L'information, capital immatériel de l'entreprise Comment concilier sécurité, enjeux économiques et libertés fondamentales ?

Garance Mathias et Charlène Gabillat
garancemathias(@)gmail.com

Avocat à la Cour
9 rue Notre Dame de Lorette – 75009 PARIS
Cabinet d'Avocats MATHIAS

Résumé L'information est une notion complexe, mais incontournable dès lors que l'on aborde la problématique de la sécurité des systèmes d'information. Toutefois, contrairement aux idées reçues, le droit n'appréhende que de manière lacunaire et disparate cette notion qui revêt pourtant un caractère économique considérable. L'entreprise n'a donc pas d'autres choix que de concilier ses propres impératifs (économiques, sociaux) avec les droits fondamentaux, et plus spécifiquement la liberté d'expression et le droit d'accès à l'information. Néanmoins, l'absence de protection satisfaisante par le droit de la notion d'information pousse les entreprises à organiser, elles-mêmes, par la voie contractuelle la maîtrise de la diffusion de leurs informations.

Mots clefs : information, sécurité, système d'information, droits fondamentaux, réseaux sociaux, vie privée, Internet.

1 Introduction

« celui à qui vous dites votre secret devient maître de votre liberté » La Rochefoucauld

De par sa nature polymorphe, l'information, actif immatériel et élément clé de l'entreprise, pose nécessairement la question de la sécurité des systèmes d'information. En effet, la préoccupation majeure des entreprises est aujourd'hui leur sécurité et plus précisément, la maîtrise de la diffusion de l'information au travers de ces fameux systèmes d'information. La gestion de la sécurité passe donc par des mesures d'ordre technique mais cette exigence est également appréhendée par le droit.

Or, force est de constater que le droit s'adapte difficilement aux défis posés par la société de l'information, notamment ceux mis en exergue par la sécurité des systèmes d'information ou ceux nés de l'émergence des réseaux sociaux. Il convient par ailleurs d'insister sur le fait que le

statut juridique de l'information faisait peu l'objet d'écrits avant l'essor des nouvelles technologies de l'information et de la communication.

Aujourd'hui, l'immatériel étant au cœur de la croissance économique, l'information est l'objet de toutes les convoitises, d'où la nécessité d'organiser sa protection. Par capital immatériel, on entend « tout ce qui n'est pas matériel ni quantifiable dans les comptes de l'entreprise, mais participe à la richesse matérielle de celle-ci. La reconnaissance de cette notion permet de prendre en considération des éléments non tangibles, sans réalité physique ni même financière immédiate, dans la richesse globale de l'entreprise » [1].

Au surplus, Internet s'est révélé être un média incontournable pour la diffusion de l'information, qu'elle soit vraie ou fausse, à un public le plus large possible (à titre d'illustration, les réseaux sociaux font partie intégrante du quotidien et le site Wikileaks a permis de mettre en exergue une nouvelle conscience citoyenne suite à la communication d'informations). Dès lors, de nombreux enjeux juridiques majeurs gravitent autour de cette notion.

Selon l'étymologie latine, informare signifie « donner une forme à un fait afin d'en assurer sa communication à quelqu'un ». Cependant, si plusieurs dispositions légales traitent de la notion d'information, aucune définition juridique n'est donnée par le législateur.

Quant à la doctrine, force est de constater qu'elle se perd dans les hésitations et la multitude de définitions proposées. Ainsi, à titre d'illustration, selon M. le professeur CATALA, l'information consiste en tout message formulé pour être transmis à autrui [2]. En revanche, M. le professeur GALLOUX définit l'information comme étant toute « forme ou (...) état particulier de la matière ou de l'énergie susceptible d'une signification [3] ». Force est de constater que le terme information semble échapper à toute définition juridique en raison de son aspect immatériel et volatile. Nous sommes donc en présence d'une notion « fuyante » [4].

