Celle-ci implique en particulier le secret des correspondances* ». Et l'applique au courrier électronique : « *L'employeur ne peut prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ».

Le droit prétorien cherche à concilier, la sphère professionnelle avec le respect de la vie privée et le secret des correspondances. Ainsi les exigences de l'exécution loyale du contrat de travail limitent la liberté d'expression du salarié, devoir de discrétion et confidentialité, absence de dénigrement, d'injures, de diffamation (arrêts relatifs au réseau social *Facebook* : Cons. prud'h. Boulogne-Billancourt, 19 nov. 2010, n^{os} 10/00853 et 09/00316 ; CA Paris, 9 mars 2011, n° RG : 09/21478 ; CA Besançon, 15 nov. 2011, n° RG : 10/02642 ; CA Rouen, 15 nov. 2011, n° RG : 11/01827 ; CA Reims, 24 oct. 2012, n° RG : 11/01249 ; CA Reims, 9 juin 2010, n° RG : 09/03205 ; Cons. prud'h. Guingamp, 20 oct. 2011, n° 10/00097 ; T. corr. Paris, 17^{e} ch. corr., 17 janv. 2012, n° 10/34008 ; CA Douai, 16 déc. 2011, n° RG : 10/02317). L'employeur a un devoir de transparence, d'information de l'employé sur les moyens de contrôles de l'activité et de surveillance (Cass. soc., 10 janv. 2012, n° 10-23.482, Bull. civ. V, n° 2 ; Charte informatique, CE, CHSCT), et un devoir de loyauté des modalités d'accès aux données informatiques (poursuite de l'employeur qui instrumentalise son subordonné « administrateur » pour accéder au système d'infor-

mation, ...). La présomption de professionnalité des outils de l'entreprise est étendue aux objets personnels connectés sur le réseau ou matériel de l'entreprise (Cass. soc., 12 févr. 2013, n° 11-28.649, P+B) sans résoudre le cas du BYOD.

L'accès par l'employeur est possible si les documents et mails sont professionnels et le salarié n'a pas à être averti, ni présent, ni dument appelé.

Mais il faut discriminer les documents privés et professionnels et distinguer la copie conservatoire de l'ouverture des documents. Le recueil des documents par copie de support est possible hors la présence du salarié si les documents identifiés comme privés ne sont pas ouverts. L'intitulé doit être apparent et clair pour identifier la sphère personnelle sans ambigüité (apparence du fichier Jpeg..., nom d'un dossier photo bébé, l'objet d'un mail ; Cass. soc., 30 mai 2007, n° 05-43.102, D), l'intitulé vague « *essais divers, essais divers B, essais divers restaurés* » a été jugé insuffisant (Cass. soc., 15 déc. 2009, n° 07-44.264, Bull. civ. V, n° 284). Le fichier « *Mes documents* » généré automatiquement par le système, n'est pas privé, l'intitulé doit être explicite (initiales insuffisantes... ; Cass. soc., 10 mai 2012, n° 11-13.884, Bull. civ. V, n° 135).

La présence du salarié est requise pour l'ouverture des fichiers ou mails identifiés sans ambigüité comme personnels ; il peut être dûment appelé, sauf risque ou événement particulier (Cass. soc., 17 mai 2005, n° 03-40.017, Bull. civ. V, n° 165). Le même régime s'applique aux courriels (Cass. soc., 17 juin 2009, n° 08-40.274, Bull. civ. V, n° 153). Mais l'impossibilité d'ouvrir même les mails professionnels si le règlement intérieur (RI) le stipule (Cass. soc., 26 juin 2012, n° 11-15.310, Bull. civ. V, n° 196) doit faire prêter attention à sa mise à jour au regard de la jurisprudence parfois plus clémente. Le mail, même identifié comme « *PERSONNEL* » et au contenu privé mais qui cause un trouble objectif dans l'entreprise ne peut bénéficier du secret des correspondances et peut être cause de licenciement : le contenu privé n'est pas un blanc-seing (Cass. soc., 6 juin 2007, n° 05-43.996, D). Un arrêt similaire relève que la mention « *données personnelles* » était insuffisante, au regard de la charte qui préconisait « *PRIVÉ* » (Cass. soc., 4 juill. 2012, n° 11-12.502, D, sur l'intitulé insuffisant pour être personnel).

B.– La réaction de l'entreprise à l'attaque nécessite le recueil de la preuve lequel va dépendre de la voie choisie en fonction du but recherché

L'entreprise attaquée va devoir d'abord sauvegarder son réseau, ses données et contenir ou détourner l'attaque.

Mais le recueil de la preuve va dépendre de son état de cybersécurité, de l'exercice de la fonction de RSSI, des outils de journalisation, des sauvegardes et des ressources humaines pour les exploiter. Il s'agit de ne pas piétiner la scène de crime en recherchant dans les traces ni d'agir offensivement à son tour (CDSE, Sécurité et stratégie n° 8, févr. 2012, <https://www.cdse.fr/securite-strategie-no8,1395.html>). C'est interdit en droit français car seul l'État dispose du droit régalien de violence légitime, la justice étant publique et plus privée. Tant le livre blanc de 2013 que le projet de loi de programmation militaire donnant une capacité offensive au ministère de la Défense le rappellent (http://www.defense.gouv.fr/sante/actualites/projet-de-loi-de-programmation-militaire, <http://www.defense.gouv.fr/actualites/dossiers/sept-2011-cyberdefense-enjeu-du-21e-siecle/france/voir-les-articles/le-calid-l-expert-technique-en-securite-informatique-du-ministere>).

Le recueil des traces s'effectue par les techniciens du SI ou par un huissier requis, ou lors des constatations du service d'enquête saisi d'une plainte selon sa compétence territoriale (CA Paris, 3e ch. inst., 9 mai 2008, n° RG :2008/00897). Dans son plan de réaction à l'attaque, le contact avec les forces de Police ou de Gendarmerie, aura été identifié de façon à être conseillé au plus vite car la preuve informatique dépérit rapidement.

La voie de la procédure civile avec le recours à l'huissier de justice doit être particulièrement bien pesée en raison du dépérissement des preuves (TGI Paris, ch. req. , 30 janv. 2013, Bouygues Telecom c/ Publicis Webformance), de la qualité nécessaire au recueil de la preuve qui peut être rapidement mise en doute. Mais l'on constate souvent la lenteur d'exécution des ordonnances successives du président du tribunal de grande instance pour finalement un traitement du dossier au pénal. Il a l'avantage d'une rapidité incomparable et facilite la preuve qui est libre, comme on le constate dans nombre de dossiers prud'homaux à l'origine.

Les autorités administratives indépendantes ou les enquêteurs à la recherche de la preuve se rendent chez le tiers qu'est l'entreprise pour des constatations ou perquisitions. Une cybersécurité développée permettra de remettre les éléments rapidement ou de les localiser chez un hébergeur ou un prestataire technique.

***

Aujourd'hui l'*homo oeconomicus* se doit d'être également un *homo juridicus*, pour assurer sa cybersécurité et celle d'autrui. Pour devenir un consommateur avisé, il doit apprendre à mesurer les dangers qui menacent la collectivité et à appliquer les bons comportements, tant dans la sphère privée que professionnelle. C'est tout à l'honneur de l'entreprise que de l'y aider en établissant sa cybersécurité (cybersécurité : état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense (ANSSI)), il y va de sa pérennité (CDSE, Sécurité et stratégie n° 11, déc. 2012, <https://www.cdse.fr/securite-strategie-no11.html>; La cybersécurité en entreprise : se protéger juridiquement et se former, Quéméner M. et Souvira A.), les objectifs des cybercriminels étant de nature à attaquer les fondements de l'entreprise voire de la faire disparaître.

Mais il faut d'abord prendre conscience du risque numérique, c'est un devoir de l'entreprise vis à vis de ses employés et de ses actionnaires, pour la cybersécurité des échanges à travers le monde (Arpagian N., La cybersécurité, Que sais-je, PUF, 2010). ■

La coopération entre les organes de lutte contre la cybercriminalité. Pour une stratégie globale de « *cybersécurité* » française

Par Myriam QUÉMÉNER

Magistrat

→RLDA 4845

Attaques informatiques quotidiennes, espionnages de sociétés et vols de données sensibles, saturation de sites Internet d'entreprises et de ministères, les cybermenaces contre les systèmes d'information sont aujourd'hui au coeur des préoccupations étatiques. Appropriation de données personnelles, économiques et commerciales d'entreprises victimes de leurs concurrents ou de puissances étrangères, arrêts de services nécessaires au bon fonctionnement de l'économie ou de la vie quotidienne, compromission d'informations de souveraineté, telles sont les conséquences potentielles ou réelles des liens étroits entre le numérique et les activités humaines.

De nombreuses affaires ont donné un fort retentissement à ces dérives de l'Internet comme celle de Bercy, celle du géant Sony où plus de 77 millions de comptes clients ont été piratés sur les sites de jeux et de vidéos en ligne ou celles de plusieurs grandes entreprises françaises ont pour leur part subi des escroqueries *via* des e-mails faussement signés par la direction des groupes industriels.

L'espace numérique représente aujourd'hui un enjeu fondamental pour la sécurité des États, des structures économiques quelle que soit leur taille, des petites et moyennes entreprises (PME) aux multinationales (Gruselle B., Enquête sur la sécurité numérique des entreprises, Fondation pour la recherche stratégique, févr. 2013, <http://www.frstrategie.org/barreFRS/publications/rd/2013/RD_201301.pdf>) et aux établissements financiers. La sécurité dans le cyberespace revêt des aspects à la fois économiques, stratégiques, judiciaires et idéologiques (Huyghe F.-B., Des armes à la stratégie, Revue internationale et stratégique, 2012/3 n° 87, p. 53-64. DOI : 10.3917/ris.087.0053).

Ainsi sont apparus les termes de cyberdéfense (Rapport Bockel, La cyberdéfense, un enjeu mondial, une priorité nationale, <http://www.senat.fr/rap/r11-681/r11-681.html>), de cybersécurité et de cybercriminalité (Rapport Bockel, précité). S'il existe une certaine porosité entre ces concepts, seuls les deux premiers visent directement la sécurité nationale mais pour traiter les affaires de cybercriminalité, il est indispensable de connaître le contexte global des attaques dans le cyberespace ainsi que les cibles visées.

La cybercriminalité, notion polymorphe, désigne l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment sur le réseau Internet comme les atteintes aux systèmes automatisés de données, celles où les réseaux sont utilisés comme moyens pour commettre des crimes ou délits classiques – escroqueries, fraudes, blanchiment d'argent ou contrefaçons – et enfin celles où les délinquants utilisent les technologies numériques comme support d'infractions de contenus illicites tels la pédopornographie ou le racisme (La cybercriminalité, une menace de quelle ampleur ?, p. 69 et s., *in* Cahiers Français n° 360, janv.-févr. 2011, La Documentation française).

