(In) sécurité du système d'information : quelles responsabilités ?

Marie Barel*

Juriste,
consultant spécialisée TIC
et sécurité de l'information et des systèmes
mbarel@links-conseil.net

Résumé Les risques associés à un problème de sécurité du système d'information et leurs conséquences juridiques en matière de responsabilité sont perçus par la plupart des professionnels de l'informatique et en particulier les DSI, les RSSI ainsi que les administrateurs Réseaux et Systèmes, comme une jungle peu lisible, porteuse de craintes diffuses et partant mal contrôlées. L'objectif de cette présentation est de donner à ceux inquiets au regard des responsabilités qu'ils encourent, quelques clés de décodage du système juridique susceptible de s'appliquer dans leurs activités quotidiennes de protection, de surveillance, de contrôle et de mise en conformité du réseau d'entreprise.

Ainsi, après un résumé des principes de mise en jeu de la responsabilité civile et pénale des personnes physiques et morales (section 1), nous examinerons, à travers différents cas, les principaux contextes opérationnels dans lesquels les acteurs de la sécurité de l'entreprise et, en particulier, les DSI ou les RSSI, continuent de s'interroger sur l'étendue de leur responsabilité (section 2).

Ordre juridique concerné : France

1 Notions élémentaires du droit de la responsabilité

Nous présenterons ici, de façon très résumée, les différentes voies d'action en responsabilité qui peuvent être envisagées, ainsi que les conditions auxquelles elles doivent répondre.

On distinguera ainsi la voie civile (1.1) de la voie pénale (1.2), dont on peut noter d'ores et déjà la divergence des philosophies, la première visant à une simple *réparation* pécuniaire du préjudice subi tandis que la seconde tend d'abord à obtenir la *punition* du justiciable[1].

[1] Notons ici néanmoins une particularité du droit français, que l'on ne retrouve pas généralement dans les droits étrangers, qui est que le juge pénal peut *simultanément*

1.1 La responsabilité civile

La responsabilité civile, qui consiste en l'obligation de réparer le préjudice causé à autrui, peut avoir différents fondements ; en particulier, les sources de responsabilité qui pourront être recherchées en matière de sécurité des systèmes d'information sont :

- l'inexécution d'une obligation née d'un contrat (**responsabilité contractuelle**) – à cet égard, on rappellera ici que l'externalisation de la gestion de la sécurité du SI par contrat (infogérance), si elle permet d'organiser les responsabilités respectives du client et du prestataire en fixant l'étendue de leur responsabilité *civile* ainsi que son plafond financier, elle ne permet pas à l'inverse d'alléger la responsabilité *pénale* du responsable sécurité de l'entreprise[2], l'aménagement contractuel d'un transfert de responsabilité pénale étant inopérant en cette matière qui est « d'ordre public »[3] ;

ou (en l'absence de relation contractuelle),

- la faute : on parle ici de **responsabilité civile délictuelle ou quasi-délictuelle,** selon que la faute a été commise de façon intentionnelle ou non (par négligence ou imprudence). Dans tous les cas[4], le demandeur à l'action devra rapporter la preuve à la fois d'une faute, d'un préjudice et d'un lien de causalité, l'appréciation portée par le juge se faisant en référence au comportement de l' « homme raisonnable »..., le problème pour le DSI –ou le RSSI- étant, de ce point de vue et comme le souligne un auteur avec humour, que « le concept de *DSI raisonabilus* n'a pas encore émergé de façon très claire » !

Cette faute, source de responsabilité, peut avoir été commise :

- par soi-même ; ou bien encore ;
- par une personne qui dépend de soi : **responsabilité dite « du fait des préposés »**, telle que prévue à l'article 1384 alinéa 5. Nous verrons plus loin dans nos développements dans quelles conditions la responsabilité de l'employeur peut être engagée du fait des agissements de ses salariés, et surtout comment il peut en principe s'en exonérer.

---

prononcer une sanction pénale et fixer le montant d'une réparation civile (lorsque la plainte est assortie d'une constitution de partie civile destinée à demander la réparation pécuniaire du dommage). Cette situation aboutit souvent à de curieuses conséquences, tantôt une peine symbolique assortie d'indemnisations élevées, tantôt une lourde condamnation pénale assortie d'un euro symbolique à titre de réparation.

[2] Sur ce sujet, lireciter2.

[3] En ce sens, la loi « Informatique et libertés » qui prévoit, en cas de sous-traitance de traitements de données à a caractère personnel, que l'entreprise qui confie ces données à un tiers porte elle-même, en tant que « responsable du traitement », toutes les obligations légales afférentes à la sécurité et la confidentialité des données. Dès lors, conformément à l'article 35 de la loi du 6 août 2004, c'est à l'entreprise cliente de prescrire au prestataire les mesures de sécurité que celui-ci doit respecter, et ce sera la responsabilité pénale de l'entreprise cliente qui sera recherchée en cas de problème.

[4] Articles 1382, 1383 et 1384 du code civil – articles qui, sur les 2328 que contient ce code représentent à eux seuls 10 % des décisions rendues par les tribunaux.

1.2 La responsabilité pénale

La responsabilité pénale, qui est une **responsabilité personnelle** (et non assurable), oblige de supporter la peine prévue pour l'infraction qu'on l'a commise soi-même. De plus, pour être punissable, rappelons qu'il faut rapporter la preuve des trois éléments constitutifs de l'infraction[5] :

- élément *légal* : suppose l'existence préalable d'un texte incriminant et sanctionnant les agissements visés (étape de qualification de l'infraction) ;
- élément *matériel* : suppose que l'infraction s'est matérialisée par différents actes (il peut s'agir aussi de l'omission de réaliser un acte prescrit par la loi ou le règlement)
- élément *intentionnel* : suppose la volonté (consciente et libre) de l'auteur. Il est important ici de faire la différence entre la *volonté* et le **mobile** (qui, lui, est indifférent[6]). Ainsi, la volonté détermine l'infraction alors que le mobile tente d'en justifier la commission, d'y apporter une raison, un motif. De même, lorsque la loi prévoit un *dol spécial* (par exemple, les actes de terrorisme supposent, pour emporter cette qualification, le " but de troubler gravement l'ordre public, ou la terreur "), celui-ci ne se confond pas avec le mobile : le dol spécial est invariable, pour une même infraction, quel que soit le ou les auteurs, tandis que le mobile, lui, reste personnel et varie suivant l'auteur.