1. C. BOURRET et al., « Capital immatériel et information professionnelle. L'émergence d'un concept nouveau : l'information durable », Documentaliste-Sciences de l'Information, 2008/4 Vol. 45, p. 4-12. DOI : 10.3917/docsi.454.0004

2. P. CATALA, « Ébauche d'une théorie juridique de l'information », Dalloz , chronique, 1984, p. 97 ss.

3. J.-C. GALLOUX, « Ebauche d'une définition juridique de l'information », D. 1994, chr., p.229 et s.

4. M. VIVANT, « La privatisation de l'information par la propriété intellectuelle », Revue internationale de droit économique, 2006/4 t. XX, 4, p. 361-388. DOI : 10.3917/ride.204.0361

Cependant, le principe, tant en jurisprudence que dans les textes, reste que l'idée n'est pas protégeable par le droit. En d'autres termes, comme le disait très justement Henri DESBOIS [5], les idées sont dites « de libre parcours » (ce qui explique notamment son absence de protection par le droit d'auteur). Le secret demeure donc encore à ce jour une notion pertinente. L'information, en vue de sa protection, voire de sa réservation, doit-elle suivre le même sort ? Encore faut-il pouvoir juger de manière stratégique de ce que l'on divulgue et de ce que l'on garde secret.

Ces propos et interrogations nous amènent à considérer que la notion d'information est indéniablement liée à celle d'intelligence économique. Or, la définition de l'intelligence économique elle-même est sujette à débat. Aussi, la définition qui semblerait la plus légitime serait celle donnée par le rapport MATRE [6], aux termes duquel il s'agit de « l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques. Ces diverses actions sont menées légalement avec toutes les garanties de protections nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleurs conditions de qualité, de délais et de coût ».

Ainsi, se distinguent trois fondements de l'activité d'intelligence économique : la collecte d'information, la protection de l'information et donc de la sécurité et, enfin, la veille d'influence ou de contre influence (appelée également désinformation). Par conséquent et de par sa valeur économique importante, l'information impose de mettre en œuvre une politique de sécurité du système d'information au sein de l'entreprise ; laquelle devra être nécessairement évolutive, de par la nature même du système d'information, et adaptée aux dispositions légales.

Il conviendra donc de s'interroger sur la manière dont la loi et les juges appréhendent cette notion d'information et de la nécessaire opposition qui ne manque pas de survenir entre certains droits fondamentaux et la volonté des entreprises de protéger leur patrimoine informationnel.

5. H. DESBOIS, Le droit d'auteur en France, 3ème éd., Dalloz, Paris, 1978, p.5 et s.

6. Intelligence économique et stratégie des entreprises, travaux du groupe présidé par Henri MARTRE, Commissariat général au plan, la document française, février 1994

2 L'information saisie par le droit

2.1 La notion d'information dans la loi

En dépit du fait que la notion d'information n'est pas définie in extenso par la loi, des droits spéciaux la concernant ont été organisés par le législateur. Ces dispositions légales demeurent cependant lacunaires et nous pouvons regretter l'absence d'uniformité entre celles-ci. Sans prétendre à l'exhaustivité, nous rappellerons les principaux textes abordant la notion d'information.

De prime abord, citons la loi Godfrain du 5 juillet 1988 (articles 323-1 et suivants du Code pénal) sur les intrusions informatiques, qui n'est efficace qu'en cas d'intrusion avérée et réprime l'accès ou le maintien frauduleux dans un système de traitement automatisé de données. Ainsi, le terme utilisé est ici celui de donnée et non celui d'information. De même, le législateur a organisé le régime du droit d'auteur et des producteurs qui ne permet pas de protéger efficacement l'accès et l'utilisation des bases de données. Encore une fois, notons l'utilisation du terme de données. Vient ensuite la législation sur les brevets, laquelle exclue expressément les méthodes, le savoir-faire, ou les idées. Là encore, la notion d'information est sous-jacente mais non utilisée en tant que telle. Egalement, la loi sur le secret de fabrique qui n'a d'intérêt que dans un domaine restreint puisque ne concernant uniquement et seulement que les personnes appartenant à l'entreprise. De même, les dispositions concernant la violation du secret professionnel, inadapté au secret des affaires, ont un champ d'application très précis et ne s'appliquent qu'à un nombre limité de personnes. Il parait également nécessaire de rappeler que la législation sur la protection des logiciels n'inclut pas la protection des informations traitées par le logiciel en cause. Si la législation relative à la concurrence déloyale et aux clauses de non-concurrence revêt parfois l'apparence d'une « issue de secours » pour les entreprises qui voient leurs informations utilisées par leurs concurrents, il est essentiel d'insister sur le fait que ce régime ne s'applique que dans des conditions difficiles à réunir. Enfin, citons la loi Informatique et libertés de 1978 (modifiée par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004) qui a un impact considérable sur les entreprises ayant à traiter de données nominatives, c'est-à-dire toutes données qui permettent d'identifier de manière directe ou indirecte un individu [7].