Le centre d'analyse stratégique, dans une note récente (Centre d'analyse stratégique, Cybersécurité, l'urgence d'agir, Note d'analyse 324, mars 2013, < http://www.strategie.gouv.fr/content/cybersecurite-urgence-na324>) précise que la cybercriminalité désigne l'ensemble des infractions pénales commises via les réseaux informatiques comme les vols de données à caractère personnel ou industriel, les fraudes (Dalloz AJ pénal, dans son numéro 5/2012, a consacré un dossier à la cybercriminalité intitulé « Cybercriminalité : l'adaptation de la réponse pénale », AJ Pénal 2012, p. 252). Dans une optique de protection étatique, elle correspond et est définie comme les actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible (<http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf>).

Avec le développement des cyberattaques, il a été nécessaire d'augmenter le niveau de sécurité des systèmes d'information de l'État par la mise en place d'une politique interministérielle de sécurité.

On évoque aujourd'hui aussi le terme plus vaste de cybersécurité (Défense et sécurité des systèmes d'information – Stratégie de la France, site <http://www.ssi.gouv.fr/site_article318.html>) qui est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. La cybersécurité (Arpagian, La cybersécurité, éd. Puf Paris, Collection Que sais-je, p. 10 et s.) correspond à des techniques de protection des systèmes d'information connues depuis une vingtaine d'années sous le terme de sécurité des systèmes d'information (SSI). Elle s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une cyberdéfense qui est l'ensemble des mesures techniques ou non permettant à un État de défendre dans le cyberespace les systèmes d'information qu'il juge essentiels (Défense et sécurité des systèmes d'information, précité). La puissance publique a ainsi dû revoir ses stratégies et sa législation pour tenter de juguler ces phénomènes (Centre d'analyse stratégique, Internet : prospective 2030, Note d'analyse 02, juin 2013, <www.strategie.gouv.fr/content/internet-prospective-2030-NA-02-juin-2013>).

Il convient tout d'abord de présenter les structures de lutte contre la cybercriminalité et leurs compétences puis d'aborder leur coordination afin de mettre en place une véritable politique de cybersécurité.

La France s'est dotée d'une stratégie pour se défendre et se protéger dans le cyberespace afin de répondre aux cybermenaces. La protection des infrastructures vitales, la lutte contre les attaques informatiques et contre le cyberterrorisme, la coopération internationale en matière de cybersécurité, la coopération entre les secteurs public et privé, sont des enjeux fondamentaux.

Avec le développement des cyberattaques, il a été nécessaire d'augmenter le niveau de sécurité des systèmes d'information de l'État par la mise en place d'une politique interministérielle de sécurité. Chaque administration se conforme à un ensemble de règles devant être respectées par les utilisateurs et les informaticiens mais l'hétérogénéité des pratiques en la matière nuit encore gravement à leur compréhension et à leur application.

I.– L'ARSENAL ORGANISATIONNEL FACE AUX CYBERMENACES

À la suite de la publication du Livre blanc sur la défense et la sécurité nationale (<http://archives.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/livre_blanc_1337/livre_blanc_1340/index.html>), identifiant les attaques informatiques de grande envergure contre les infrastructures nationales comme une des menaces majeures pour la France, le Gouvernement a renforcé de façon significative les capacités nationales en matière de cyberdéfense. Il définit la protection des systèmes d'information comme une composante à part entière de notre politique de défense et de sécurité. Il accorde, pour la première fois, une place importante à la menace représentée par les attaques informatiques.

Face à la criminalité numérique les services étatiques se sont mis progressivement en ordre de bataille avec la création de l'ANSSI et de services spécialisés au niveau de la Police, de la Gendarmerie et des Douanes.

1. L'Agence nationale de sécurité des systèmes d'information (ANSSI)

Pour faire face au défi croissant que représentent les cyberattaques, et suite aux recommandations du Livre blanc sur la défense et la sécurité nationale, l'Agence nationale de sécurité des systèmes d'information (ANSSI, anciennement Direction centrale de la sécurité des systèmes d'information [DCSSI], créée en 2001) a été créée en juillet 2009. Il s'agit d'une agence interministérielle, située au sein des services du Premier ministre. L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information (D. n° 2009-834, 7 juill. 2009, du Premier ministre, portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information »). À ce titre, elle est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées.

Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. Elle a notamment pour mission de détecter et réagir au plus tôt en cas d'attaque informatique, grâce à un centre de détection chargé de la surveillance permanente des réseaux sensibles et de la mise en œuvre de mécanismes de défense adaptés aux attaques ; prévenir la menace, en contribuant au développement d'une offre de produits de très haute sécurité ainsi que de produits et services de confiance pour les administrations et les acteurs économiques ; jouer un rôle de conseil et de soutien aux administrations et aux opérateurs d'importance vitale; informer régulièrement le public sur les menaces, notamment par le biais du site Internet gouvernemental de la sécurité informatique, lancé en 2008, qui a vocation à être le portail Internet de référence en matière de sécurité des systèmes d'informations.

L'ANSSI constitue un réservoir de compétences destiné à apporter son expertise et son assistance technique aux administrations et aux opérateurs d'importance vitale. Elle est chargée de la promotion des technologies, des systèmes et des savoir-faire nationaux. Elle contribue au développement de la confiance dans l'économie numérique. Elle assure la tutelle du centre de transmission gouvernemental chargé de mettre en œuvre les moyens de commandement et de liaison nécessaires au Président de la République et au Gouvernement. Son objectif est de sensibiliser aux risques informatiques actuellement encourus par les systèmes sensibles.

L'ANSSI est ainsi chargée d'élaborer le **référentiel général de sécurité** (RGS), qui désigne l'ensemble des règles relatives aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, qui participent à la sécurité des informations et qui doivent respecter certaines fonctions, comme la signature électronique, l'authentification ou la confidentialité.

Elle exerce ainsi un rôle d'assistance à la maîtrise d'ouvrage des ministères et du secteur privé dès lors que la sécurisation de leurs systèmes d'information concerne les intérêts fondamentaux de la Nation. L'ANSSI apporte ainsi son soutien dans de nombreux projets d'importance (comme par exemple le passeport biométrique ou le dossier médical personnel) et elle oeuvre à l'intégration de la sécurité des systèmes d'information dans plusieurs programmes de défense. L'agence est également chargée de définir les recommandations générales, les référentiels techniques et les méthodes dans tous les aspects concourant à la sécurité des systèmes d'information.

Dans le cadre du renforcement des capacités en la matière au ministère de la Défense, un poste d'officier général chargé de la cyberdéfense **a été créé en 2011.** Il coordonne l'action du ministère dans ce domaine et sert d'interface principale en cas de crise cyber.

> *Dans le cadre du renforcement des capacités en la matière au ministère de la Défense,un poste d'officier général chargé de la cyberdéfense a été créé en 2011.Il coordonne l'action du ministère dans ce domaine et sert d'interface principale en cas de crise cyber.*

2. La direction centrale du renseignement intérieur (DCRI)

La DCRI est chargée de prévenir et réprimer, sur le territoire de la République, les activités inspirées, engagées ou soutenues par des puissances ou des organisations étrangères et de nature à menacer la sécurité du pays. Elles consistent dans la lutte contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la nation. La contre-ingérence étrangère, traditionnellement associée au contre-espionnage, couvre un domaine élargi dans un contexte multipolaire. L'objectif de la DCRI est de déceler et de neutraliser toute menace résultant des activités de services de renseignement de pays adverses, d'organisations ou d'agents se livrant à l'espionnage, au sabotage ou à la subversion. La menace terroriste, très évolutive, exige des services de sécurité une adaptation permanente.

La DCRI, qui combine ses capacités de service de renseignement et de service de police judiciaire spécialisé, est en mesure de détecter, de surveiller et le cas échéant d'interpeller les individus, les groupes et les organisations de nature subversive susceptibles de se livrer à des actes de terrorisme ou d'atteinte à l'autorité de l'État. Au titre des menaces émergentes, la lutte contre les proliférations des armes nucléaires, bactériologiques, chimiques ou balistiques s'inscrit dans une dynamique de coopération avec le secteur économique et industriel. De surcroît, le développement d'une société dépendante des technologies de l'information et des communications justifie l'investissement consacré à la lutte contre la cybercriminalité.

Enfin, la DCRI est inscrite dans une véritable politique publique d'intelligence économique initiée depuis 2003, et peut ainsi faire face à de nouveaux enjeux dans un esprit de partenariat avec les entreprises publiques et privées.

3. L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC)

Créé en 2000, cet office à vocation interministérielle a une compétence nationale en matière d'enquêtes de police judiciaire spécialisées à caractère sensible à portée nationale ou internationale et a en charge notamment la lutte contre les réseaux nationaux contrefaisant les cartes bancaires ou les réseaux internationaux de piratage des distributeurs automatiques de carburant et de billets.

Il est chargé de lutter contre toutes les formes de délinquance apparues avec l'avènement des nouvelles technologies de l'information et de la communication (informatique, téléphonie et cartes bancaires), que celles-ci soient liées ou facilités par ces dernières. Captation de données, usurpation d'identité, piratage, distributeurs de billets piégés, escroqueries sur mobiles et autres actes de cyberdélinquance sont de la compétence de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). L'office traque les affaires complexes sur tout le territoire et anticipe les menaces, grâce à des matériels informatiques d'investigation de très haut niveau, l'objectif étant d'être au plus près du mode de fonctionnement des escrocs et de décrypter leurs modes opératoires de plus en plus élaborées.

Il traite les affaires informatiques les plus importantes dont est saisie la Direction centrale de la police judiciaire. L'OCLCTIC intervient sur des affaires d'envergure nationale et internationale dans le cadre d'enquêtes liées aux technologies de l'information et de la communication (par exemple : intrusion, entrave ou altération de systèmes informatiques, de contrefaçon de cartes de paiement, atteintes aux personnes et aux biens).

Outre sa vocation opérationnelle, l'office intègre d'autres missions relatives à la coordination, l'assistance technique, la centralisation et la diffusion de l'information dans le domaine de la cybercriminalité. L'OCLCTIC assure également la gestion des échanges internationaux (Interpol, Europol et G8H24 – réseau regroupant les pays signataires de la Convention de Budapest sur la cybercriminalité, 23 nov. 2001) en tant que point de contact unique national. La plate-forme d'assistance technique, spécialement équipée de matériels et de logiciels d'investigations de haut niveau technologique assure l'assistance aux services d'enquêtes, la formation des enquêteurs spécialisés en criminalité informatique, la veille technologique, les interceptions judiciaires Internet et la gestion des signalements des sites illicites. L'OCLCTIC gère enfin une plateforme (<https://www.internet-signalement.gouv.fr>) police-gendarmerie destinée à recueillir tous les signalements de contenus illicites sur Internet et qui fonctionne actuellement sur la base de relations engagées avec les professionnels de l'Internet accessible au grand public.

4. La Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI)

Ce service opérationnel d'une trentaine de policiers qui dépend de la Préfecture de police de Paris est spécialisé dans les enquêtes en milieu informatique. Elle assiste tous les services enquêteurs qui la sollicitent dès lors qu'ils sont confrontés au numérique et assure une mission de formation et de sensibilisation à la sécurité auprès des autres services de Police, des entreprises et diverses

institutions. La BEFTI est compétente sur Paris et les trois départements limitrophes (92, 93 et 94). Toutefois avec l'accord des autorités judiciaires, cette compétence peut être étendue à l'ensemble du territoire national.