Ainsi, il résulte de ce qui précède que, sur le plan pénal, la responsabilité de l'**employeur** (dirigeant de l'entreprise) ne pourra être retenue que si celui-ci a intentionnellement participé à la commission de l'infraction – ce qui constituerait un cas tout à fait exceptionnel, l'hypothèse la plus courante étant que le salarié a agi à l'insu de son employeur. Notons cependant bien ici que, comme le souligne d'ailleurs les plus éminents praticiens du droit[7], l'employeur (même en dehors de toute participation à la commission de l'infraction), qui aurait pris connaissance du délit commis par son salarié, aura le plus grand intérêt à dénoncer les faits aux autorités judiciaires, se plaçant ainsi du côté des poursuivants pour démontrer son absence d'implication dans les faits litigieux. Une abstention, voire pire le silence « en connaissance des faits », pourrait à l'inverse faire revêtir à l'employeur

[5] Article 111-3 du code pénal. Correspond à l'adage « *nullum crimen, nulla poena sine lege* » (« pas de crime, pas de peine sans loi »).

[6] Pour une affirmation du caractère inopérant du mobile en tant que fait justificatif d'une infraction, on peut citer dans le domaine SSI :

Soc. 1er octobre 2002, Gaz. pal. 20 avril 2003, p. 33, note Tessalonikos > au sujet d'un salarié qui avait voulu critiquer les choix de sa direction informatique en matière de sécurité ; à l'appui de ses critiques sur le dispositif en place, ledit salarié avait procédé à des tests d'intrusion sans autorisation de sa hiérarchie et accédé à des données auxquelles il n'était pas habilité à accéder avec son propre mot de passe. Confirmation de son licenciement pour faute grave.

[7] Par exemple, Me Alain Benssousan à l'occasion de la table ronde sur la « gestion de crise » (Eurosec 2005) ou Me Oliver Iteanu dans le cadre du Salon juridique de l'Internet et du numérique, édition 2004 – conférence sur » la responsabilité du RSSI dans l'entreprise ».

l'habit du complice ou, mais de manière encore plus improbable, la qualité de coauteur (à condition de prouver dans ce cas que la fourniture de moyens ayant concouru à l'infraction a été faite avec l'intention de commettre le délit).

Il convient également de souligner, pour la suite des développements, que les **personnes morales (entreprises)** ne peuvent être pénalement poursuivies que lorsque la loi ou le règlement le prévoit expressément, conformément à l'article 121-2 du code pénal. Par exemple, l'article 323-6 du code pénal prévoit que les personnes morales peuvent être déclarées responsables des infractions définies aux articles 323-1 et suivants (entrave ou atteintes aux systèmes et aux données informatiques).

Enfin, et surtout, la question de savoir si les **DSI*** et les **RSSI*** encourent une responsabilité pénale conduit à se pencher sur le mécanisme de la **délégation de pouvoir** « qui a pour objet et pour effet d'opérer un transfert de la responsabilité pénale du chef d'entreprise vers le préposé délégataire »[8].

La question de la délégation de pouvoir et de la responsabilité pénale du DSI/RSSI. –

Ainsi, comme a pu l'exposer précédemment Me Isabelle Renard [REN], les DSI et les RSSI encourent bien, en tant que spécialistes de la sécurité des systèmes d'information, une responsabilité pénale sous réserve que ceux-ci aient été investis dans ce domaine d'une délégation de pouvoir valable.

Pour ce faire, la preuve de la délégation qui doit être rapportée par le chef d'entreprise – et dont les fondamentaux du régime ont été fixés, en l'absence de dispositions légales y afférent, par les tribunaux eux-mêmes – consiste en la réunion de trois éléments qui caractérisent le transfert de compétences envers la personne délégataire :

1. *autorité* : signifie que la personne investie de la délégation doit avoir un pouvoir de commandement tel que les salariés appliquent ses directives. Ainsi, dans le cadre du SI*, le délégataire doit par exemple être en position de faire respecter les modalités d'utilisation des ressources informatiques définies dans la charte de l'entreprise. A cet égard, Me Renard, dans son article précité, s'interroge à juste titre sur le point de savoir si un RSSI peut être valablement muni d'une délégation de pouvoir, « *puisque généralement cette fonction ne s'accompagne pas de pouvoir hiérarchique* » ;
2. *compétences* : en matière de SI, s'ajouteront ici aux compétences techniques la connaissance et la maîtrise des textes légaux dont le DSI ou, éventuellement le RSSI, aura la charge de contrôler l'application ;
3. *moyens* : vise en particulier le budget alloué au délégataire pour mettre en œuvre les mesures nécessaires pour maîtriser les risques identifiés de l'entreprise.

[8] Ainsi, le mécanisme en question ne joue que dans le cadre de relations hiérarchiques organisées dans une entreprise ou un groupe d'entreprises et ne peut en aucun cas, comme nous l'indiquions plus haut, s'appliquer entre une société cliente et le salarié d'un tiers (infogérant par exemple).

Au-delà de ces conditions de validité de la délégation de pouvoir, d'autres exigences portant sur *l'objet* de la délégation doivent encore être satisfaites :

- la délégation doit être précise (à cet égard, si aucune règle de forme n'est en principe requise- la jurisprudence admettant même les délégations verbales dès lors qu'elles sont dépourvues d'ambiguïté -, le délégataire en matière de SI aura ici intérêt à exiger un écrit très précis quant à l'étendue de sa mission et quant au champ exact de la délégation de pouvoir), et
- elle doit revêtir un caractère de permanence (pas de délégation à une personne occupant temporairement le poste).

Enfin, d'après la jurisprudence, le chef d'entreprise est tenu d'informer le salarié des conséquences produites par la délégation de pouvoir, à savoir un transfert de responsabilité pénale, mais il n'est a priori pas nécessaire que le salarié l'ait formellement acceptée pour que celle-ci soit valable (par contre l'expression d'un refus ne permettrait pas que la délégation produise d'effet).