7. Article 2 de la loi relative à l'informatique, aux fichiers et aux libertés « Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à

Dès lors, en présence de cette multitude de textes, il apparaît que l'information est susceptible de bénéficier d'une protection selon des modalités extrêmement variables ; ce qui n'est pas pour faciliter la gestion de l'information et de sa sécurité par les entreprises. Notons tout de même la récente proposition de loi relative à la protection des informations économiques qui a été votée le 23 janvier 2012 en première lecture par l'Assemblée Nationale. Dans l'hypothèse où le Sénat adopte également ce texte, un nouveau délit de « violation du secret des affaires » sera inséré dans le Code pénal.

A cette occasion, une définition des informations à caractère économique protégées a été donnée par le législateur. Ainsi, il s'agit d'informations « ne constituant pas des connaissances générales pouvant être facilement et directement constatées par le public, susceptibles d'être source, directement ou indirectement, d'une valeur économique pour l'entreprise, et pour la protection desquelles leur détenteur légitime a pris, après consultation du comité d'entreprise et information des salariés de l'entreprise, des mesures substantielles conformes aux usages. »

2.2 La notion d'information face aux juges

Dans le cadre de ce développement, nous évoquerons la mise en état en matière civile et l'instruction en matière pénale. Il semble en effet opportun de rappeler quelques règles en matière civile d'administration de la preuve. Selon l'article 10 du Code de procédure civile, le juge peut ordonner d'office toutes les mesures légalement admissibles. En outre, l'article 11 du même Code permet au magistrat de tirer toutes les conséquences de l'abstention ou du refus d'une partie d'apporter son concours aux mesures d'instruction. Ainsi, le juge peut enjoindre à l'autre partie de produire, au besoin à peine d'astreinte, un élément de preuve qu'elle détiendrait.

Dans le cadre de l'instruction pénale, le tribunal pourra ordonner aux officiers de police judiciaire, notamment des réquisitions (demande de relevés de communications aux opérateurs, etc.), des perquisitions ou des saisies des supports des informations avec accès au système d'information. Sachant que les officiers de police judiciaire peuvent également créer des copies des données stockées sans qu'il soit nécessaire de saisir le matériel ou encore d'effectuer des perquisitions à distance. De manière générale,

un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. »

le magistrat est guidé par le principe de loyauté dans la recherche des preuves et celui de la présomption d'innocence dans le cadre pénal.

Un constat par voie d'huissier peut également permettre d'établir et de rapporter une preuve. En effet, la présence de l'officier ministériel permettra de s'assurer que l'information numérique est éligible au statut de preuve numérique. Pour ce faire, elle doit satisfaire les critères suivants : l'authenticité (origine de l'information), l'intégrité (le contenu de l'information) et la traçabilité (la chaîne de traitement de l'information). La collecte d'éléments de preuve est également possible sur les réseaux sociaux, sous réserve de ne pas franchir la frontière de la sphère publique. A titre d'illustration, il est ainsi possible pour un huissier de procéder à un constat via un « ami Facebook » par lequel il aura accès aux informations litigieuses.

Quelle que soit la nature de la procédure, le juge appréciera souverainement les faits et les éléments de preuve qui lui sont soumis à l'occasion des contentieux. En effet, le juge dressera sa propre hiérarchie des preuves, voire en rejettera certaines. Pour ce qui est du système d'information des entreprises, il est fort probable que le tribunal ordonne une expertise afin d'être éclairé par un homme de l'art sur l'aspect technique du litige, d'autant que la matière est une nouvelle venue dans les prétoires.

Expert dont le rôle est crucial compte tenu du fait que, bien souvent, le juge aura tendance à suivre les préconisations de ce dernier. Il convient en effet, de bien avoir à l'esprit que le rapport d'expertise susceptible d'être rédigé emporte, dans la majeure partie des cas, la conviction du tribunal et influence ainsi fortement la solution qui sera donnée au litige. A noter que ces expertises se dérouleront en présence des parties et seront soumises au respect du principe du contradictoire.

D'un point de vue économique, se pose également la question de la maîtrise des coûts de la preuve numérique. Dans cette optique, l'entreprise devra effectuer des choix quant aux mesures à mettre en œuvre, qu'il s'agisse de cibler les postes, les serveurs, les volumes ou de sauvegarder les informations. De même, il sera nécessaire d'adopter une logique d'anticipation, à savoir conserver les sauvegardes effectuées, constituer une documentation.