La Brigade (cf. l'interview d'Anne Souvira, chef de la BEFTI, Expertises 2011, n° 364, p. 409 et s.) intervient principalement dans les affaires relatives à la propriété intellectuelle portant atteinte aux systèmes de communication tels le piratage informatique, les intrusions dans les ordinateurs ou les réseaux mais également dans certains délits spécifiques comme la contrefaçon de logiciels ou de bases de données, les infractions aux fichiers nominatifs, les fraudes téléphoniques ou aux chaînes à péage. D'une manière générale, elle n'enquête pas sur les infractions traditionnelles commises par Internet, hormis le cas où le mode opératoire est particulièrement technique ou inédit.

5. Les services de la Gendarmerie nationale face à la lutte contre la cybercriminalité

Le Service technique de recherches judiciaires et de documentation (STRJD) est chargé d'administrer l'information judiciaire, de faire circuler et traiter les messages de demande de rapprochement et de gérer les bases de données. Son relais sur le terrain est constitué par les brigades départementales de renseignement et d'investigation judiciaire (BDRIJ).

Au sein du STRJD donc a été constituée en 1998 une équipe chargée de détecter les infractions sur les réseaux ouverts au public. Depuis, cette équipe a crû progressivement pour atteindre l'organisation actuelle:

- le département de répression des atteintes aux mineurs sur Internet (RAMI) ;

- le département des investigations sur Internet (D2I), à vocation plus généraliste ;

- le département soutien et appui.

> *L'administration des Douanes est fortement investie dans la lutte contre les contrefaçons et, chaque année, elle parvient à intercepter d'importants volumes de marchandises prohibées de toute nature.*

La Division de lutte contre la cybercriminalité (DLCC) du Service technique de recherches judiciaires et de documentation (STRJD) de la Gendarmerie nationale a une compétence nationale en matière d'infractions liées à la cybercriminalité. La Gendarmerie nationale effectue une veille Internet au Centre technique qui forme un réseau d'enquêteurs spécialisés (NTECH). Cette entité procède, à la demande des unités de gendarmerie ou des magistrats, aux examens scientifiques ou expertises nécessaires à la conduite des enquêtes judiciaires, apporte aux unités d'enquête le soutien nécessaire au bon déroulement des constatations, participe à la formation des techniciens en identification criminelle et à l'information des enquêteurs, étudie le développement des matériels et des techniques d'investigation criminelle. L'Institut de recherche criminelle de la Gendarmerie est équipé d'un laboratoire pour récupérer les données stockées sur tous les supports numériques saisis tels que les disques durs, les téléphones mobiles et les smartphones. Les services d'expertise traitent les éléments de preuve numériques recueillis.

6. Les Douanes

L'administration des Douanes est fortement investie dans la lutte contre les contrefaçons et, chaque année, elle parvient à intercepter d'importants volumes de marchandises prohibées de toute nature.

Elle a pour mission de surveiller les flux de marchandises. Les services douaniers ne peuvent pas intervenir lors de la commande ou de l'achat en ligne d'un produit proposé sur un site Internet. Les saisies opérées dans le fret postal et le fret express, mode d'acheminement privilégié de la contrefaçon vendue sur Internet, représentaient environ 1 % des articles saisis en 2005, 16 % en 2011 et 30 % en 2012 (avec 1,4 million d'articles interceptés).

En 2002, un service national de douane judiciaire (C. pr. pén., art. 28-1 et R. 15-33-1 et s.) a été créé, permettant de renforcer le dispositif global de lutte contre la contrefaçon. Spécialement habilités, les agents de ce service ont la capacité d›effectuer des enquêtes confiées par des magistrats en vue de remonter les trafics à dimension internationale. La loi de lutte contre la contrefaçon du 29 octobre 2007 a élargi la compétence du service de douane judiciaire qui traite désormais de toutes les infractions prévues au Code de la propriété intellectuelle, qui touchent l'ensemble des droits de propriété intellectuelle. Aujourd'hui, environ 40 % de l'activité de ce service concerne la contrefaçon par Internet. Une cellule « *cyberdouane* » ayant vocation à lutter contre la criminalité sur Internet a été mise en place au sein de la direction nationale du renseignement et des enquêtes douanières et dispose de moyens importants et notamment d'une vingtaine de douaniers afin de faire de la veille et repérer des trafics. Le service « *cyberdouane* » *développe la coopération opérationnelle interministérielle en vue de détecter et traquer sur Internet les infractions. Il est devenu un acteur majeur de la veille coordonnée des administrations en charge de la* cyberdélinquance, afin de favoriser l'échange d'information entre services afin de remonter les filières.

II.– L'INSTITUTION JUDICIAIRE

La cybercriminalité fait inévitablement son entrée dans les prétoires et vient bousculer la justice qui doit désormais s'adapter au monde numérique et à ses dérives. Si depuis une trentaine d'années, les tribunaux se spécialisent (Jean J.-P., Les nouveaux territoires de la politique criminelle, RSC 2007, p. 666) de plus en plus en raison de la complexité croissante des contentieux (notamment en matière économique et financière, de terrorisme, de santé publique, de crimes contre l'humanité), tel n'est pas encore le cas pour la cybercriminalité mais cette voie est désormais ouverte, notamment depuis la publication du rapport *Bockel* (Bockel J.-M., La cyberdéfense : un enjeu mondial, une priorité nationale, <http://www.senat.fr/rap/r11-681/r11-681.html>) qui préconise la création d'une juridiction spécialisée.

En effet, il y aurait une logique à adopter une telle organisation s'agissant d'affaires présentant des aspects complexes de technicité avérée avec en outre une dimension internationale. Il apparaît nécessaire d'instituer un pôle juridictionnel spécialisé à compé-

tence nationale pour réprimer les atteintes graves aux systèmes d'information telles des cyberattaques d'envergure visant par exemple les organismes d'importance vitale (OIV), les administrations voire les États. La coopération judiciaire internationale fonctionnera d'autant mieux qu'elle s'appuiera sur ces pôles spécialisés disposant des personnes et des moyens adéquats pour traiter au mieux les dossiers les plus difficiles (Jean J.-P., précité).

Il faudra aussi dans un souci d'efficacité que toute la « *chaîne pénale* » soit spécialisée, c'est à dire parquet, instruction et juridiction de jugement. Par contre, pour les affaires courantes d'escroqueries par Internet, pédophilie par Internet et affaires moins complexes, on pourrait prévoir d'institutionnaliser le réseau des magistrats « *cyber référents* » bénéficiant d'une formation obligatoire au plan national tant au niveau du parquet que du siège. Un groupe de travail interministériel dédié à la cybercriminalité sera à l'évidence une force de proposition en la matière afin d'améliorer le traitement judiciaire des procédures. Par ailleurs, au niveau du ministère de la Justice, il serait pertinent de créer un véritable « *pôle numérique* » dédié à la mise en œuvre d'une politique pénale en la matière et au suivi des travaux européens – d'autant que l'on évoque à nouveau la création d'un poste de procureur européen – et internationaux relatifs à la cybercriminalité. Ce service devrait aussi avoir un rôle d'expertise et de conseil auprès des magistrats en poste en juridiction.

De même, à l'heure où une vaste réflexion est lancée sur la modernisation de l'action publique dans le cadre d'une commission présidée par M. Jean-Louis Nadal, procureur général honoraire près la Cour de cassation (<http://www.justice.gouv.fr/la-garde-des-sceaux-10016/toute-lactualite-de-la-garde-des-sceaux-10259/mission-confiee-a-m-jean-louis-nadal-25689.html>), la question des réponses et de l'organisation des parquets face à ce contentieux émergent que constitue la cybercriminalité devrait être inévitablement posée. En effet, la lettre de la mission précise d'ailleurs que « *les priorités de politique pénale doivent être repensées et s'articuler soit autour des phénomènes criminels ou délictuels causant les plus grands troubles ou préjudices à la collectivité soit vers les dommages aux victimes les plus graves* » (<http://www.presse.justice.gouv.fr/art_pix/LettremissionNadal.pdf>). Or, il apparaît que les cybermenaces entrent dans ce champ et ses incidences pénales appellent des réponses spécifiques et adaptées du ministère public puisque désormais les parquets sont inévitablement confrontés à une délinquance visant ou utilisant les réseaux numériques tel Internet pour commettre ses méfaits (Quéméner M., Vers une réforme globale de l'action publique, Revue du Grasco n° 6, juill. 2013, p. 7 et s.).

III.– L'ARSENAL EUROPÉEN ET INTERNATIONAL

La lutte contre les cybermenaces impose inévitablement des réponses coordonnées et internationales (<http://www.justice.gouv.fr/justice-penale-11330/cybercriminalite-la-necessite-dune-reponse-coordonnee-22472.html>). Le ministère des Affaires étrangères veille à la cohérence des positions françaises en matière de cybersécurité au sein des différentes instances et appuie le développement de partenariats internationaux dans ce domaine.

Au niveau européen, la cybersécurité s'inscrit aussi dans une stratégie précise et s'est concrétisée notamment en janvier 2013 par la création du Centre européen de lutte contre la cybercriminalité (<https://www.europol.europa.eu/ec3>), qui fait partie d'Europol et sert de point focal dans la lutte contre ce phénomène au sein de l'UE. Il a pour mission de mettre en commun le savoir-faire en matière de cybercriminalité au niveau européen pour aider les États membres à se doter de moyens, de contribuer aux enquêtes cybercriminelles des États membres et de permettre, en étroite collaboration avec Eurojust, aux enquêteurs européens sur la cybercriminalité, relevant de la justice comme des services de répression, de s'exprimer d'une seule voix.

> *Il faut aujourd'hui que les États s'inscrivent dans une vision prospective afin de mieux répondre aux évolutions de ces « cyberphénomènes » qui augmentent et se diversifient.*

On peut aussi citer l'Enisa (<http://www.enisa.europa.eu>) qui est l'agence européenne pour la sécurité des réseaux et de l'information qui participe aussi à la stratégie de cybersécurité de l'Union européenne.

Face à l'accroissement des cyberincidents qui peuvent causer un grand préjudice à la sécurité et à l'économie, une stratégie en matière de cybersécurité visant la sécurité des réseaux et de l'information (SRI) a été annoncée par la Commission le 7 février 2013 afin de garantir « *un cyberespace ouvert, sûr et sécurisé* » (Communiqué Comm. UE n° IP/13/94, 7 févr.2013, <http://europa.eu/rapid/press-release_IP-13-94_fr.htm>). Une coopération avec d'autres pays doit permettre de renforcer la sécurité dans l'UE et de protéger davantage les citoyens. Les pays de l'UE devront collaborer plus étroitement pour promouvoir la cybersécurité à l'échelle mondiale en insistant sur l'application de la législation internationale existante aux réseaux informatiques et en aidant d'autres nations à renforcer leur sécurité dans ce domaine.