En dernier lieu, notons également que, depuis une jurisprudence relativement récente (Cass. Crim.* 30 octobre 1996), la sub-délégation de pouvoir est possible dès lors que le sub-délégataire est lui-même pourvu de la compétence, de l'autorité et des moyens nécessaires pour exercer sa mission. Ainsi, un DSI pourrait déléguer en partie ses pouvoirs à un autre salarié : le RSSI par exemple, ou plus vraisemblablement et dans le cadre de grands groupes, aux responsables informatiques chargés de départements ou de filiales (sous réserve du principe de non cumul des délégations de pouvoir[9]).

Ainsi, pénalement responsable sous réserve de délégation de pouvoir valide, on sait pourtant combien la mission de la DSI se complexifie au fil de l'adoption de nouvelles réglementations et normes internationales, ce qui rend chaque jour plus difficile la maîtrise d'un SI devenu la source potentielle d'infractions de plus en plus variées, parmi lesquelles :

- le téléchargement illicite de logiciels ou fichiers protégés par le droit d'auteur au sein de l'entreprise ;
- le manquement au respect de l'obligation de sécurité afférente aux données à caractère personnel[10] traitées par l'entreprise (données clients comportant des informations financières par exemple) ; et
- toutes les infractions pénales susceptibles d'être commises par les salariés sur le réseau en utilisant les moyens de l'entreprise (diffamation, trafic d'images pédophiles, fuite d'informations confidentielles, etc.).

Pour mesurer de manière plus concrète le risque de voir engager cette responsabilité « du fait du système d'information », nous envisagerons maintenant de traiter succinctement plusieurs hypothèses tirées du contexte opérationnel en matière de SSI.

[9] Suivant ce principe, pour une filiale ou un département déterminé, une seule personne devra être investie du pouvoir.

[10] Pour une définition, voir l'article 2 de la loi n ° 2004-801 du 6 août 2004 modifiant la loi historique « Informatique et libertés » du 6 janvier 1978 : `http://www.cnil.fr/index.php?id=300`

2 Cas de mise en jeu de la responsabilité dans différents contextes opérationnels SSI

Les cas de responsabilité civile ou pénale envisagés dans le cadre du présent article traiteront des hypothèses suivantes :

- *préjudice causé à un tiers* au travers du système d'information
- responsabilité engagée *du fait d'un salarié*
- responsabilité *du fait des mesures de surveillance opérées sur le réseau d'entreprise*
- responsabilité engagée *en raison d'un défaut de mise en conformité à la réglementation.*

2.1 De la responsabilité civile ou pénale du *fait d'un préjudice causé à un tiers* au travers du système d'information de l'entreprise

Cas du défaut de sécurisation d'un traitement de données à caractère personnel L'hypothèse posée est la suivante : une entreprise enregistre les réponses de ses clients à un questionnaire en ligne sur son site web dans un fichier non protégé auquel un tiers parvient à accéder. Il est précisé que ce fichier contient des données à caractère personnel et qu'il procède d'une collecte de données loyale et ayant rempli les formalités préalables de déclaration auprès de la CNIL.

Dans ce cadre, il est nécessaire de définir en premier lieu qui est le « responsable du traitement », au sens de la loi « Informatique et libertés ». La loi du 6 janvier 1978, modifiée par la loi n ° 2004-801 du 6 août 2004, le définit en son article 3-I comme celui qui détermine les finalités et les moyens du traitement considéré. Il ne s'agit donc pas, d'une manière générale, du service informatique ni du sous-traitant technique[11] qui a la charge de gérer ces traitements, mais bien de l'entreprise propriétaire de ces traitements et à travers elle, son représentant légal.

Ensuite, il convient de rappeler quelles sont les obligations qui pèsent sur le responsable d'un traitement de données à caractère personnel en matière de sécurité du fichier. Sur ce point, c'est l'article 34 de la loi précitée qui prévoit que :

« *Le responsable du traitement est tenu de prendre toutes précautions utiles (. . .) pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* »

En cas de manquement cette obligation de sécurité et de confidentialité des données, le législateur a prévu une peine de 5 ans d'emprisonnement et 300.000 euros d'amende (art. 226-17 du code pénal). Toutefois, en l'absence de prescriptions techniques précises, c'est au responsable du traitement de déterminer les

[11] Voir nos précédentes remarques concernant la responsabilité de l'infogérant SSI et les dispositions de l'article 35 de la loi du 6 août 2004.

mesures à mettre à œuvre, en fonction « *de la nature des données et des risques présentés par le traitement.* »

Enfin, sur les conséquences de l'absence de mesure de protection du système d'information et plus particulièrement de la partie d'un site web hébergeant des données à caractère personnel, il est intéressant de rappeler également, après l'affaire *Kitetoa*, que le responsable du traitement concerné se trouverait empêché de :

1 ° se constituer partie civile en vue de l'obtention d'une réparation pécuniaire car celui-ci ne saurait « *se prévaloir de ses propres carences et négligences pour arguer d'un prétendu préjudice* »[12] en réalité subi par les personnes concernées ;

2 ° reprocher à un tiers d'avoir accéder frauduleusement à ces données « *à défaut de toute indication [du caractère confidentiel] de ces données et de tout obstacle à l'accès* »[13].

Toutefois, cette décision majeure, qui prend le contre-pied de la position classique en caractérisant l'absence d'élément intentionnel par le défaut d'une interdiction (et non plus d'une autorisation[14]) *expresse* du maître du système et conditionne l'incrimination d'accès frauduleux à l'existence d'un dispositif de sécurité, ne doit pas être interprétée comme un revirement complet de la jurisprudence. Elle marque simplement, selon nous, une plus grande intransigeance à l'égard des certaines « victimes » d'accès frauduleux qui ont failli à leur obligation de sécurité prévue par la loi, les circonstances de l'espèce dans l'affaire *kitetoa* étant par ailleurs marquées par l'usage de « *moyens réguliers* » et par un contexte applicatif : pages d'un site web, " *qui ne font par définition l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services* " et où « *même s'agissant de données nominatives, l'internaute y accédant dans de telles conditions* (cf. supra, 2 °) *ne peut inférer de leur seule nature qu'elles ne sont pas publiées avec l'accord des intéressés.* »

Cas de l'attaque par rebond Prenons cette fois pour hypothèse celle de serveurs de messagerie mal configurés qui vont être utilisés par des pirates comme relais de *spamming* pour diffuser massivement un message à caractère publicitaire, mais qui contient en réalité un virus. Dans quelle mesure la responsabilité de l'entreprise et ses responsables (dirigeants, DSI, ...) peut-elle être engagée du fait du préjudice causé aux victimes de ces attaques ?

