Les agissements en ligne des salariés : un risque majeur pour les entreprises

Nicolas Samarcq
Juriste TIC
nsamarcq@lexagone.com

Luc Masson
Responsable de rédaction
Lexagone.com

Lorsque des salariés commettent des actes illicites considérés comme fautifs ou non et qu'ils causent à autrui[1] des dommages, l'employeur[2] répond de ces dommages sur le fondement de l'article 1384 alinéa 5 du Code civil.

Nous rappellerons ici pour mémoire que la responsabilité pénale du chef d'entreprise du fait d'un de ses salariés n'est envisagée que très restrictivement par la jurisprudence en application du principe de personnalité des peines[3]. Toutefois, ce principe connaît quelques modérations. En effet, en matière d'hygiène et de sécurité, les faits dommageables accomplis par des salariés au sein de l'entreprise rejaillissent sur la responsabilité pénale de l'employeur[4], sauf délégation de pouvoir valablement constituée[5].

Il en est de même en cas de mise en jeu de la responsabilité civile de l'employeur pour les agissements de ses salariés réalisés à partir du matériel informatique de l'entreprise. En principe, sa responsabilité personnelle ne peut être mise en jeu qu'à la triple condition que le salarié (préposé, au sens du Code civil) soit toujours sous la subordination juridique de l'employeur, qu'il ait causé un dommage à l'occasion de son travail et avec les outils de l'entreprise, utilisés conformément à leur destination.

Sans revenir sur la genèse juridique de l'article 1384 alinéa 5, nous savons que la responsabilité civile de l'employeur était envisagée dans ce cas précis comme une garantie de solvabilité offerte aux victimes. Pendant longtemps, les juges ont ainsi exigé qu'une faute volontaire ou non du salarié soit caractérisée pour retenir la présomption de responsabilité de l'employeur. Depuis une dizaine d'années, la jurisprudence a décidé de rompre avec cette solution qui n'écartait pas la responsabilité personnelle du salarié sur le fondement de l'article 1382 du Code civil.

La Cour de cassation considère désormais que la responsabilité du salarié ne peut être engagée à l'égard des tiers, lorsqu'il a agi sans excéder les limites de sa mission[6]. La qualité de salarié est ainsi devenue, « *en elle-même, une cause d'irresponsabilité civile dès lors qu'il n'a pas excédé ses fonctions* »[7]. Autrement dit, l'employeur ne peut s'exonérer de sa responsabilité que si son préposé a agi hors des fonctions auxquelles il est employé, sans autorisation, et à des fins étrangères à ses attributions. Le dirigeant doit en conséquence démontrer que son salarié est l'auteur d'un « abus de fonctions ».

---

[1] Tiers ou cocontractants.
[2] Désigné comme le commettant par l'article 1384 al. 5 du Code civil.
[3] Article L. 121-1 Code pénal : « *Nul n'est responsable pénalement que de son propre fait* ».
[4] Article L 263-2-1 et R 261-3 Code du travail.
[5] 5 arrêts de la Cour de cassation, ch. crim., 11 mars 1993, Bull. crim., n° 112.
[6] Sur le fondement de l'article 1384 alinéa 5 du Code civil : Cour de cassation, ch. com., *Société Rochas c/ Société Valières*, 12 octobre 1993, R.T.D. civ., 1994, p. 111, obs. Jourdain. Cour de cassation, Ass. plén., *Costedoat*, 25 février 2000, J.C.P., II, 10295, conclusions Kessous, note Billiau.
[7] (J.) Lasserre-Capdeville, *L'appréciation du rapport d'autorité en matière de responsabilité du fait d'autrui*, R.R.J., n°2, 2005, pp.685-705.

Or, la preuve de cet abus est délicate à apporter. En effet, la jurisprudence française considère que le salarié agit dans le cadre de ses fonctions dès lors que le délit se réalise durant son temps de travail et avec les moyens mis à disposition par son employeur[8].