Un des axes majeurs de la stratégie nationale est en effet le développement des coopérations internationales : outre la mise en place de relations bilatérales sur les questions de cybersécurité, la France contribue activement à la formulation de ces politiques au sein des organisations internationales. À cet égard, une attention toute particulière est porté aux travaux en cours à l'OTAN, à l'ONU, à l'OSCE, dans le cadre de l'Union européenne, mais aussi au Conseil de l'Europe (<www.coe.int>) qui s'attache à faire vivre la Convention de Budapest, seul traité actuel relatif à la cybercriminalité.

De même, des relations étroites sont établies avec Interpol (<http://www.interpol.int>) qui a mis en place une stratégie en matière de lutte contre la cybercriminalité qui s'articule autour de la formation, l'échange d'informations et la mise en place d'opérations internationales afin de démanteler des réseaux de cybercriminels.

IV.– LA MISE EN PLACE PROGRESSIVE D'UNE STRATÉGIE DE CYBERSÉCURITÉ

Il faut aujourd'hui que les États s'inscrivent dans une vision prospective (Wolf P., Vallée L., Cyberconflits, quelques clés de compréhension, Rapp. ONDRP 2011, p. 787 et s.) afin de mieux répondre aux évolutions de ces « *cyberphénomènes* » (Quéméner M., Cybersociété, entre espoirs et risques, L'Harmattan, 2013) qui augmentent et se diversifient. Malgré des efforts conséquents, on constate encore parfois un manque de lisibilité face à l'ensemble de ces structures

qui travaillent encore de façon trop cloisonnée alors que la lutte contre la cyberdélinquance implique une coopération accrue entre administrations avec la mise en commun des informations et du renseignement et avec le secteur privé.

Afin d'améliorer le traitement judiciaire des procédures relatives à la cybercriminalité, un groupe de travail interministériel mis en place en juillet 2013 rendra son rapport en fin d'année avec des préconisations concrètes et opérationnelles pour améliorer le traitement judiciaire des procédures relatives à la cybercriminalité sans méconnaître les problématiques économiques liées notamment au e-commerce et à l'emploi. Cette démarche interministérielle vise à l'adaptation de la norme, des méthodes et des organisations aux nouveaux enjeux posés par les cybermenaces et devrait ainsi parfaire cette stratégie globale de cybersécurité. L'efficacité de cette stratégie passe aussi par le renforcement des actions de sensibilisation et de formations pluridisciplinaires de l'ensemble des acteurs concernés. ■

Contrefaçon de marques et e-réputation sur les réseaux sociaux : les nouveaux défis des titulaires de marques

Internet et maintenant le développement des réseaux sociaux obligent les titulaires de marque à s'adapter constamment pour lutter contre les nouvelles formes d'atteintes à leurs droits que ces outils permettent de réaliser. Outre la difficulté d'identifier et d'appréhender ces atteintes, toute la question est de savoir si les moyens juridiques dont ces titulaires disposent sont bien adaptés et peuvent être mis en œuvre de manière efficace.

Par Aurélia MARIE

Associée du Cabinet Beau de Loménie

Et Carole GHASSEMI

Juriste stagiaire

Gaston VEDEL

Juriste

→RLDA 4846

Internet et maintenant les réseaux sociaux sont des outils formidables de promotion et de visibilité que les titulaires de marques se sont maintenant largement appropriés. Quelle marque n'a pas sa page Facebook, son compte Twitter, ne surveille pas le nombre de consultations de son site, ne fait pas vivre son blog. Selon une étude TNS Sofres de 2011, 44 % des internautes affirment « *aimer utiliser internet pour tenter de peser sur le comportement des entreprises* » (Étude TNS-Sofres, La réputation se joue-t-elle sur les réseaux sociaux ?, 8 févr. 2011). Mais l'usage de ces nouveaux modes de communication et d'échanges a également multiplié le domaine du possible en matière de contrefaçon et ainsi réactualisé pour les titulaires des marques, le vieux mythe des Danaïdes, condamnées à remplir sans fin un tonneau sans fond.

Ainsi, à peine les titulaires des marques ont-ils pris conscience de l'intérêt pour leur communication, d'être présents sur les réseaux sociaux, qu'ils doivent faire face aux problèmes et enjeux de l'e-réputation.

Quant à l'imagination des contrefacteurs, elle est, on le sait bien, sans limite et elle s'est bien entendu emparée de ces mêmes outils, pour développer de nouveaux modes de diffusion de leurs activités illicites, toujours plus difficiles à identifier. Ainsi, les atteintes portées aux titulaires de marques se multiplient et se diversifient encore, au travers du développement des réseaux sociaux. Celles-ci ne consistent d'ailleurs plus simplement en des actes de contrefaçon pure et simple, d'autres atteintes voyant le jour, au travers d'usages préjudiciables nouveaux, tels que le « *username squatting* » (cette pratique résulte de la fausse appropriation par un tiers d'un username identique ou similaire à une marque par le biais d'une adresse URL personnalisée telle que <http://facebook.com/marque>) ou le « *page squatting* » (cette atteinte vise l'utilisation par un tiers d'une marque afin de nommer une page risquant d'entraîner une confusion avec la page officielle de la marque. Le cas s'est par exemple posé pour la marque Coca-Cola dont deux fans avaient créé une page sur Facebook autour de la marque. L'entreprise a alors décidé de prendre contact avec ces utilisateurs influents et d'en faire ses porte-paroles) ou bien encore sous

la forme d'atteinte à l'e-réputation (*cf.* par ex. l'affaire *Nestlé Killer*, où au printemps 2010, la société Nestlé a été mise en cause par l'association Greenpeace pour ses pratiques liées à l'utilisation de l'huile de palme et à la déforestation. Face à la déferlante de critiques sur les réseaux sociaux fondées notamment sur le détournement du logo KitKat, le cours de l'action a chuté contraignant la société Nestlé à fermer sa page Facebook pendant plusieurs jours).

Plus d'un million six cent milles internautes ont montré leur soutien au bijoutier niçois *via* la page Facebook lui étant dédié (<https://www.facebook.com/soutienaubijoutierdenice>), à savoir l'atteinte portée sur la toile à l'image de la marque ou de son titulaire, sujet que les réseaux sociaux ont rendu particulièrement sensible. Il n'est que de voir la polémique suscitée par le nombre de « *like* » générés sur Facebook à propos de l'affaire *Stéphane Turk*.

Nous tenterons ici de faire le point sur les actions que peuvent mettre en œuvre les titulaires de marques, à l'encontre des atteintes portées à leurs droits sur les réseaux sociaux, étant précisé qu'en parallèle, la concertation avec les douanes dans le cadre des moyens qui leur sont donnés pour lutter contre la contrefaçon garde, bien sûr, toute son importance (*cf.* par ex. sur la question de l'intervention des autorités douanières, Marie A. et Lassemblée-Léon F.-G., La contrefaçon sur Internet : nouvelles difficultés, nouveaux enjeux, AJ Pénal 2012, n° 5, p. 263 et s.).

Le premier constat qui peut être fait d'évidence, est que le développement des réseaux sociaux rend plus difficile l'appréhension des atteintes portées aux marques (I). Il n'en reste pas moins que des réponses sont envisageables et peuvent être mises en œuvre avec succès, même si elles diffèrent parfois des solutions traditionnelles (II).

I.- LA DIFFICILE APPRÉHENSION DES ATTEINTES AUX MARQUES SUR LES RÉSEAUX SOCIAUX

Par atteintes portées aux marques, on visera ici tant les actes classiques de contrefaçon, à savoir la vente de marchandises contrefaisantes, que les usages non autorisés de la marque d'un tiers, y compris ces usages nouveaux apparus avec le développement des réseaux sociaux, ou bien encore les atteintes portées à l'image d'une marque sur la toile.

Dans tous les cas, ces atteintes, quand elles sont effectuées au travers des réseaux sociaux, sont particulièrement complexes à appréhender du fait des difficultés liées à leur qualification juridique (A) et à l'identification des personnes qui en sont responsables (B).

A.- Une qualification juridique difficile

Ainsi, la première question à se poser est de savoir si ces atteintes peuvent répondre à la qualification de contrefaçon de marque (1). Il convient aussi de déterminer si elles peuvent de manière alternative ou cumulative répondre à d'autres qualifications juridiques (2).

1. La contrefaçon de marque

Pour pouvoir être qualifié de contrefaçon de marque, l'usage que fait un tiers de la marque d'autrui doit être un usage dans la vie des affaires, susceptible de créer un risque de confusion sur l'origine des produits et services en cause dans l'esprit du consommateur concerné (*cf.* notamment, CJCE, 11 nov. 1997, aff. C-251/95, Sabel c/ Puma ; CJCE, 29 sept. 1998, aff. C-39/97, Canon ; CJCE, 22 juin 1999, aff. C-342/97, Lloyd).

Plus que du critère classique du risque de confusion, dont l'appréciation n'appelle pas de commentaire particulier, la qualification de la contrefaçon de marque sur les réseaux sociaux semble essentiellement dépendre du point de savoir si l'usage du signe protégé est effectué dans la vie des affaires (a) et s'il s'agit ou non d'une utilisation à titre de marque (b).

a) L'utilisation du signe argué de contrefaçon dans la vie des affaires

L'usage d'un signe protégé à titre de marque n'est susceptible d'être considéré comme contrefaisant que si le contrefacteur présumé a utilisé ledit signe dans la vie des affaires, c'est-à-dire, selon les critères posés par la Cour de justice des Communautés européennes (*cf.*, par ex., CJCE, 12 nov. 2002, aff. C-206/01, Arsenal Football Club) aujourd'hui Cour de justice de l'Union européenne, et repris par la Cour de cassation (*cf.* par ex., Cass. com., 10 mai 2011, n° 10-18.173, Bull. civ. IV, n° 72), dans le cadre « *d'une activité commerciale visant à un avantage économique et non dans le domaine privé* ».

Or on peut supposer que le plus souvent, l'usage par un tiers de la marque d'autrui sur les réseaux sociaux s'inscrira « *dans le domaine privé* », et qu'ainsi la réalisation de la condition d'usage dans la vie des affaires ne sera le plus souvent pas réalisée.

Force est de constater toutefois que, parmi les décisions ayant pu statuer sur ce sujet, nombreuses sont celles qui ont retenu la contrefaçon, bien que l'utilisation du signe protégé à titre de marque dans la vie des affaires n'ait pas été expressément caractérisée (*cf.* par ex., TGI Paris, 25 avr. 2013, n° 12/12159, AFFIF c/ La Palme d'Or, C. ; TGI Paris, réf., 19 oct. 2012, n° 12/57315, Alexy, Lombard c/ Groupon France, Gerin Lanaro ; TGI Paris, 6 juill. 2012, n° 11/03287, P. c/ Piment DDB SAS ; TGI Paris, réf., 21 juin 2011, n° 11/54113, F., Graphic Evolution, SAS IWTV c/ Pressimo On Line ; TGI Paris, 24 mai 2011, n° 09/18007, Nexity c/ R. ; CA Aix-en-Provence, 16 mars 2011, n° RG : 09/15033, S., L., Sintesia c/ CA Plus ; TGI Paris, 14 nov. 2007, n° 07/09760, La Guinguette Pirate c/ La Jonque). Néanmoins, ces espèces concernaient à chaque fois l'utilisation d'une marque dans un contexte manifestement commercial, si bien que l'existence d'un usage dans la vie des affaires n'a vraisemblablement pas été discutée par les parties.