D'abord, précisons en ce qui concerne le *spam*, que celui-ci ne fait pas l'objet de sanction spécifique, mais peut être poursuivi sur d'autres fondements tels que la prospection commerciale non sollicitée, la collecte frauduleuse des adresses e-mails ou bien encore l'entrave au fonctionnement du système lorsque l'envoi répété des messages conduit (de façon intentionnelle) à une saturation de la

[12] Tribunal correctionnel de Paris, 13 octobre 2002 - *Revue Communication Commerce électronique*, mai 2002, p.31, note Grynbaum

[13] Cour d'appel de Paris, 12$^{\text{ème}}$ ch., 30 octobre 2002 – Même revue, janvier 2003, p. 30, note Grynbaum

[14] Cf. CA Toulouse, 31$^{\text{ème}}$ ch., 21 janvier 1999

bande passante des serveurs ciblés voir un blocage de l'accès à la messagerie (on parlera ici plutôt d'*e-mail bombing*).

Toutefois, en réalité, dans notre hypothèse, le *spam* n'est que le moyen de propager un contenu illicite, en l'occurrence un virus, ce qui est susceptible de relever du nouvel article 323-3-1 du code pénal, introduit par la loi du 21 juin 2004 (plus connue sous l'acronyme « LEN » ou « LCEN »). Pour mémoire, ce texte sanctionne :

« le fait, sans motif légitime, de d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. » [15]

Ainsi, on peut s'interroger sur le point de savoir si cette infraction est susceptible d'incriminer celui qui, de bonne foi, relaye ou retransmet le *mail* infecté par le biais de sa messagerie électronique elle-même compromise, à de nouveaux destinataires.

De prime abord, on pourrait répondre que, s'agissant d'un délit, le juge pénal exigera la preuve de l'intention du diffuseur du message[16], preuve souvent difficile à rapporter et qui en l'espèce devrait faire défaut puisque l'hypothèse envisagée est bien celle d'une transmission *involontaire* du message infecté. Cependant, les victimes infectées, et plus particulièrement les entreprises dont la productivité et la continuité même peuvent être gravement compromise suite à ces attaques virales[17], essaieront avant tout d'obtenir réparation de leur dommage en se plaçant sur le terrain de la responsabilité civile délictuelle ou quasi-délictuelle, le défaut de configuration du serveur pouvant alors être considéré soit comme une faute soit comme une négligence dans la sécurisation du système origine de l'attaque...

La tendance des juges à se montrer moins cléments avec les responsables de SI qui ne corrigent pas les failles de sécurité (cf. *supra*, affaire Kitetoa) impose dès lors de se montrer très prudent. En définitive, dans tous les cas d'attaque par rebond – qui recourent généralement à des techniques sophistiquées pour dissimuler l'installation par exemple d'un *rootkit* sur un serveur Web (tunnel IPV6, cryptage, logiciels anti-*forensic*, etc.)[18], et en particulier s'agissant des

[15] Pour plus de détails sur les conditions et le champ d'application de cette nouvelle disposition, voir notre article : *Nouvel article 323-3-1 du code pénal : le cheval de Troie du législateur ?* – MISC 14, juin 2004.

[16] Article 121-3 du code pénal : « Il n'y a point de crime ou de délit sans intention de le commettre, et donc la volonté de causer le dommage à autrui doit pouvoir être établie.

[17] Les particuliers victimes, elles, en raison du seuil de juridicité, adopteront plutôt un réflexe de protection technique (installation/mise à jour d'anti-virus) que d'engager des poursuites judiciaires ...

[18] Pour un panorama des publications sur les techniques anti-forensic qui consistent à détruire, camoufler, modifier des traces ou prévenir la création d' « empreintes électroniques » dans le but de limiter les moyens d'enquête ou d'examen d'un système, voir : *Anti-forensic*, L. Roger – Actes de la conférence SSTIC'05 (pp. 403 & s.).

grandes entreprises qui possèdent leur propre infrastructure (auquel cas elles peuvent être assimilées à un fournisseur d'accès au sens de la loi sur la sécurité quotidienne –LSQ– du 15 novembre 2001) doivent impérativement conserver toutes les preuves susceptibles d'établir leur innocence, et notamment les données techniques de connexion telles que stipulées dans le récent décret d'application du 24 mars 2006[19].

2.2 Responsabilité civile ou pénale engagée *du fait des agissements d'un salarié*

Cas des propos diffamatoires tenus sur le blog d'un salarié Il s'agit ici d'envisager les responsabilités encourues du fait des propos diffamatoires qui seraient tenus à l'encontre d'une société concurrente de l'entreprise par un salarié auteur d'un *blog* satirique. Ce dernier, bien qu'hébergé par un tiers, est administré par le salarié à son domicile, le soir, au moyen du portable mis à sa disposition par l'entreprise.

Comme indiqué plus haut, la responsabilité *civile* de l'entreprise ou de l'employeur peut trouver sa source dans la faute commise par un « préposé » (autrement dit un salarié), à moins qu'il ne démontre que celui-ci a commis un abus de fonction. C'est la Cour de cassation, dans un arrêt de principe rendu en chambre plénière du 19 mai 1988[20], qui a fixé les conditions dans lesquelles l'employeur (appelé ici le « commettant ») peut s'exonérer de cette responsabilité « de plein droit »[21], à savoir lorsque le « préposé » a agi :

i – *hors des fonctions* auxquelles il est employé,

ii – *sans autorisation* et

iii – *à des fins étrangères* à ses attributions.