Par ailleurs, les juges sont également confrontés à la problématique du « vol » et du « recel » d'informations. L'enjeu juridique est de savoir si un élément immatériel comme l'information peut être l'objet d'un vol. L'article 311-1 du Code pénal définit en effet ce délit comme la soustraction d'une « chose », c'est-à-dire, dans la conception classique, un élément corporel susceptible de déplacement physique. Sur ce point, la jurisprudence

parait des plus incertaines. Après des décisions ambiguës, les tribunaux semblent ne sanctionner que le vol du support d'informations (clef usb, l'ordinateur, etc.). En effet, compte tenu de l'immatérialité des données, il n'y a pas de dépossession à proprement parler.

Suite au vol des données, l'infraction de recel peut également être caractérisée. En effet, l'article 321-1 du Code pénal définit le recel comme « le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit. Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit. Le recel est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende ».

Le recel ne sera constitué que si les choses détenues proviennent d'une action qualifiée de crime ou de délit par la loi : fondement nécessaire à l'élément matériel de l'infraction. L'élément intentionnel du délit de recel consiste en effet dans la connaissance de l'origine frauduleuse des objets recelés. Il appartiendra ainsi au Ministère Public ou aux parties civiles d'établir l'élément intentionnel de l'infraction, sachant que son existence relève de l'appréciation souveraine des juges du fond, au vu des éléments de preuve régulièrement soumis aux débats.

Ainsi, à titre d'illustration, la chambre criminelle de la Cour de cassation, dans un arrêt du 20 octobre 2010 a reconnu que « (...) pour déclarer M. X. coupable de l'infraction reprochée, [la Cour d'appel] énonce que celui-ci a sciemment recélé les fichiers clients de son ancien employeur, la société ADT France, en les détenant et en les utilisant, après son licenciement, sachant que ces éléments provenaient d'un vol au préjudice de ladite société (...) ».

Toutefois, dans le cadre de données immatérielles, il est difficile d'envisager un acte de détention matérielle au sens habituel du terme. Toutefois, ces informations, données collectées vont faire l'objet d'une conservation au sein d'une base de données.

3 L'équilibre entre protection de l'information et droits fondamentaux

3.1 La liberté d'expression, le libre accès à l'information et le droit à la protection de la vie privée sociétaire

De prime abord, le droit à l'information au public constitue une composante de la liberté d'expression, laquelle offre à toute personne la possibilité, non seulement d'exprimer individuellement des opinions, mais en-

core de communiquer des informations. Ce droit fondamental est consacré par la Convention Européenne de Sauvegarde des Droits de l'Homme en son article 10 [8]. En outre, toute personne intéressée par une information doit pouvoir en avoir librement connaissance. Le droit à l'information ou d'accéder à celle-ci est en effet considéré comme une véritable « pierre angulaire et garante la plus sûre de la démocratie » [9].

A cette liberté d'expression et au droit d'accès à l'information semble parfois s'opposer le droit au respect de la vie privée, du domicile et de la correspondance, consacré par l'article 8 [10] de cette même Convention. La vie privée se ramène à un ensemble d'informations diverses dont le ou les sujets principaux ne souhaitent pas a priori la divulgation. Selon le doyen CARBONNIER, la notion de vie privée peut se définir comme étant « la sphère secrète de la vie où l'individu aura le pouvoir d'écarter les tiers. C'est le droit à être laissé tranquille [11] ».

Cependant, compte tenu de cette définition et des dispositions de la Convention Européenne de Sauvegarde des Droits de l'Homme, cette notion peut-elle s'appliquer à l'entreprise ? La notion de vie privée n'est-elle pas trop réductrice aujourd'hui au regard de l'importance que peuvent revêtir les informations afférentes à une entreprise telle la rémunération des dirigeants par exemple ?

Cette notion étant d'origine prétorienne, il n'est pas exclu qu'au fil du temps, les juges continuent à la faire évoluer dans un sens favorable aux personnes morales dont on peut considérer qu'elles ont également un « droit à la tranquillité ». Dès lors, un équilibre doit être trouvé entre ces prérogatives d'égale importance. Il convient en effet de pouvoir obtenir réparation.