On relève cependant certaines décisions qui ne retiennent l'existence d'une contrefaçon qu'après avoir expressément caractérisé un usage dans la vie des affaires, en reprenant les critères classiques dégagés par la Cour de justice et repris par la Cour de cassation en France (*cf.*, par ex., TGI Paris, 17 mai 2013, n° 12/01288, B. dit Chico, Jal Production c/ C. ; TGI Paris, 22 févr. 2013, n° 11/09488, Révolution mobile c/ NC Numéricable, Numéricable ; CA Paris, 20 févr. 2013, n° RG : 10/14470, Go On Media c/ Novapress, Radio Nova ; TGI Paris, 10 juill. 2009, n° 07/14171, Bayard Presse c/ Youtube LLC (US), Youtube LLC (IR)).

Ainsi, dans une ordonnance en date du 4 avril 2013, le président du TGI de Paris, a, dans une affaire relative à la reproduction de la marque semi-figurative H&M au sein de vidéos sur Youtube et Google visant à critiquer la politique de l'entreprise, écarté la contrefaçon, au motif que « *le signe reproduit sur leurs sites Internet ne vise pas plus à désigner qu'à promouvoir un produit qui serait offert à*

la vente, mais seulement à informer l'internaute du comportement éventuel de la société titulaire de la marque en question, de sorte qu'il n'a pas pour but de renseigner le consommateur sur la nature ou l'origine d'un produit et n'est nullement utilisé dans la vie des affaires » (TGI Paris, réf., 4 avr. 2013, n° 13/52578, SAS H&M Hennes & Mauritz Logistics GBC France, H&M Hennes & Mauritz c/ Google, Youtube LLC (US)).

Pourtant, dans une espèce assez similaire à la précédente, où étaient également en cause des actes de dénigrement et de contrefaçon de marque, le TGI de Paris a retenu une solution inverse en retenant la contrefaçon sans caractériser l'usage du signe argué de contrefaçon (*cf.*, par ex., TGI Paris, 24 mai 2011, n° 09/18007, Nexity c/ R.).

Hormis cette décision isolée, qui s'explique probablement par l'absence d'arguments développés par le défendeur, le contexte dans lequel s'inscrit l'utilisation de la marque apparait ainsi essentiel à la qualification de contrefaçon de marque utilisée sur un réseau social et en application des critères jurisprudentiels précédemment rappelés, il est par conséquent en principe nécessaire que cet usage se fasse dans un cadre commercial et non pas à titre simplement privé.

La qualification de contrefaçon est ainsi bien écartée lorsque l'usage de la marque est par exemple effectué par un utilisateur du réseau social pour commenter les activités du titulaire de la marque ou si cet usage consiste en des commentaires et appréciations effectués par les « *fans* » d'une marque donnée, même si cet usage n'est pas conforme à l'image que le titulaire souhaite donner à sa marque.

b) L'utilisation du signe argué de contrefaçon à titre de marque

Par ailleurs, l'usage de la marque d'un tiers sur les réseaux sociaux n'est susceptible d'être contrefaisant que si le signe en cause est utilisé « *à titre de marque* », c'est-à-dire pour identifier l'origine des produits et services concernés (*cf.* notamment, CJCE, 25 janv. 2007, aff. C-48/05, Opel ; CJCE, 11 sept.2007, aff. C-17/06, Céline).

De la même manière que pour l'utilisation du signe dans la vie des affaires (voir *supra*, § a), l'utilisation du signe pour identifier une origine de produits ou de services n'est pas systématiquement caractérisée par les juridictions françaises (*cf.* notamment TGI Paris, 25 avr. 2013, n° 12/12159, AFFIF c/ La Palme d'Or, C. ; TGI Paris, réf., 19 oct. 2012, n° 12/57315, Alexy, Lombard c/ Groupon France, Gerin Lanaro ; TGI Paris, 6 juill. 2012, n° 11/03287, P. c/ Piment DDB SAS ; TGI Paris, réf., 21 juin 2011, n° 11/54113, F., Graphic Evolution, SAS IWTV c/ Pressimo On Line ; TGI Paris, 24 mai 2011, n° 09/18007, Nexity c/ R. ; CA Aix-en-Provence, 16 mars 2011, n° RG : 09/15033, S., L., Sintesia c/ CA Plus ; TGI Paris, 14 nov. 2007, n° 07/09760, La Guinguette Pirate c/ La Jonque).

Le TGI de Paris a toutefois, dans un jugement en date du 22 février 2013, écarté la contrefaçon de marque alléguée par le demandeur, au motif que « *dans leur utilisation la plus exposée, à savoir dans le cartouche qui figure sur la page d'accueil du site internet, sur la page Facebook et sur le compte Twitter, les signes en cause étaient insérés au sein de la phrase* «la révolution du mobile commence… le 11 mai 2011», *qui sert manifestement à introduire l'événement de la conférence de presse et non à désigner un service.* […] *L'emploi de ces signes dans ces conditions ne peut pas générer de risque de confusion sur l'origine des services offerts* » (*cf.* TGI Paris, 22 févr. 2013, n° 11/09488, Révolution mobile c/ NC Numéricable, Numéricable).

De même dans une autre affaire, la qualification de contrefaçon a été exclue par le tribunal de grande instance de Paris, s'agissant de l'utilisation d'un « *signe protégé à titre de marque* […] *non pour désigner l'origine de services ou produits mais pour désigner [un] festival de musique ukrainien* » (*cf.* TGI Paris, réf., 3 févr. 2012, n° 12/50396, S. ZProject Ltd, Kazantip Gmbh c. B., C.).

Aussi, tant que l'usage d'une marque est extérieur à l'identification de l'origine des produits ou services que cette dernière vise, la contrefaçon ne semble pas pouvoir être retenue.

La nécessité, certes parfois théorique, pour les juridictions de caractériser un usage de la marque d'un tiers pour identifier l'origine de produits et services visés, laisse dès lors une latitude certaine aux utilisateurs des marques sur les réseaux sociaux et réduit significativement les possibilités, pour les titulaires de marque, de s'y opposer.

Néanmoins, d'autres qualifications alternatives, voire cumulatives peuvent être envisagées.

2. *Les autres qualifications envisageables*

Les utilisateurs des réseaux sociaux peuvent en effet voir leur responsabilité engagée sur d'autres fondements, et parfois même dans l'hypothèse d'une utilisation de la marque hors-commerce. Si la concurrence déloyale ou parasitaire (a), susceptible d'être aussi mise en œuvre, implique à nouveau un cadre commercial, la diffamation ou de l'injure publique (b), cette fois-ci en sont déconnectées.

a) Concurrence déloyale ou parasitaire

De manière assez classique, l'utilisation de la marque d'un tiers sur un réseau social peut – au-delà de la contrefaçon de marque – donner lieu à une condamnation pour concurrence déloyale ou parasitaire, notamment lorsqu'un tel usage est susceptible de tromper le consommateur sur les liens existants entre le contrefacteur et le titulaire de la marque.

Ainsi, l'utilisation d'une marque comme pseudonyme sur les réseaux sociaux peut être caractérisée de parasitisme lorsque celui qui usurpe cette marque tente de tirer profit sans bourse délier d'une valeur économique d'autrui lui procurant un avantage concurrentiel injustifié, fruit d'un savoir-faire, d'un travail intellectuel et d'investissements (*cf.* par ex., TGI Paris, 17 mai 2013, n° 12/01288, B. dit Chico, Jal Production c/ C.).

S'agissant de la protection de l'e-réputation, la répression du dénigrement, assimilé à un acte de concurrence déloyale et caractérisé par l'action de « *jeter publiquement le discrédit sur les produits, l'entreprise ou la personnalité d'un concurrent* » (*cf.* par ex., TGI Paris, 24 mai 2011, n° 09/18007, Nexity c/ R. ; TGI Paris, réf. 3 févr. 2012, n° 12/50396, S. ZProject Ltd, Kazantip Gmbh c/ B., C.), est susceptible de constituer une protection efficace à condition toutefois que les propos en cause soient considérés comme excédant les limites de la liberté d'expression, frontière subjective dont les contours sont difficiles à déterminer.

La qualification de dénigrement permet ainsi d'agir contre les appréciations négatives touchant les produits, les services ou les prestations d'une entreprise industrielle ou commerciale, alors que la loi du 29 juillet 1881 sur la liberté de la presse, on va le voir maintenant, ne permet quant à elle que de sanctionner une atteinte à la

réputation ou à l'honneur d'une personne physique ou morale exclusivement (*cf.* par ex., TGI Paris, 24 mai 2011, n° 09/18007, Nexity c/ R.).

b) Diffamation ou injure publique

La diffamation et l'injure publique sont des infractions pénales qui incriminent en effet respectivement « *toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne* » (L. 29 juill. 1881, art. 29, al. 1er, sur la liberté de la presse) et « *toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait* » (L. 29 juill. 1881, art. 29 *in fine*) et qui sont sanctionnées par des peines pouvant aller jusqu'à 1 an d'emprisonnement et 45 000 euros d'amende, et 12 000 euros d'amende.

Plus précisément, la diffamation doit être appréciée en tenant compte à la fois du contenu des propos et du contexte dans lequel ils s'inscrivent. Ils ne doivent pas consister en l'expression d'une opinion ou d'un jugement de valeur autorisés par le libre droit de critique, ce dernier cédant en revanche devant les attaques personnelles (*cf.*, par ex., TGI Paris, réf., 27 févr. 2013, n° 12/57704, G. c/ S).

Ces deux infractions supposent de surcroît une certaine publicité. La Cour de cassation a ainsi pu exclure la qualification de diffamation pour des propos tenus sur Facebook et MSN du fait que ces derniers n'étaient accessibles – du fait des paramétrages limitant l'accès aux propos litigieux – qu'« *aux personnes agréées par l'intéressée, en nombre très restreint* » (Cass. 1re civ., 10 avr. 2003, n° 11-19.530, Bull. civ. I, n° 70).

Mais au final, ces délits de presse sont régulièrement retenus par les juridictions pénales pour sanctionner des propos tenus par les utilisateurs des réseaux sociaux (*cf.*, par ex., TGI Bobigny, ch. corr., 15 nov. 2012, R., MMA Vie c/ L.).

Agir sur la base de ces incriminations peut aussi permettre d'obtenir la suppression des contenus correspondants sur les réseaux sociaux dans le cadre d'une action civile (TGI Paris, 29 févr. 2012, n° 11/18014, Clinique vétérinaire réservée aux chats), de ce point de vue souvent plus favorable au demandeur que l'action pénale, ou bien encore en usant des procédures offertes par la loi n° 2004-575 du 21 juin 2004 sur la confiance dans l'économie numérique (TGI Paris, réf., 2 août 2011, n° 11/56240, Cogefisd, Sogirouvet c/ Froidefond.).