Puis, la chambre criminelle de la cour a précisé dans un autre arrêt de 1988[22] qu'était dans l'exercice de ses fonctions le salarié qui a trouvé dans son emploi « *l'occasion et les moyens de sa faute* ».

Appliquée au domaine des technologies d'information, cette jurisprudence a donné lieu à une décision (que l'on jugera, avec d'autres [ITE], plutôt sévère) rendue par le TGI* de Marseille le 11 juin 2003 (*SA Escota c./ Sté Lycos, Sté Lucent Technologies et M. N.B.*[23]), dans laquelle les juges ont déclaré responsable

[19] Décret n° 2006-358 relatif à la conservation des données des communications électroniques (paru au JO du 26 mars 2006). C'est sans surprise que le texte a opté pour la durée de conservation maximum prévue par la loi, soit un an. De plus, il fixe les catégories de données à conserver : identification de l'utilisateur et destinataires de la communication, type d'équipements terminaux, date, heure et durée de chaque échange, services complémentaires utilisés, fournisseurs (soit, dans les grandes lignes, les données envisagées dans le cadre de la Convention sur la cybercriminalité adoptée en 2001).

[20] Bull. civ. n° 5 ; D.1988.513, note Larroumet

[21] C'est-à-dire automatique (il n'est pas nécessaire de rapporter aucune faute de l'employeur lui-même)...

[22] Cass.crim., 23 juin 1988 – Gaz.Pal. 1989.1.13, note Doucet

[23] Consultez les minutes du jugement sur : `http://www.juriscom.net/documents/tgimarseille20030611.pdf`

de contrefaçon l'employeur du créateur d'un site Internet litigieux[24] en constatant que "*le site litigieux a été réalisé sur le lieu de travail grâce aux moyens fournis par l'entreprise*" ; que, dans la mesure où « *la libre consultation des sites Internet était autorisée et aucune interdiction spécifique n'était formulée quant à l'éventuelle réalisation de sites Internet ou de fourniture d'informations sur des pages personnelles* », la faute salarié avait été commise « *dans le cadre des fonctions auxquelles il était employé* ».

Gageons que cette sévérité du tribunal dans l'affaire Escota (dont les faits sont parfaitement similaires à l'hypothèse retenue dans le présent cas) ne fera pas école et que les juges chargés de l'appel sauront rétablir l'équilibre en fonction de la réalité de la participation de chacun à la réalisation du dommage causé par les agissements d'un salarié.

A cet égard, on peut mesurer, au vu de ce premier jugement, l'importance que revêt l'interprétation des chartes de bon usage des ressources informatiques de l'entreprise. Ces documents, qui sont autant de véritables guides comportementaux, doivent en particulier permettre de dessiner très précisément les contours de l'usage à des fins privés toléré par l'entreprise, lequel comportera par exemple les critères de définition suivants :

- un usage non susceptible d'amoindrir les conditions d'accès professionnel
- ne mettant pas en cause la productivité de l'utilisateur
- ne portant pas atteinte aux intérêts ou la réputation de l'entreprise
- ni de nature à causer un quelconque préjudice à un tiers.

Responsabilité pénale du fait d'un comportement délictueux d'un salarié Après la responsabilité civile, il s'agit ici d'envisager la mise en jeu de la responsabilité *pénale* de l'entreprise ou son représentant du fait d'une *infraction* commise par le salarié dans le cadre de son emploi. Entre autres hypothèses, on peut citer ici deux exemples qui sont dans « l'air du temps » :

- téléchargement en mode P2P de fichiers pirates (audio, vidéo ou logiciels contrefaits) – art. L.335-3 CPI*
- téléchargement d'images pédophiles – art. 227-23 C.pén.*

En effet, la responsabilité pénale du chef d'entreprise (et de l'entreprise elle-même si la loi le prévoit – cf. *supra*, principe de légalité) peut tout à fait être engagée pour toute infraction causée dans l'entreprise par un préposé dans la mesure où le chef d'entreprise est tenu d'une obligation de surveillance et de contrôle sur le fonctionnement de l'entreprise. Cependant, force est de constater

[24] Plus précisément, il s'agissait d'un site satirique dénommé « Escroca », tendant à dénoncer les abus dont faisait preuve (selon le créateur du site) la société Escota, concessionnaire de la construction et de l'exploitation d'autoroutes du sud-est de la France. L'action intentée sur les chefs de contrefaçon de marque, contrefaçon des pages du site "escota.com" et pour les propos obscènes et les insultes proférées à l'attention de ses employés et de ses dirigeants, était dirigée contre le créateur du site mais également son hébergeur (*Multimania* devenu *Lycos*) et son employeur auquel il était reproché de ne pas avoir surveillé ses salariés.

que les cas de condamnation du dirigeant sur ce fondement sont très rares. Les raisons principales en sont les suivantes ...

Pour pouvoir être retenue, la responsabilité pénale de l'employeur nécessiterait de démontrer sa participation intentionnelle à la commission de l'infraction, scénario qui serait plutôt exceptionnel par rapport à l'hypothèse la plus courante qui est que le salarié agit dans ces cas de figure à l'insu de cet employeur. Ce dernier n'est donc certainement pas (sauf encore une fois, caractère très exceptionnel) co-auteur de l'infraction du salarié et, de la même façon, il ne revêtira généralement pas non plus l'habit du complice, l'élément moral de la complicité (qui est définie à l'article 121-7 du code pénal) impliquant, comme l'explicite les tribunaux, « *une participation volontaire et consciente de l'aide apportée à la commission d'une infraction* (...) »[25], « *une simple négligence ne pouvant être assimilée à une participation intentionnelle* »[26].

Ainsi, dans un jugement rendu par le Tribunal correctionnel du Mans le 16 février 1998 (Monsieur le Procureur de la République / Philippe H) où des images pédophiles avaient été téléchargées par un salarié sur l'Internet, la responsabilité du dirigeant n'a pas été recherchée sur le plan pénal.