Par ailleurs, avec le développement des réseaux sociaux (Facebook, Twitter, Google +, etc.), il est de plus en plus difficile de protéger sa vie privée. Cela est d'autant plus vrai qu'une partie des informations sont divulguées à l'initiative même des personnes concernées (notamment les salariés) et que le droit à l'oubli n'existe pas à proprement parler. A noter

8. Article 10 de la Convention Européenne de Sauvegarde des Droits de l'Homme - Liberté d'expression « 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. (...).

9. In Libertés et Droits Fondamentaux, Dalloz 2005, 11ème édition, n°483, p.371

10. Article 8 de la Convention Européenne de Sauvegarde des Droits de l'Homme - Droit au respect de la vie privée et familiale « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

11. J. CARBONNIER, Droit civil, tome 1, PUF 1999

toutefois que la réputation numérique est encadrée par le droit, notamment celui du droit à l'image et du grief de diffamation.

Il convient de revenir sur la question de la preuve qui se pose avec acuité dans le milieu professionnel, notamment quant à sa validité mais également du fait qu'elle est susceptible de toucher directement les droits et libertés fondamentaux des salariés. En effet, s'il est loisible à l'employeur d'organiser la surveillance des salariés, ces derniers bénéficient d'une jurisprudence favorable à la protection de leur vie privée, quand bien même ils se trouvent sur leur lieu de travail. L'arrêt Nikon de la chambre sociale de la Cour de cassation du 2 octobre 2001 est, à ce titre, particulièrement protecteur des droits des salariés [12].

Aussi, à titre d'illustration, comment procéder lorsque l'employeur suspecte l'un de ses salariés de diffuser des informations dénigrant la société qui l'emploie ou bien, de vendre au plus offrant certaines informations confidentielles relatives à l'entreprise ? Plus précisément, comment concilier le droit des salariés au respect de leur vie privée et l'impact de cette exigence sur la validité de la preuve collectée avec la volonté – légitime – de l'employeur de protéger son patrimoine informationnel ?

Depuis un arrêt de la chambre sociale de la Cour de cassation du 18 octobre 2006 [13], une présomption du caractère professionnel des données hébergées sur le lieu de travail du salarié a été instituée. En revanche, s'il est clairement indiqué que le dossier est d'ordre privé, il est considéré que l'employeur porte atteinte à la vie privée de son salarié s'il en prend connaissance et ce, même si l'employeur a de fortes raisons de penser que le salarié, par exemple, capte frauduleusement des informations auxquelles il n'est pas censé avoir accès. A noter que la preuve sera parfois recevable dans l'hypothèse de risques ou évènements particuliers qu'il conviendra alors de traiter au cas par cas. Toutefois, il convient de s'entourer d'éventuelles autorisations judiciaires afin d'encadrer les opérations de constat dans le respect des règles du droit du travail.

12. « (...) Attendu que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale 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 ».

13. « Mais attendu que les dossiers et fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence (...) »

Le site d'informations Wikileaks, en publiant les rapports secrets du département de l'Etat américain a voulu mettre un terme aux agissements militaires des Etats-Unis à l'étranger. Indépendamment de la volonté d'informer et de faire primer la liberté d'expression, on ne peut douter qu'il y ait eu des dommages collatéraux, notamment du fait de la révélation d'identités par croisement d'informations. Se pose donc la problématique, au sein d'une entreprise, qui reste vulnérable, selon laquelle les mécanismes actuels de communication peuvent être inadaptés face aux réseaux sociaux.

Conformément à la loi pour la confiance dans l'économie numérique, l'hébergeur a l'obligation de conserver les données permettant l'identification de quiconque ayant contribué à la création d'un contenu mis en ligne et ce, pendant une durée d'un an. En outre, la Commission Nationale Informatique et Libertés est également souvent sollicitée par les internautes, dont des entreprises, se plaignant de la publication de propos qui leur sont défavorables. La loi Informatique et Libertés permet en effet à toute personne présentant des motifs légitimes de demander la suppression de données la concernant et diffusées sur Internet.

Lorsque les juges sont saisis de cette question, il est à noter que leur appréciation des atteintes à la réputation numérique est délicate compte tenu de ces nouvelles pratiques. En effet, l'évaluation du préjudice est complexe. Le juge, dont l'appréciation est souveraine, prendra alors en compte la nature de la publication, sa durée, sa réitération, si les faits sont anodins ou déjà connus du public, etc.

A côté des critères traditionnels tels que la notoriété de la société victime et la gravité du préjudice subi par elle, les juges du fond ont déjà estimé qu'il doit être tenu compte de l'attitude de la victime. Par conséquent, il est primordial que les entreprises mettent en place une protection de leur système d'information. En effet, à titre d'illustration, un juge pourrait fort bien considérer que telle ou telle mesure technique n'a pas été mise en œuvre.