B.– La difficile appréhension des personnes responsables des atteintes aux marques et à l'e-réputation sur les réseaux sociaux

La loi n° 2004-575 du 21 juin 2004 sur la confiance dans l'économie numérique (dite loi LCEN) a mis en place un régime de responsabilité dérogatoire du droit commun pour certains prestataires de services de la société de l'information, tels que les fournisseurs d'accès et les hébergeurs (1), limitant ainsi les possibilités d'action contre ces acteurs majeurs de l'internet alors que l'identification des personnes responsables des atteintes aux marques et à l'e-réputation et utilisatrices de leurs services est difficile (2).

1. *Les spécificités du régime de responsabilité des acteurs de l'Internet*

Aux termes de l'article 6, I, 2° de la LCEN, les hébergeurs de services de communication au public en ligne sont « *les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ».

Pour bénéficier de la qualification d'hébergeur, le titulaire du réseau social doit assurer le stockage d'informations mises en ligne par des tiers en se contentant d'assurer un rôle strictement technique et neutre. Cette qualification s'oppose à celle d'éditeur de services de communication au public en ligne, correspondant à la personne qui détermine, à tout le moins a une capacité d'action sur les contenus mis à la disposition du public.

Les réseaux sociaux exerçant leurs activités sous la qualification d'hébergeur ne peuvent être tenus responsables des contenus mis en ligne par les utilisateurs que (i) s'ils ne retirent pas immédiatement et volontairement les contenus à caractère manifestement illicites mis en ligne (contenus en matière de pédophilie, de crime contre l'humanité et d'incitation à la haine raciale), ou (ii) s'ils n'agissent pas promptement pour retirer les contenus illicites à compter de la notification du caractère manifestement illicite qui leur en est faite, par les titulaires de droits auxquels les atteintes sont portées (voir *infra*). À cet égard, la contrefaçon impliquant une part d'appréciation éventuellement subjective, les titulaires de marques ne peuvent compter sur un retrait systématique et spontané des contenus litigieux par les hébergeurs.

En pratique, il est de plus parfois difficile de déterminer la frontière entre hébergeur et éditeur de contenus dans la mesure où, souvent, les titulaires de réseaux sociaux réalisent un certain nombre d'opérations en complément de la stricte mise en ligne des contenus, correspondant à l'activité d'hébergement. Tant que ces opérations répondent à des contraintes d'ordre purement technique (limitation des risques d'incompatibilités de certains fichiers, optimisation de la capacité d'intégration du serveur, organisation et classification des contenus stockés, facilitation de l'accès de l'utilisateur), elles n'excluent pas la qualification d'hébergeur.

Il est en ainsi des opérations purement techniques de réencodage ou de formatage des fichiers accueillis (*cf.* par ex. TGI Paris, 29 mai 2012, n° 10/11205, TF1 et a. c/ Youtube ; Cass. 1re civ., 17 févr. 2011, n° 09-67.896, Bull. civ. I, n° 30 ; CA Paris, 14 avr. 2010, n° RG : 08/01375, Omar S. et a. c/ Dailymotion ; TGI Paris, 28 nov. 2008, Lafesse c/ Youtube, Canal + et Studiocanal ; TGI Paris, 15 avr. 2008, n° 08/01371, Lafesse c/ Dailymotion), de la mise en place d'outils de cadres de présentation, tels que des outils de mise en page, des champs permettant à l'éditeur de fournir des informations sur la nature du contenu ou la fourniture de lecteur des contenus mis en ligne (*cf.* par ex. TGI Paris, 29 mai 2012, préc. ; Cass. 1re civ., 17 févr. 2011, n° 09-67.896, préc.; CA Paris, 14 avr. 2010, préc. ; TGI Paris, réf., 9 févr. 2009, n° 09/51032, P. c/ B., Sivit, Univerpodcast, Myspace, ZePeople, iTunes Store), de la mise à disposition d'outils de classement et de gestion des informations mises en ligne, tels que des outils de navigation, des moteurs de recherche ou des outils de référencement (TGI Paris, 29 mai 2012, n° 10/11205, TF1 et a. c/ Youtube ; CA Paris, 13 oct. 2010, Roland Magdane c/ Dailymotion ; CA Paris, 14 avr. 2010, n° RG : 08/01375, Omar S. et a. c/ Dailymotion ; TGI Paris, 13 mai 2009, n° 08/15277, Temps Noir et a. c/ Youtube, Google Video et Dailymotion ; TGI Paris, 29 avr. 2009, Roland Magdane c/ Dailymotion ; T. com. Paris, 27 avr. 2009, n° 2007054335, Davis Film c/ Dailymotion ; TGI Paris, 28 nov. 2008, Lafesse c/ Youtube, Canal + et Studiocanal ; TGI Paris, 15 avr. 2008, n° 08/01371, Lafesse c/ Dailymotion) ou bien encore de la subordination du stockage au respect des conditions générales d'utilisation du site (*cf.* par ex., TGI Paris, 10 avr. 2009, n° 06/18473, Zadig Productions et a. c/ Dailymotion). Ces opérations doivent toutefois s'effectuer par auto-

matisme technique, sans que le prestataire de services de stockage n'intervienne ou n'opère de choix éditoriaux sur les contenus mis en ligne.

C'est dans le cadre de la jurisprudence intervenue dans ce domaine que les principaux titulaires de réseaux sociaux, tels que les sociétés Youtube et Dailymotion, pour leurs services d'hébergement de vidéos, ou encore Facebook ont pu voir leurs activités qualifiées de prestations d'hébergement de services de communication au public en ligne.

En revanche, dès lors que le titulaire du réseau social participe activement ou a une capacité d'action sur le contenu mis en ligne, il est qualifié d'éditeur et est soumis aux règles de responsabilité de droit commun. C'est ainsi que la société Go On Media, titulaire d'un réseau social permettant aux internautes de créer leur propre radio, a été considéré comme éditeur du contenu mis en ligne sur son réseau social du fait du « *contrôle du contenu des radios créées par les internautes, y compris sur les messages qu'ils peuvent diffuser, incluant notamment le titre et le slogan de la radio* » (CA Paris, 20 févr. 2013, n° 10/14470, Go On Media c/ Novapress, Radio).

2. *La difficile identification des personnes à l'origine des atteintes aux marques et à l'e-réputation*

Aux restrictions liées au régime de responsabilité spécifique des acteurs de l'Internet s'ajoutent les difficultés d'identification des personnes à l'origine des atteintes aux marques et à l'e-réputation.

En effet, les réseaux sociaux permettent à tout un chacun de mettre en ligne des contenus sans avoir à préalablement s'identifier ou en offrant la possibilité pratique de contourner les mécanismes censés permettre une telle identification. Les pseudonymes et autres noms d'usage sont ainsi fréquemment utilisés afin de dissimuler la véritable identité de l'auteur d'un contenu portant atteinte à une marque ou à l'e-réputation d'une entreprise.

La LCEN impose toutefois aux personnes mettant en ligne des contenus une obligation d'identification et aux hébergeurs de contenus, et ainsi aux réseaux sociaux, une obligation de conservation des données permettant l'identification des personnes contribuant à la création d'un contenu (LCEN, art. 6, II, 1°). Le manquement à ces obligations est théoriquement sanctionné pénalement par un an d'emprisonnement et 75 000 euros d'amende (375 000 euros pour les personnes morales).

L'obtention de ces données requiert toutefois d'obtenir du juge judiciaire, saisi sur requête, la levée d'anonymat et la transmission par l'hébergeur du contenu litigieux des éléments d'identification.

Encore faut-il s'adresser à l'entité juridique légalement hébergeur du contenu. Ainsi, dans une affaire où la demande de communication des éléments d'identification avait été dirigée contre la société Facebook France, alors que l'hébergeur du site Facebook était la société de droit américain Facebook Inc, les mesures de communication forcée initialement ordonnées ont été annulées (*cf.* par ex., TGI Paris, réf., 28 juill. 2010, n° 10/56491, G. c/ Facebook France, annulant les mesures de communication forcée ordonnées [TGI Paris, réf., 13 avr. 2010, n° 10/53340, G. c/ Facebook France]).

Encore faut-il également que l'hébergeur soit domicilié en France ou présente des critères de rattachement avec la France, pour que les dispositions de la loi LCEN puissent lui être appliquées (L. n° 78-17, 6 janv. 1978 mod., prévoyant que sont soumis à la loi française les traitements « *dont le responsable est établi sur le territoire français* » ou « *recourt à des moyens de traitement situés sur le territoire français* »). En effet, dans une espèce mettant en œuvre une procédure visant à obtenir la communication des données d'identification d'une personne ayant publié des contenus sur son compte Twitter, le président du TGI de Paris a considéré que les dispositions de la LCEN ne s'appliquaient pas à la société Twitter Inc., non établie en France, et dont il n'a pas été démontré qu'elle utilisait des moyens de la société Twitter France, ou de toute autre entité située sur le territoire français, autrement qu'à des fins de transit (TGI Paris, réf., 24 janv. 2013, n^{os} 13/50262 et 13/50276, UEJF, AIPJ, MRAP, LICRA, SOS Racisme-Touche Pas à mon Pote c/ Twitter Inc., Twitter France). Le président du TGI de Paris a toutefois fait droit aux mesures de communication des données d'identification des auteurs des tweets litigieux, détenus par la société Twitter Inc, sollicitées sur le fondement du droit commun (CPC, art. 145). Ces dernières devront, quoi qu'il en soit, faire l'objet d'une procédure d'exéquatur complexe et couteuse aux États-Unis.

Enfin, la procédure LCEN ne permet pas nécessairement une identification précise de la personne à l'origine de la mise en ligne des contenus litigieux. Ainsi, dans une affaire où la procédure sur requête fondée sur les dispositions de la LCEN avait été admise, les éléments d'identification fournis se sont révélés être manifestement inexacts car ils conduisaient à un individu *a priori* sans relation avec les faits reprochés. Toutefois, lors du jugement de l'affaire au fond, en se fondant sur un faisceau concordant d'indices mis en avant par le demandeur, tels que les relations professionnelles entretenues entre les protagonistes, le pseudonyme utilisé par l'auteur présumé des contenus contrefaisants, le TGI de Paris a estimé que cet auteur avait été suffisamment identifié (TGI Paris, 24 mai 2011, n° 09/18007, Nexity c/ R.).

II.– LES RÉPONSES ENVISAGEABLES POUR FAIRE CESSER LES ATTEINTES AUX MARQUES ET À L'E-RÉPUTATION SUR LES RÉSEAUX SOCIAUX

A.– Les actions envisageables à l'encontre de l'hébergeur

Dans la mesure où la jurisprudence considère que les actes de contrefaçon de marque ou d'atteintes à l'e-réputation ne constituent pas un contenu manifestement illicite au sens de la LCEN (voir *supra*), les titulaires de réseaux sociaux exerçant leur activité en tant qu'hébergeurs ne peuvent voir leur responsabilité engagée du fait de contenus portant atteinte aux marques ou à l'e-réputation de tiers que dans l'hypothèse où ledit tiers leur notifie l'existence dudit contenu illicite.