Toutefois, il en aurait très certainement été autrement s'il avait été démontré que le dirigeant avait été informé du comportement délictueux sans rien faire pour le faire cesser. Il est donc fortement recommandé par l'ensemble des praticiens de veiller à toujours se placer « du côté des poursuivants » en dénonçant les faits auprès des autorités de police et justice, l'abstention ou le silence « en connaissance de cause » étant alors susceptible de se transformer en aide ou assistance à la commission du délit (cf. *supra*, Cass.crim. 23 juin 1988).

2.3 Responsabilité civile ou pénale engagée du fait des mesures de surveillance opérées sur le réseau d'entreprise

La cybersurveillance est au cœur des relations de travail modernes et le fragile équilibre entre le respect des droits du salarié (vie privée, secret des correspondances, ...) et le droit de contrôle et de surveillance[27] de l'employeur sous-tend la licéité des contrôles qui sont opérés sur le réseau d'entreprise. De nombreux écueils menacent ainsi le « long fleuve tranquille » (soyons un peu ironique !) qu'est aujourd'hui la vie des professionnels de la SSI qui voient dans ce domaine, à défaut d'un encadrement rigoureux, de nombreuses occasions d'engagement de leur responsabilité.

Cas du contrôle de la messagerie électronique Ainsi, en matière de contrôle de la messagerie électronique, la jurisprudence s'est progressivement formée et

[25] T.corr.* Lyon, 19 décembre 1983 – Gaz.Pal. 1985.somm.216, note Doucet
[26] Crim., 6 décembre 1989 – Dr.pénal.1990.117
[27] L'employeur tire ces droits de son pouvoir de direction - Cass. Soc 14 mars 2000 Dujardin c/ Sté Instinet

a mûri depuis l'arrêt Nikon du 2 octobre 2001[28]. S'agissant de la responsabilité des personnes en charge de ce contrôle, c'est la lecture de l'affaire du laboratoire de l'« ESPCI » qui suscite le plus d'intérêt (CA Paris, 17 décembre 2001), et ce à un double point de vue : d'une part, les juges du fond y ont adopté une interprétation restrictive de la notion d'interception illégale de correspondance et, d'autre part, ils ont précisé les limites de la mission de contrôle des administrateurs :

- Sur la notion d'interception illégale de correspondance : « *L'interception est définie par les dictionnaires Larousse comme Hachette autour de deux notions : d'une part, le fait d'arrêter quelque chose ou quelqu'un à son passage, d'autre part, celui de s'emparer, de prendre par surprise ce qui appartient à quelqu'un d'autre. Le tribunal* (TGI Paris, 2 nov. 2000) *s'est référé à cette seconde acception en retenant qu'il y avait eu "prise de connaissance par surprise". Or, (...) il résulte des espèces les plus proches des faits de l'actuelle procédure (Cass. Crim., 14 avril 1999 Dalloz 1999 Somm. p. 324 pour l'exploitation de la messagerie d'un appareil "Tatoo" et CA Aix-en-Provence 12 décembre 1996 JCP 1997 jurisprudence 22975 pour un appareil Tam Tam) que ne constituent pas une interception la lecture et la retranscription de messages dès lors que celles-ci ne nécessitent ni dérivation ou branchement et sont effectuées sans artifice ni stratagème ce qui reprend d'ailleurs une précédente formule utilisée à l'occasion de l'écoute d'une conversation téléphonique (Cass. Crm. 2 avril 1997 bull n ° 131). Au cas d'espèce* (surveillance opérée à partir du serveur de messagerie), *aucun artifice ni stratagème ne peut être retenu. (...)* ».
- Sur les limites de la mission des administrateurs de réseaux : « *Il est dans la fonction des administrateurs de réseaux d'assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité ce qui entraîne, entre autre, qu'ils*

[28] Affirmation du principe de respect de la vie privée et du secret des correspondances personnelles, « *ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* » (`http://www.courdecassation.fr/agenda/arrets/arrets/99-42942arr.htm`), reprise dans plusieurs décisions des juges du fond (notamment, CA Chambéry – 6 novembre 2003, Mme Anne O. c./ CGEA Annecy : `http://www.foruminternet.org/documents/juridprudence/lire.phtml?id=961`), qui précisent que ne sont protégés que les seuls messages qui présentent un caractère personnel, à l'exclusion des correspondances de nature professionnelle. A cet égard, on soulignera que le juge ne manque pas, en ce qui concerne les critères de distinction entre messages à caractère privé et ceux d'ordre professionnel, de se référer le cas échéant à la norme définie dans la Charte d'utilisation de l'entreprise. Voir notamment : Conseil de prud'hommes Nanterre, 15 septembre 2005 (`http://www.foruminternet.org/documents/juridprudence/lire.phtml?id=980`) – au sujet de messages d'un salarié ne comportant pas la mention « PRV » (pour privé) imposée par la Charte, ou encore : CA Douai, 26 novembre 2004, M. Philippe B. c./ SA Laboratoires Pharmaceutiques Rodael, M. Paul E. (`http://www.foruminternet.org/documents/juridprudence/lire.phtml?id=957`)– au sujet de courriers à caractère professionnel mais stockés sur son PC et verrouillés dans des fichiers informatiques personnels du salarié.

> *aient accès aux messageries et à leur contenu, ne serait-ce que pour les débloquer ou éviter des démarches hostiles. (. . .) Par contre il apparaît des éléments du dossier que les (administrateurs) ont mis en place une surveillance particulière afin de connaître le contenu des correspondances émises ou reçues par (l'étudiant). (. . .) (Que si) La préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposaient – de la même façon que la Poste doit réagir à un colis ou une lettre suspecte. Par contre la divulgation du contenu des messages ne relevait pas de ces objectifs.* »

En définitive, l'arrêt de la Cour d'appel – dont nous venons de citer les principaux extraits –, contribue bien à clarifier le rôle et la responsabilité des administrateurs réseau (à cet égard, on soulignera que les recommandations de la CNIL concernant « le rôle des administrateurs informatiques » se situent également dans le droit fil de cette jurisprudence[29]). Cependant, il n'adresse pas de réponse précise à la problématique pratique qui va se poser dès lors aux opérationnels chargés du contrôle de la messagerie, à savoir comment réagir face à la constatation de faits graves et préjudiciables à l'entreprise au cours des opérations de contrôle[30].