Il existe également de nombreux régimes spécifiques en matière de manipulation offensive de l'information. La rumeur comme la désinformation sont des armes utilisées pour discréditer les concurrents ou les déstabiliser. La rumeur, qui peut se définir comme la divulgation de renseignements inexacts ou encore de faits partiellement exacts mais présentés d'une manière qui nuira nécessairement à l'entreprise concernée, aura inévitablement des impacts économiques négatifs sur cette dernière.

La désinformation (communication délibérée d'informations fausses, trompeuses ou de nature à induire en erreur) peut concerner des propos

semant le doute ou rapportant des difficultés rencontrées par un concurrent. Les pratiques de manipulation de l'information sont certes appréhendées par le droit mais d'une manière qui parait manquer de cohérence et de réactivité. Face à la rapidité de la propagation des informations sur Internet, les sanctions arriveront tardivement et il sera difficile de réparer le préjudice.

En dernier lieu, le développement de pratiques contestataires (défaçage de sites, détournement de la marque, déni de service, etc.) constitue une des nouvelles pratiques de malveillance en vogue. Là encore, même si la réponse juridique existe, celle-ci se heurtera le plus souvent à une impossibilité d'application compte tenu du caractère international de ces pratiques illicites. En effet, la pratique révèle les nombreuses difficultés que posent les infractions commises via internet. Le cybermonde reste en effet le seul domaine où les Etats exercent leur souveraineté car il n'existe que peu de coopération internationale en la matière. Ainsi, dès lors que l'origine de l'infraction trouve son origine hors de France, il est difficile d'engager des poursuites contre l'auteur du dommage.

3.2 La maîtrise de la diffusion de ses informations par l'entreprise

Pour maîtriser la diffusion des informations, il importe de contractualiser la sécurité du système d'information et d'organiser la responsabilité contractuelle. En effet, la gestion des accès aux comptes et aux données du système d'information fait partie intégrante de la sécurité des systèmes d'information.

La loi Informatique et Libertés impose, dans son article 34 [14], une obligation de sécurité et de confidentialité des données ce qui oblige le responsable du traitement à définir notamment une politique d'habilitation et de gestion des droits d'accès permettant de garantir les seules catégories de destinataires qui seront autorisés ont accès aux informations nominatives traitées.

Aussi, dès lors qu'il s'agit de contrôler l'accès à l'information, les clauses de confidentialité offrent une grande souplesse pour organiser le respect du secret des informations que l'on désire protéger, notamment dans le cadre de la négociation avec une autre entreprise. Ces clauses qui sont définies, d'un commun accord entre les parties au contrat, peuvent

14. Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

notamment aborder la notion d'informations publiques ainsi que les conditions d'une éventuelle divulgation à des tiers ou les modalités à mettre en œuvre pour assurer la sécurité des échanges (l'utilisation d'outils de chiffrement par exemple).

Au sein des entreprises, les salariés sont soumis à une obligation de discrétion. En effet, selon l'article 226-13 du Code pénal « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende ». Le secret professionnel s'impose en effet à ceux qui par leur état ou leur profession ont une obligation de secret en ce qui concerne les faits dont la connaissance leur est parvenue dans l'exercice de leur profession (avocats, banquiers, policiers, magistrats...).

Aussi, dans le domaine de la sécurité, la divulgation de l'information peut être soumise à des règles de protection comme le secret défense. Pour l'essentiel, la protection du secret défense est organisée en France par des articles du Code pénal, du Code de la Défense ou encore des instructions, des arrêtés. Ces textes régissent les différentes étapes de la vie des documents classifiés, de leur conception à leur destruction, en passant par leur conservation ou leur circulation. Ainsi, l'accès à d'éventuels documents classifiés, selon leur niveau de classification, est strictement lié à l'habilitation des personnels, et justifié par leur « besoin d'en connaître ».

Ne peuvent ainsi être autorisées à accéder à des éventuels documents classifiés, dans des catégories strictement définies (confidentiel, secret ou très secret défense), que certaines personnes, à l'issue d'une procédure d'enquête personnalisée par les services de sécurité, et sous réserve qu'elles occupent certains postes répertoriés le plus souvent dans des catalogues d'emplois. Ces habilitations délivrées après appréciation de la vulnérabilité éventuelle des personnes concernées peuvent être retirées à tout moment, selon l'évolution personnelle ou professionnelle du détenteur de l'habilitation. Les lieux de conservation des documents classifiés sont soumis à une réglementation stricte et le respect des normes de sécurité est garanti par des inspections régulières.