Une partie de la jurisprudence considère que cette notification est un préalable obligatoire pour la mise en œuvre de la responsabilité de l'hébergeur du fait de contenus illicites (*cf.* par ex. CA Paris, 9 mai 2012, n° 10/12711, 120 Films et a. c/ Dailymotion ; TGI Paris, 22 sept. 2009, n° 09/06246, ADAMI, Omar, Fred et a. c/ Youtube).

En outre, la notification doit respecter un certain formalisme et notamment préciser la date de la notification, les éléments d'identification du notifiant et du destinataire, la description des faits litigieux, les motifs pour lesquels le contenu doit être retiré, une copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.

La jurisprudence s'est initialement montrée partagée sur le respect de ce formalisme, certaines juridictions faisant preuve de souplesse en admettant que « *la connaissance effective du caractère illicite des données* [...] *peut* [...] *être prouvée par tous* [...] *moyens* » (*cf.* par ex. TGI Paris, 10 juill. 2009, n° 07/14171, Bayard Presse c/ Youtube LLC (US), Youtube LLC (IR)), alors que d'autres imposaient une notification strictement conforme aux dispositions de la LCEN. La Cour de cassation semble toutefois considérer que la notification doit inclure l'ensemble des mentions prescrites par la LCEN (Cass. com., 17 févr. 2011, n° 09-15.857, D, suivi par CA Bordeaux, 10 mai 2012, Amen c/ K.), imposant ainsi un lourd formalisme à la personne subissant une atteinte sur un réseau social.

Une fois la notification à l'hébergeur de l'existence des contenus litigieux réalisée selon les formes prescrites, il revient à ce dernier d'agir « *promptement pour retirer* [les] *données ou en rendre l'accès impossible* » (LCEN, art. 6, I, 2°). L'appréciation du prompt retrait des contenus illicites dépend essentiellement des faits propres à chaque espèce. En fonction des circonstances, la jurisprudence a pu estimer suffisamment rapide un retrait réalisé entre 12 et 72 heures à compter de la notification faite à l'hébergeur.

Dans l'hypothèse où l'hébergeur n'aurait pas procédé au retrait des contenus illicites dans un délai jugé satisfaisant, sa responsabilité peut être engagée sur le terrain du droit commun (C. civ., art. 1382). Aussi, quand bien même le contenu serait illicite du fait de son caractère contrefaisant, le réseau social-hébergeur ne devrait théoriquement voir sa responsabilité engagée que sur le terrain de la responsabilité délictuelle, ce qui est désormais majoritairement le cas en jurisprudence, malgré quelques décisions anciennes en sens contraire retenant – à tort semble-t-il – la contrefaçon de marques (*cf.* par ex. TGI Paris, 10 juill. 2009, n° 07/14171, Bayard Presse c/ Youtube LLC (US), Youtube LLC (IR)).

B.– Les actions envisageables à l'encontre de l'éditeur

1. *Les actions contentieuses*

Une fois l'identification de l'éditeur assurée (voir *supra*), plusieurs types d'actions judiciaires peuvent être engagées.

Dans le contexte des réseaux sociaux, où il est important de réagir avant tout « *buzz* » autour des propos incriminés, les actions en référé, voire en référé d'heure à heure, sur le fondement de l'article L. 716-6 du code de la propriété intellectuelle pour les atteintes aux marques et sur le fondement des articles 808 et 809 du code de procédure civile pour les atteintes à l'e-réputation, apparaissent les plus appropriées pour obtenir dans des délais très brefs la cessation sous astreinte des atteintes sur les réseaux.

Les actions au fond peuvent ensuite permettre, le cas échéant, une indemnisation plus complète du préjudice commercial ou d'image subi et des mesures complémentaires (publication du jugement). À cet égard, le tribunal de grande instance de Paris a pu retenir pour évaluer le préjudice subi par le demandeur, la banalisation et la dépréciation de la valeur des marques *La Palme d'Or* dues à l'utilisation du symbole très connu de la palme pour désigner des services de restauration (TGI Paris, 25 avr. 2013, n° 12/12159, AFFIF c/ La Palme d'Or, C.).

Toutefois, en pratique, le préjudice lié à la contrefaçon de marque sur les réseaux sociaux ou l'atteinte à la réputation du titulaire de marques ou de ses produits et services est encore assez mal indemnisé. À ce titre, les montants alloués au titre de la contrefaçon excèdent rarement 20 000 euros, même dans des décisions retenant la contrefaçon d'une marque renommée ou des atteintes d'une particulière gravité (*cf.* par ex., TGI Paris, 25 avr. 2013, préc., AFFIF c/ La Palme d'Or, C. [20 000 €] ; TGI Paris, réf., 19 oct. 2012, préc., Alexy, Lombard c/ Groupon France, Gerin Lanaro [provision de 10 000 €] ; TGI Paris, 6 juill. 2012, préc., P. c/ Piment DDB SAS [5 000 €] ; TGI Paris, 17 mai 2013, préc., B. dit Chico, Jal Production c/ C. [6 000 € au titre de l'atteinte à la marque, 10 000 € au titre de la concurrence déloyale et 15 000 € au titre du préjudice moral]).

2. *Les actions non-contentieuses*

En cas d'atteinte supposée à une marque sur les réseaux sociaux, il peut être risqué d'agir sur le terrain judiciaire. En effet, pour la majorité des utilisateurs, les sites communautaires sont perçus comme des espaces privés où chacun est libre de s'exprimer comme il le souhaite. Une action en justice pourra alors être perçue comme une « *agression* » par les utilisateurs de ces réseaux qui sont par ailleurs, autant de consommateurs potentiels des produits ou services proposés par la marque et son titulaire. Ce dernier risque alors très fortement, du fait de son action, un effet « *boomerang* » diamétralement opposé à celui initialement recherché (*cf.*, par ex., les affaires *Nestlé Killer, BP* ou encore *Detox*, préc.).

C'est pourquoi, en pratique, les titulaires de marque agissent souvent directement par le biais des outils mis à leur disposition par les réseaux sociaux. En vertu de leurs conditions générales d'utilisation (CGU), les propriétaires des réseaux sociaux soumettent leurs utilisateurs à certaines obligations et notamment celle de certifier qu'ils disposent des droits relatifs aux contenus qu'ils publient en ligne (extrait des CGU de Facebook : « *vous ne publierez pas de contenu et vous n'entreprendrez rien sur Facebook qui pourrait enfreindre les droits d'autrui ou autrement enfreindre la loi* »). Les utilisateurs peuvent donc voir leur responsabilité contractuelle engagée et la violation de leurs obligations au titre de ces CGU se règle en pratique par la fermeture des pages ou la suppression des contenus litigieux. Il est à noter que le titulaire de la marque n'étant pas partie au contrat, ce n'est pas lui qui pourra mettre en œuvre ces moyens d'action. Toutefois, le fait de notifier aux propriétaires de réseaux les contenus illicites permettra à ces derniers d'intervenir et de mettre en œuvre les mesures précitées prévues au contrat avec leurs utilisateurs.

Conscient que des violations des droits de propriété intellectuelle sont susceptibles d'être opérées par leurs intermédiaires, les propriétaires de réseaux sociaux ont également mis en place une procédure appelée « *auto-réglementée* ». Ainsi, la majorité des réseaux sociaux proposent la possibilité d'un dépôt de plainte en ligne (signaler une violation de vos droits - Marque de commerce <https://www.facebook.com/help/contact/?id=351297704961969>, <https://support.twitter.com/forms/trademark>, vérifiés le 27 sept.2013). Ce système qui se présente sous la forme d'un formulaire à remplir, s'apparente à une notification, et présente l'avantage de ne requérir aucune qualification précise de l'atteinte subie.

Si ces procédures sont rapides, efficaces et gratuites, elles ne permettent toutefois pas d'obtenir systématiquement la suppression de contenus portant atteinte à des marques ou à l'e-réputation de tiers, celle-ci restant la décision du propriétaire du réseau.

De fait, même si les solutions classiques prévues par notre droit restent applicables et peuvent trouver une certaine efficacité, il n'en reste pas moins qu'elles peuvent parfois sembler à la fois limitées et inadaptées

à la rapidité de la diffusion des informations sur les réseaux sociaux et à leur ampleur.

Aussi, la protection de l'e-réputation passe en réalité principalement par l'élaboration d'une stratégie de surveillance et d'occupation des réseaux sociaux. En effet, alors que 55 % des internautes (Enquête IPSOS, Marques et réseaux sociaux, un mariage mondialement heureux, 30 janv.2013) affirment que les réseaux sociaux leur permettent de s'informer sur les marques et les produits qu'elles représentent, les entreprises se dotent de *community managers* (Le *community manager*, ou animateur de communautés web, est un expert des communautés en ligne. Son rôle est de fédérer une communauté d'internautes autour d'un intérêt commun et d'animer les échanges sur ce thème, tout en veillant au respect des règles de bonne conduite au sein de la communauté. Il a pour mission principale de développer la présence de l'organisation dont il se fait le porte-parole [marque, association, personnalité...] sur les médias sociaux : <http://www.e-marketing.fr>) afin de pouvoir leur répondre au mieux et endiguer rapidement les atteintes susceptibles de dégénérer en mouvement collectif. À ce titre, s'est développé un nouveau phénomène : le *personal branding*, qui consiste à construire et organiser sa réputation sur Internet afin de promouvoir et de valoriser l'image de sa marque principalement par le biais d'agence de communication.

Il reste à espérer que le droit ne sera pas totalement évincé de ces enjeux et qu'il saura trouver des moyens efficaces et adaptés pour répondre aux nouvelles questions et aux nouveaux problèmes qu'ils génèrent.

Ainsi, et pour se référer à un dernier mythe, les titulaires de marque auront-ils le sentiment de ne pas avoir ouvert pour leur plus grand malheur la boîte de Pandore et, au final, les maux contenus dans la boite ayant été libérés, l'espérance leur reste de trouver les moyens de les surmonter et de s'en affranchir. ■

E-réputation : quels risques pour les entreprises et les particuliers ?

La réputation d'une entreprise qui hier reposait entre les mains d'un petit groupe de professionnels de la communication est devenue aujourd'hui, avec l'arrivée d'Internet et des réseaux sociaux la e-réputation. Cette e-réputation ne se construit plus dans le vase clos des entreprises mais par la prise en compte globale de l'ensemble de ses parties prenantes. Une évolution que trop d'entreprises tardent à intégrer dans leur stratégie de communication.

Par Karin ROUBAUDI

Fondatrice de l'Aventure Corporate, membre de l'Agence Française
www.aventurecorporate.com

→RLDA 4847

L'e-réputation est l'image « *online* » d'une personne physique ou morale.