Sur le fondement de l'article 1384 alinéa 5 du Code civil, qui rend le commettant civilement responsable des fautes commises par son préposé, la Cour d'appel d'Aix en Provence[9] a ainsi confirmé la condamnation d'un employeur pour avoir mis à disposition d'un salarié les moyens techniques nécessaires à la mise en ligne d'un site internet satirique dénigrant une société tierce.

En l'espèce, la Cour a estimé que le salarié a agi dans le cadre de ses fonctions en tant que « *technicien test (…), dont l'activité est la construction d'équipements et de systèmes de télécommunication (…), et dans lesquelles l'usage d'un ordinateur, et d'internet, doit être quotidienne* ».

Les juges ont ensuite relevé que ses actes ont été réalisés avec l'autorisation de son employeur en se fondant sur une note de service du directeur des ressources humaines. Celle-ci autorisait les salariés à utiliser les équipements informatiques mis à leur disposition pour consulter d'autres sites que ceux présentant un intérêt en relation directe avec leur activité au sein de la société, « *dès lors que ces utilisations demeurent raisonnables, (…) et respectent les dispositions légales régissant ce type de communication et les règles internes de la société, l'accès aux sites à caractère explicitement sexuel et contrevenant aux valeurs de la société Lucent Technologies étant prohibé »*[10].

Enfin, la Cour a considéré qu'il n'a pas agi à des fins étrangères à ses attributions, puisque selon la note précitée, les salariés étaient également autorisés à disposer d'un accès internet en dehors de leurs heures de travail.

L'analyse de la Cour d'appel sur la portée de cette note de service, qui fonde son argumentation sur la coïncidence de l'acte litigieux avec la mission du salarié, n'emporte pas notre totale adhésion. Cette note a été strictement interprétée par la Cour à défaut d'interdiction spécifique quant à l'éventuelle réalisation de sites internet ou de publications d'informations en ligne. Or, à notre sens, l'interdiction de consulter des pages internet contraires aux lois et à l'image de l'entreprise, prohibait *de facto* la réalisation d'un tel site qui inclut nécessairement sa consultation.

Dès lors, pour se prémunir des agissements illicites de leurs salariés, les entreprises pourraient être tentées d'interdire dans leurs chartes internet ou règlements intérieurs toute utilisation des moyens de communication modernes à des fins personnelles. Cependant, cette interdiction absolue est sans effet juridique depuis le célèbre arrêt « Nikon » du 2 octobre 2001 qui rappelle que le salarié a droit à une sphère privée au sein même de l'entreprise (principe de proportionnalité : article L. 120-2 du Code du travail).

En conséquence, il est préférable de prévoir au sein des règlements intérieurs d'entreprise[11] une clause autorisant une utilisation personnelle, ponctuelle et raisonnable des sites internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs, et qui ne met pas en cause l'intérêt ou l'image de l'entreprise. Dans un second temps, le règlement doit préciser de manière exhaustive les comportements interdits au sein de l'entreprise : consulter des sites pédophiles ou pornographiques, télécharger de la musique, des films ou tout autre programme, développer un site internet à partir de son poste de travail, dialoguer sur des tchats ou forums à caractère non professionnel, etc …

---

[8] Cour de cassation, 2ème ch. civ., n° 96-11785, 24 juin 1998.
[9] Cour d'appel d'Aix en Provence, *Lucent Technologies c/ Escota, Lycos France, Nicolas B*, 13 mars 2006, Juriscom.net : <http://www.juriscom.net/jpt/visu.php?ID=807>.
[10] TGI de Marseille, *SA Escota c/ Société Lycos, Société Lucent Technologies et M. Nicolas,* 11 juin 2003, Juriscom.net : <http://www.juriscom.net/jpt/visu.php?ID=273>.
[11] Incorporer la charte internet dans le règlement intérieur de l'entreprise présente l'avantage que celui-ci s'impose à l'ensemble des salariés, sans avenant au contrat de travail et sans devoir recueillir la signature individuelle de chaque employé.