Tenus à une obligation stricte de confidentialité les empêchant de révéler le contenu de ces constatations à leur supérieur hiérarchique qui dispose pourtant de l'autorité et du pouvoir de décision, les juges les autorisent simplement, et sans autre recommandation, à « prendre toutes les mesures que la sécurité impose ». La CNIL, quant à elle, pour tenter de répondre aux inquiétudes des administrateurs après de la condamnation de leurs pairs en 2001, indique dans son Rapport précité (cf. notes de bas de page) que ceux-ci seraient libérés de leur obligation de confidentialité dans les cas suivants :

- mise en cause du « bon fonctionnement technique des applications »
- mise en cause de la « sécurité » ou de « l'intérêt de l'entreprise »
- « disposition législative particulière » les contraignant à faire état des informations auxquelles ils ont eu accès dans le cadre de leur mission.

---

[29] 2ème Rapport sur la cybersurveillance sur les lieux de travail (Edition 2004, mise à jour décembre 2003 - `http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf`) : « Les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes sont conduits par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions à l'Internet, fichiers "logs" ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail. Un tel accès n'est contraire à aucune disposition de la loi du 6 janvier 1978. »

[30] Sur le sujet, lire : *Le rôle de l'administrateur réseau dans la cybersurveillance*, *Me Martine Ricouart-Maillet et Caroline Requillart* - `http://www.juriscom.net/pro/2/priv20020408.pdf`

On le voit, la situation des administrateurs est pour le moins inconfortable car les règles du jeu ainsi énoncées ne leur permettent pas de cerner véritablement leur marge de manœuvre en cas de constatation ou de suspicion de faits graves nécessitant des mesures de contrôle *non contradictoires*. De plus, seul un juge saisi sur requête est à même, en vertu de son pouvoir d'appréciation souverain[31], de qualifier les faits révélés par les traces enregistrées[32].

Cas de l'opération commando « bureau propre » ! De la même façon, les opérations de contrôle inopiné menées de plus en plus couramment par les départements sécurité de grandes entreprises dans le cadre d'audits de sécurité[33], trouvent leurs limites dans le même principe fondamental de respect de la vie privée des salariés et la chambre sociale de la Cour de cassation, dans un arrêt du 17 mai 2005[34], est venue préciser sur ce point les justifications dont peut se prévaloir l'employeur pour prendre connaissance des fichiers personnels des salariés.

En l'espèce, c'est la découverte par un employeur de photos érotiques[35] dans le tiroir du bureau d'un salarié *absent* qui l'avait conduit à effectuer une recherche

[31] Sur les règles de procédure en matière d'appréciation des preuves, voir dans les actes de la conférence SSTIC'05 : *Délits informatiques et preuve : le défi de l'impossible ?*, par Marie Barel

[32] Rappelons ici que la collecte et la conservation de ces traces, même assurée par un huissier de justice (sur ce point, voir le référentiel Inforensique SI04 : `http://www.celog.fr/sommaire.php3?page=referentiel`), doit toujours respecter un certain nombre de formes élémentaires destinées à garantir la qualité de la preuve et en particulier, décrire les conditions qui ont entouré les opérations de contrôle , les précautions prises pour prendre copie des données et en garantir l'intégrité. Pour un exemple de placement sous scellés jugé irrecevable, voir : CA Douai, 17 décembre 2004 – Me Philippe E. c/ Mme Marie-Claude M. > `http://www.foruminternet.org/documents/jurisprudence/lirephtml?id=954`

[33] Pour mémoire, l'intervention de Mme Pelegrin-Bomel au SSTIC'05 : *La sécurité chez Bouygues Telecom.*

[34] Texte de l'arrêt : `http://www.droit-tic.com/juris/aff.php?id{\_}juris=29`

[35] Précisons ici que la possession comme la consultation d'images érotiques ou bien même à caractère pornographique n'est pas constitutive en soi d'une infraction et relève de la seule privée du salarié, sauf lorsque ces images (ou vidéos) pornographiques sont susceptibles d'être vues ou perçues par des mineurs. Par ailleurs, en matière d'images pédophiles, la simple consultation ne relève pas directement des faits incriminés à l'article 227-23 du code pénal. Ainsi un arrêt de la Cour de Cassation (Crim., 5 janvier 2005 - `http://www.legalis.net/breves-article.php3?id{\_}article=1448`) a estimé justifiée la décision de relaxe qui était intervenue en faveur d'un homme qui avait consulté, dans un espace multimédia municipal, des images pédopornographiques sur Internet car le prévenu s'était contenté de visualiser ces clichés sans les enregistrer, les imprimer ou les envoyer à une adresse de courrier électronique. La seule captation automatique des images incriminées dans la mémoire temporaire de l'ordinateur pendant trois jours ne suffisait pas à matérialiser l'infraction de détention (en effet, statuant par défaut - c'est-à-dire en l'absence du

sur le disque dur de l'employé (et dont les juges du fond relèvent par ailleurs que l'accès à l'ordinateur n'était protégé par aucun mot de passe). Cette enquête, *non contradictoire* et occasionnée en dehors d'un contrôle systématique – ce qui, selon la Cour d'appel, lui conférait dès lors le caractère d'une « *circonstance exceptionnelle* », révéla « *un ensemble de dossiers totalement étrangers à ses fonctions figurant notamment sous un fichier intitulé « perso »* ", motivant un licenciement pour faute grave.

Or, suivant l'attendu de principe adopté ici par la Cour de cassation, « *l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus dans le disque dur de l'ordinateur qu'en présence de ce dernier ou celui-ci dûment appelé* », à moins que cela ne soit justifié par un « *risque ou évènement particulier* » (notions qui restent encore à préciser dans la jurisprudence à venir mais dont on peut estimer, par analogie avec celle adoptée en matière de fouille sur le lieu de travail[36], qu'elles reposeront sur trois types de critères :

- atteinte à la sécurité de l'entreprise,
- degré de gravité certain et
- caractère d'urgence.