De même, il est également essentiel d'anticiper les hypothèses de départ des salariés. Or, nombreuses sont les entreprises qui font l'impasse sur ce principe pourtant primordial de la sécurité des systèmes d'information. En effet, la plus grande faiblesse de la sécurité du système d'information reste le facteur humain.

Dès lors, comment garantir que le salarié ne part pas avec le fichier client ou fournisseur dans le but de créer sa propre société, sur la base

de ces informations « volées » ? En effet, comme vu précédemment, les juges sont, encore aujourd'hui, hésitants quant à la condamnation du vol d'information. Aussi vaut-il mieux anticiper cette situation en mettant en place des clauses contractuelles.

En présence d'une clause de non concurrence, l'employé qui ne respecte pas cette clause engage sa responsabilité contractuelle tandis que la société qui débauche peut être condamnée sur un fondement délictuelle si elle connaissait l'engagement du salarié. De même, une clause de non sollicitation de personnel peut être signée entre deux entreprises concurrentes : sa violation pourra entraîner la mise en œuvre de la responsabilité contractuelle de la société violant son engagement.

Néanmoins, en l'absence de clause ayant un tel objet, l'article L1237-3 du Code du travail prévoit que le salarié ayant rompu abusivement un contrat de travail et qui engage à nouveau ses services est responsable solidairement avec l'entreprise débaucheuse du dommage causé au précédent employeur. Par ailleurs, le débauchage – notamment lorsqu'il a pour but l'accès illégitime à des connaissances – est également sanctionné par le droit de la concurrence déloyale dès lors qu'il y a désorganisation de l'entreprise dont le salarié est débauché.

Toutefois, comment distinguer ce qui relève de l'expérience personnelle de l'employé débauché des informations concernant l'entreprise à laquelle il a appartenu précédemment ? S'il semble légitime de s'approprier des connaissances personnelles tel ne semble plus être le cas lorsque le but du débauchage est en réalité d'obtenir les secrets de concurrents. A titre d'illustration, un employé agit de manière déloyale et frauduleuse, s'il utilise, de mémoire, les codes d'accès au système d'information de son ancienne entreprise afin de s'accaparer les fichiers clients.

4 Conclusion

Il est nécessaire de mettre en place une politique de sécurité efficace visant à protéger le patrimoine informationnel. Avec le temps et le progrès technologique constant, les personnes malintentionnées finissent toujours par trouver les moyens de passer outre les « barrières de sécurité » mises en place par l'entreprise pour empêcher l'accès à son système d'information.

Au surplus, dans ce contexte de crise économique, l'impossibilité pour l'entreprise d'exercer son activité suite à une captation frauduleuse de ses informations aurait des conséquences désastreuses. La politique de gestion des risques, pour être efficace, nécessite la mise en place d'une « culture juridique » au sein de l'entreprise. En effet, tous les employés de

l'entreprise doivent prendre conscience que leurs actions sont susceptibles d'avoir des conséquences juridiques à travers notamment des formations et des séminaires de sensibilisation. En parallèle, l'entreprise doit mettre en place des politiques internes, des chartes définissant la gestion de ses actifs immatériels.

Cette gestion de l'information impose de combiner les ressources juridiques avec les ressources techniques et organisationnelles.

Références

1. M.-P Lucas de Leyssac, « Une information seule est-elle susceptible de vol ou d'une autre atteinte juridique aux biens ? », Dalloz, chronique, 1985
2. J. Dupré, Pour un droit de la sécurité économique de l'entreprise, de l'espionnage industriel à l'intelligence économique, thèse, Nice, 2000
3. P. Catala, « Ébauche d'une théorie juridique de l'information », Dalloz , chronique, 1984
4. Nicolas Moinet, « De l'information utile à la connaissance stratégique : la dimension communicationnelle de l'intelligence économique », Communication et organisation 2009
5. Bourret Christian et al., « Capital immatériel et information professionnelle. L'émergence d'un concept nouveau : l'information durable », Documentaliste-Sciences de l'Information, 2008/4 Vol. 45, p. 4-12. DOI : 10.3917/docsi.454.0004