La détermination de ces règles d'utilisation des outils de communication de l'entreprise doit également s'accompagner de la mise en place de systèmes de surveillance et d'archivage des flux entrants et sortants de données dans le respect des droits des salariés (avis des instances représentatives du personnel, information des salariés, respect de la vie privée). Ces dispositifs de contrôle ont l'avantage de limiter les agissements des salariés susceptibles d'engager la responsabilité civile et pénale du chef d'entreprise. En effet, une bonne communication interne sur leurs fonctionnements[12] dissuadera toute utilisation tendancieuse des outils informatiques de l'entreprise, tout en permettant de constater, stopper et sanctionner les éventuels abus.

D'ailleurs, ces mesures de sécurité peuvent s'imposer au chef d'entreprise en sa qualité de responsable de traitement de données personnelles[13]. Au regard de la loi Informatique et Libertés, ce dernier est effectivement tenu de prendre toutes « *précautions utiles* » pour préserver, compte tenu de l'état de l'art et des coûts liés à leur mise en oeuvre, un niveau de sécurité approprié aux données qu'il traite[14]. Le « bon professionnel »[15] doit en conséquence mettre en place les moyens humains, financiers, techniques et organisationnels nécessaires à la sécurité de son système d'information en fonction de ses activités.

Dès lors se pose la question de la nature des « *précautions utiles* » à mettre en œuvre.

L'authentification des utilisateurs par un mot de passe individuel[16], les sauvegardes sur des supports amovibles, les *firewall* et les antivirus sont les mesures de sécurité standard obligatoires pour tout système informatique ouvert sur internet. Les fichiers de journalisation des connexions[17] constituent, quant à eux, une mesure de sécurité généralement préconisée par la CNIL[18], dont le défaut de mise en œuvre ne devrait pas être un motif de sanction pour les traitements courants[19]. En revanche, lorsque des applications en réseau concernent des données sensibles (santé) ou des fichiers de police et de gendarmerie, des mesures complémentaires s'imposent aux responsables des traitements, dont la journalisation et le chiffrement des données transférées via internet[20].

Enfin, la CNIL estime qu'une durée de conservation de six mois des données de connexion et des messageries électroniques devrait être suffisante, dans la plupart des cas, pour dissuader tout usage abusif des outils de communication de l'entreprise. Dans le respect des principes de finalité et de proportionnalité, le responsable des traitements peut envisager une durée supérieure. Par exemple, la politique de gestion des traces d'utilisation des moyens informatiques et des services réseau du CNRS prévoit une durée de conservation de un an[21].

---

[12] Dispositifs de filtrage des sites non autorisés associés au *firewall*, contrôle *a posteriori* des données de connexion internet (avec ou sans contrôle nominatif individualisé), contrôle et archivage des courriers électroniques (avec ou sans contrôle individuel poste par poste), fichiers de journalisation des connexions (avec ou sans contrôle de l'activité des utilisateurs).

[13] C'est-à-dire la personne qui détermine les finalités et les moyens des traitements de données à caractère personnel (article 3-I. de la loi Informatique et Libertés).

[14] Article 34 de la loi Informatique et Libertés du 6 janvier 1978 et article 17 de la directive du 24 octobre 1995.

[15] La jurisprudence applique la notion de « *bon père de famille* » (article 1137 du Code civil) pour apprécier la responsabilité du chef d'entreprise en matière de sécurité informatique.

[16] Recommandation de la CNIL : « *le mot de passe choisi doit, si possible, être alphanumérique, d'une longueur de 6 caractères au moins, pas trop courant (évitez initiales, nom, prénom, etc.), changé périodiquement et conservé confidentiellement* ». « Un impératif : La sécurité » (Cnil.fr, <http://www.cnil.fr/index.php?id=1059>).

[17] Enregistrement à des fins de contrôle ou de reconstitution, de tout ou partie des activités effectuées sur un système ou sur une application informatique.

[18] Rapport de la CNIL du 5 février 2002 sur la cybersurveillance et Guide pratique pour les employeurs, octobre, 2005. Les traitements soumis à déclaration ou autorisation auprès de la CNIL doivent, le cas échéant, remplir une annexe « sécurité » précisant notamment les informations journalisées.