2.4 Responsabilité civile ou pénale engagée du fait d'un défaut de mise en conformité à la réglementation

Face à un contexte réglementaire et normatif à la fois singulièrement étoffé et évolutif, la lisibilité des nombreuses obligations auxquelles les entreprises du secteur des technologies de l'information et des télécoms sont aujourd'hui soumises est relativement difficile, cependant que la mise en conformité à ces textes – qui fait souvent appel à des compétences de spécialistes pour en analyser la portée –, est mise à la charge des DSI dont la fonction se complexifie. Dès lors, dans un contexte opérationnel qui fait figure de terrain miné, on comprend aisément la pression à laquelle ils sont soumis face aux nombreuses responsabilités qui leur sont déléguées.

A titre d'illustration, on peut évoquer les multiples sanctions civiles ou pénales qui sont prévues par exemple en cas de non-respect :

- des dispositions concernant la collecte, la conservation, ... ou les flux transfrontaliers de données à caractère personnel (loi du 6 janvier 1978 modifiée) ;

- des règles applicables en matière de contrôle à l'exportation de biens de cryptologie (accords de Wassenaar) ;

- des obligations de conservation des données techniques de connexion qui s'imposent non seulement aux prestataires Internet dont le métier principal est de fournir un accès à l'Internet, mais s'appliquent aussi à toutes les entreprises qui fournissent une adresse de courrier électronique à leurs salariés (loi du 15 novembre 2001 ; décret d'application du 24 mars 2006 précités).

prévenu-, les juges ne pouvaient en l'espèce tenter de requalifier l'infraction en importation).

[36] Cf. en particulier : Cass.soc., 11 décembre 2001 (Bull., V, n ° 377, p. 303) - `http://www.juritel.com/Ldj{\_}html-491.html`

Qu'ils soient pénalement et donc personnellement responsables[37] ou bien la cible potentielle des mesures disciplinaires (licenciement entre autres) susceptibles d'être prise par exemple à la suite d'une condamnation civile à l'encontre de l'entreprise qui n'a pas respecté les obligations dont il lui incombait d'assurer l'application, les responsables opérationnels se trouve dans une position très délicate qu'il convient de gérer au mieux sur la base d'une véritable Politique de Gestion des Risques Juridiques (PGRJ).

En effet, la PGRJ offre aux dirigeants et aux responsables opérationnels un *outil de lecture globale du risque juridique*, dont on vient de souligner la difficulté de diagnostic et qui a également la caractéristique d'être transversal c'est-à-dire qui concerne l'ensemble des ressources d'une organisation. Pour mettre en oeuvre une politique de gestion des risques juridiques adaptée à l'entreprise et à son environnement, des outils (veille en particulier) et une méthodologie sont nécessaires. Les principales étapes de l'établissement de cette politique [VER] consisteront à la fois en :

- l'identification et la localisation dans les ressources de l'entreprise des risques[38] potentiels et des obligations au regard des spécificités de son activité et du cadre réglementaire auquel elle se rattache ;
- l'évaluation du risque eu égard à la stratégie de l'entreprise (notamment, définition du niveau de risque acceptable en prenant en considération l'environnement juridique mais aussi technique, commercial, humain et organisationnel dans lequel l'entreprise évolue) ;
- un traitement du risque (réduction) et la gestion du risque résiduel, notamment par le recours à l'assurance.

Enfin, condition *sine qua* none pour assurer la pérennité de l'activité de l'entreprise par une mise à jour en continue de la cartographie des risques établie *ab initio*, une information et une sensibilisation des collaborateurs s'avère indispensable de façon à la fois à améliorer leur culture juridique et leur permettre d'être en mesure d'identifier de nouvelles zones de risques, contribuant ainsi à faciliter l'adaptation de l'entreprise aux changements de l'environnement juridique, économique et technique.

3 Conclusion

Ce bref exposé de la problématique de la responsabilité en entreprise liée à la gestion du système d'information et des réseaux nous a permis, à travers quelques exemples parmi les plus symptomatiques, d'entrevoir les principales catégories

[37] Sur les conditions de validité de la délégation pénale, se référer pour mémoire à la section 1.2 du présent article.

[38] Sur la notion de risque, notons ici qu'elle peut recouvrir deux acceptations, l'une négative, qui se décline principalement en risque pénal, risque financier et risque d'image, et l'autre, positive, au sens non plus de vulnérabilité mais au contraire d'opportunité pour l'entreprise qui saura anticiper les évolutions de son environnement et tirer un avantage concurrentiel des normes nouvelles.

de risques qui doivent être pris en considération au sein de la politique de gestion des risques juridiques.

Cette démarche, dans laquelle les juristes sont eux-mêmes amenés à évoluer pour proposer en premier lieu des solutions plutôt que de « dire le droit », doit permettre en particulier aux responsables opérationnels du SI dont les activités génèrent des risques de plus en plus en nombreux, de mieux maîtriser ces risques en acquérant la connaissance nécessaire des normes juridiques applicables à leur métier et d'identifier efficacement les comportements transgressifs au travers un tableau de bord des risques juridiques.

Trop souvent perçue encore comme un poste de charge inutile, la PGRJ, qui participe d'une meilleure gouvernance de l'entreprise, permet à n'en pas douter de prévenir des sinistres dont les conséquences financières sont généralement sans commune mesure avec les investissements induits par sa mise en œuvre.

Références

[ITE] Iteanu O. (2004), *Tous Cyber Criminels*, JML Editions, ISBN 2-84928-042-9.

[REN] Renard I. (2005), Les DSI et les RSSI sont-ils pénalement responsables ? (à propos de la délégation de pouvoir) `http://solutions.journaldunet.com/0502/050202{\_}juridique.shtml`

[VER] Verdun M. (2005) *La gestion des risques juridiques*, Editions Eyrolles, ISBN 2-7081-3606-2.

Abréviations

CA Cour d'appel
Cass. Cour de cassation
Civ. Chambre civile (de la)
Crim. Chambre criminelle (de la)
Soc. Chambre sociale (de la)
C.Civ. Code civil
C. Pén. Code pénal
CPI Code de la Propriété intellectuelle
DSI Directeur (ou Direction) des systèmes d'information
PGRJ Politique des Gestion des Risques Juridiques
RSSI Responsable de la sécurité des systèmes d'information
SI Système d'information
TGI Tribunal de Grande Instance