Cette image, propre à chacun, est constituée de l'ensemble des contenus et opinions émises par l'organisation elle-même et ses parties prenantes sur les réseaux sociaux, les forums de discussion, les multiples sites et blogs institutionnels, des particuliers, des médias,... Nous retenons ici la définition des parties prenantes de R. Edward Freeman : « *tout individu ou groupe d'individus qui peut influencer ou être influencé par la réalisation des objectifs de l'organisation* » (Strategic Management : a stakeholder approach, Pitman, 1984).

Ces informations et avis, hier confidentiels ou réservés à une partie des publics de l'organisation, sont aujourd'hui partagés, commentés, enrichis et relayés sur La place publique virtuelle mondiale : le WEB.

Ainsi, l'opinion d'un seul individu peut aujourd'hui devenir la conviction de tous.

Aussi, gérer son e-réputation devient un pré-requis pour l'entreprise « *durable* », celle qui veut être performante dans un monde où la responsabilité sociétale attendue doit être intégrée et, notamment, la transparence des données, le respect des droits de l'homme et du travail, l'équité, la non-discrimination, la prise en compte des intérêts des parties prenantes et des générations futures.

Gérer son e-réputation constitue un enjeu majeur de communication pour toute organisation et *a fortiori* pour les grandes entreprises visibles, cotées ou non. Et, force est de constater que jusqu'à ce jour, l'exploitation de la toile étant encore récente, l'entreprise n'en a mesuré l'enjeu que confrontée à une crise majeure.

L'entreprise doit admettre la spécificité de la communication online : elle n'est plus le seul fait de l'entreprise. Aussi, afin d'éviter des scénarios de crise, la communication unidirectionnelle d'hier doit faire place à une communication partagée, fruit d'un dialogue, impliquant l'organisation et ses parties prenantes.

RÉÉQUILIBRAGE

Nous sommes ainsi passés de la domination de l'entreprise et de l'opacité de sa communication à une répartition plus égalitaire, à une transparence aujourd'hui devenue obligatoire par la règlementation et exigée par l'ensemble de ses publics, de sa communauté, virtuelle ou non.

Les parties prenantes de l'entreprise, partisans ou détracteurs, ont en effet tout loisir de créer leur propre espace et de discuter comme bon leur semble des avantages et inconvénients des produits. Et, ces forums peuvent par l'algorithme des moteurs de recherche apparaître en première position des propositions de réponses à une recherche sur une marque. C'est ainsi qu'une entreprise de pose de fenêtre bretonne a vu pendant plusieurs mois son nom suivi d' « *escroc* » en première position sur Google...

> *« Il faut 20 ans pour bâtir sa réputation, 5 minutes pour la détruire » (Warren Buffet).*

La réputation d'une entreprise n'est plus liée uniquement à la qualité de ses produits mais également à la confiance de sa communauté. Et, si à ce jour, il n'existe pas de données officielles permettant de chiffrer l'impact de l'e-réputation sur le chiffre d'affaires, les illustrations en la matière ne manquent pas. La crise que connaît « *Ba-*

rilla » en est l'exemple, révélatrice des dégâts sur internet engendrés par une communication malheureuse. Guido Barilla, président du groupe, a ainsi dû s'excuser publiquement jeudi 26 septembre 2013, après avoir déclaré la veille au soir sur l'émission « *La Zanzara* » de la radio 24 qu'il jugeait impossible pour son groupe de mettre en scène un couple homosexuel dans ses spots publicitaires : «*Je ne ferais jamais un spot avec une famille homosexuelle, pas par manque de respect mais parce que je ne suis pas d'accord avec eux. Notre famille est de type traditionnel; la femme y occupe un rôle fondamental*».

Depuis cet incident et malgré sa rétractation, les associations homosexuelles italiennes appellent au boycott de tous les produits Barilla en particulier sur Twitter.

COMMENT L'ENTREPRISE PEUT-ELLE MAÎTRISER SON E-RÉPUTATION ?

Tout d'abord, il s'agit d'accepter l'idée qu'elle n'est plus l'unique propriétaire de son image. Les parties prenantes de l'entreprise, par leurs échanges et avis publiés sur la toile, créent une partie de l'image des marques et en constituent des prescripteurs, que l'entreprise a tout intérêt à connaître et à comprendre.

Et, dans une société ou la défiance envers les porte-parole officiels (politiques, médias, entreprises) est à son apogée, l'avis en apparence libre et sincère de l'internaute a un poids qu'aucune entreprise ne peut négliger.

Accepter cette perte de pouvoir est incontournable et salutaire. Elle permet d'entendre et de comprendre les critiques, d'instaurer un dialogue et de construire une communication crédible.

Pour entendre, encore faut-il savoir écouter. Cette Lapalissade devient, dans le monde « *online* », une vérité première. Mais la plupart des entreprises sont loin d'être équipées efficacement, n'ayant pour la plupart pas encore développé l'outil premier de gestion de l'e-reputation : une revue « *web* ». Et, la veille limitée Google, Facebook et Twitter relève du cosmétique. L'entreprise du 21e siècle, moderne, performante et durable doit intégrer ce nouveau paradigme de la communication et agir de manière holistique et efficace.

ÉCOUTER, ANALYSER, RÉPONDRE, AGIR

Il appartient à l'organisation d'analyser avec pertinence les bruits du web et de déterminer là où l'intervention est nécessaire. Un exercice complexe où il n'existe pas de vérité absolue. Doit-on répondre à une fausse information ? Doit-on se taire devant une vérité dérangeante ? Doit-on faire appel à un cabinet d'avocats ?

Coca-Cola, pionnière de la surveillance online, n'a ainsi pas été suffisamment attentive à une fausse information née en 1997 affirmant que les boissons de la marque contenaient une faible dose d'alcool. En deux ans, et en l'absence de réaction de la firme d'Atlanta, la rumeur prit corps et devint une « *vérité internet* » au point que le site AL-Kanz.org, site influent dans la communauté musulmane, et auprès d'une partie des autorités religieuses, appela au boycott de la marque.

Il fallut à Coca-Cola de long mois de communication et une demande officielle auprès de l'organisme de certification de la mosquée de Paris pour inverser la tendance. Cette rumeur, toujours en circulation sur le web, oblige la marque américaine à une surveillance attentive des forums pour éviter tout nouvel appel au boycott.

L'EFFET « *STREISAND* »

Intervenir est capital, encore faut-il adapter sa réaction aux spécificités du web.

En 2003, Kenneth Adelman, un photographe amateur, publiait sur le site pictomia.com une série de photos aériennes de domaines privés aux fins de démontrer l'érosion du littoral. Parmi ces photos, se trouvait la maison de Barbara Streisand. Bien que celle-ci n'était pas identifiée comme telle, l'actrice intenta une action en justice contre le site et le photographe afin d'interdire la publication des photos et obtenir des dommages et intérêts.

Du jour au lendemain, le web s'enflamma devant ce qu'il considérait comme une « *agression* » et la photo du domaine Streisand fut copiée un nombre incalculable de fois sur des « *sites miroirs* » hébergés à l'étranger, rendant ainsi inopérante l'action de la justice. D'un non-évènement, une photo sans intérêt, vue par quelques dizaines d'internautes incapables d'y reconnaître le havre douillet d'une star mondiale, nous sommes passés à une information commentée et relayée dans le monde entier.

Cette anecdote est aujourd'hui enseignée dans les écoles de communication sous le nom d'effet « *Streisand* » dont l'équation s'inscrit ainsi :

1 : une information sans intérêt ;

2 : un apport de notoriété ;

3 : une agression ; .

4 : un buzz.

L'intervention est un exercice délicat comme dans toute gestion de crise, et doit donc être réfléchie et prendre en compte notamment la « *psychologie* » de l'internaute, aguerri et particulièrement critique, détenteur d'un pouvoir d'influence et de nuisance puissant. L'entreprise doit donc être en conformité avec la loi, répondre aux attentes de ses parties prenantes et agir en cohérence avec ses discours.

LE WEB, UN ACCÉLÉRATEUR DE CRISE

Sur internet, les propos de l'entreprise peuvent être conservés *ad vitam aeternam*.

Une vieille déclaration oubliée peut être du jour au lendemain à l'origine d'une crise imprévue. La marque Abercrombie & Fitch en a fait récemment la cruelle découverte. Elle est aujourd'hui attaquée par les internautes pour les propos tenus dans un journal papier par son PDG Mike Jeffries, il y a sept ans, qui à l'époque étaient passés inaperçus, et récemment repris sur un site internet : « *On n'engage que des gens beaux en magasins. Les gens beaux attirent les gens beaux et nous ne voulons vendre qu'aux gens beaux et cool. Les autres, on n'en veut pas* ». Depuis sa publication la polémique online ne désenfle pas, avec appel au boycott des produits et une incidence immédiate sur les ventes : -17 %...

Devant cette nouvelle donne, la tentation de se taire peut être grande chez certains dirigeants. Hélas, le silence n'est pas une réponse pertinente dans un monde où ce que les autres disent de vous peut être au moins tout aussi dommageable. Ainsi, le contrat signé en 2005 par Bruce Wasserstein, PDG de Lazard, par lequel il s'engageait à ne pas prendre la parole publiquement pour éviter de nuire à la réputation de la banque, se révéla inefficace puisque

d'autres pouvaient rapporter ses propos sans qu'il ne puisse intervenir.

DE L'INTÉRÊT DE METTRE EN PLACE UNE STRATÉGIE D'INFLUENCE

La légèreté avec laquelle encore les entreprises appréhendent la « *websphère* » laisse à penser que l'internaute ne serait pas un client comme les autres. Or, l'internaute est « *LE* » client d'aujourd'hui... on pourrait même avancer qu'il n'est plus un simple client mais une partie prenante éclairée aux pouvoirs élargis. Son intérêt pour un produit ou un service, et la façon dont il l'exprime, peut servir une marque ou la desservir s'il en est déçu.

La FNAC a fait dernièrement l'objet d'une récrimination particulièrement négative d'une cliente sur sa page Facebook. En y répondant immédiatement, avec des excuses et une promotion à la clef, la marque a retourné la crise à son avantage. Lorsque les internautes se sont étonnés de la disparition du post négatif de la cliente de la page Facebook, la FNAC a publié la lettre de cette dernière où elle demandait à ce que l'on retire son post en concluant : « *Chez nous pas de complot ni de censure, nous traitons les problèmes au grand jour* ».

Cet échange qui s'est déroulé en une journée a généré un important flot de messages de félicitation des internautes. Et ces messages sont toujours en ligne. Ainsi, une erreur bien gérée peut se transformer en succès.

Internet n'est pas un simple outil de promotion des ventes mais représente un formidable potentiel de développement de sa réputation. Une stratégie de communication durable et performante doit intégrer ce nouveau paradigme afin de répondre aux besoins de ses publics et en particulier des nouvelles générations. La communication sur les réseaux sociaux doit être réfléchie et orchestrée par la direction de la communication, avertie de la stratégie de l'entreprise et autorisée à répondre en son nom. Enfin, attention aux « *profils* » fictifs créés par certaines entreprises afin de valoriser une marque ou d'en attaquer une autre ; ces dérapages risquent de leur revenir en boomerang en termes de ROI « *Return On Influence* » comme en termes financiers. ■