[19] Fichiers fournisseurs, salariés, clients ou prospects.

[20] Annexe sur les sécurités (Cnil.fr, <http://www.cnil.fr/fileadmin/documents/declarer/mode_d-emploi/annexes/Annexe-securites.rtf>), « Un impératif : La sécurité » (Cnil.fr, <http://www.cnil.fr/index.php?id=1059>) et recommandation pour les applications en réseau (Cnil.fr, <http://www.cnil.fr/index.php?id=1321>).

[21] B. Perrot, *Politique de gestion des traces d'utilisation des moyens informatiques et des services réseau au CNRS*, Informatique.math.univ-rennes1.fr, 19/01/2005, <http://informatique.math.univ-rennes1.fr/SPIPinfo/article.php3?id_article=37>.

Toutefois, malgré ces recommandations et prescriptions légales, une incertitude a persisté concernant l'étendue de l'obligation de conservation des données de connexion des salariés.

Un arrêt de la Cour d'appel de Paris du 4 février 2005[22] a en effet qualifié une entreprise assurant une connexion internet à son personnel, de fournisseurs d'accès internet[23] (FAI). Sur ce fondement, ces entreprises seraient dès lors tenues de « *conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu (…)* »[24], sans avoir une obligation d'identification proprement dite. A défaut, elles risqueraient d'engager leur responsabilité pénale[25].

Aujourd'hui, cette jurisprudence peut être écartée à la lecture de la nouvelle définition des opérateurs de communications électroniques de la loi anti-terroriste[26]. En effet, depuis le 23 janvier dernier, on entend par FAI toute personne offrant au public une connexion internet, y compris à titre accessoire ou gratuit[27]. Sont donc concernés, outre les FAI professionnels, les cybercafés, les *hotspots*, les hôtels et restaurants, et vraisemblablement les administrations, universités et bibliothèques offrant un accès internet au public. En revanche, les entreprises et organismes publics limitant ce service à leurs seuls salariés ou agents sont dorénavant exclus, puisque la notion de « public » suppose une mise à disposition à un ensemble d'individus indifférenciés. A titre d'exemple, concernant l'accès à un forum de discussion en ligne, le Tribunal de grande instance de Paris avait jugé en ce sens que le caractère non public du service « *suppose une sélection fondée sur un choix positif des usagers qui permette d'assurer leur nombre restreint et leur communauté d'intérêt* »[28].

En conclusion, la responsabilité civile et pénale d'un dirigeant pourra être engagée du fait des agissements de ses salariés ou de son imprudence, dès lors qu'il n'a pas mis en oeuvre les mesures de sécurité adéquates (logicielle, organisationnelle et juridique) pour protéger son système d'information contre des atteintes intérieures ou extérieures. En cas de préjudice, il devra de surcroît apporter la preuve de l'application effective de ces mesures, notamment par une sensibilisation et une formation de son personnel. A défaut de respecter cette obligation de moyen renforcée, sa police d'assurance risque de ne pas couvrir les conséquences pécuniaires de sa responsabilité.

N. S et L. M.

[22] Cour d'appel de Paris, *SA BNP Paribas c/ Société World Press Online*, 4 février 2005.
[23] L'affaire a été jugée sous l'ancien article 43-7 de la loi du 1er août 2000, abrogé par la loi pour la confiance dans l'économie numérique du 21 juin 2004.
[24] Article 6.II de la loi pour la confiance dans l'économie numérique du 21 juin 2004. Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques.
[25] Un an d'emprisonnement et de 75 000 € d'amende : article 6.VI.-1. de la loi pour la confiance dans l'économie numérique du 21 juin 2004.
[26] Loi n°2006-64 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers du 23 janvier 2006.
[27] Nouvel alinéa 2 de l'article L. 34-1 I CPCE, « *les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article* ».
[28] TGI de Paris, *Monsieur Hubert M.-V. c/ Société Edition La Découverte et Société Vivendi Universal Publishing Services*, 5 juillet 2002.