Florilège autour de la loi HADOPI et de ses conséquences pour les entreprises

« On me dit "est-ce que vous êtes prêts à un Hadopi 3 ?" Bien sûr que j'y suis prêt. [...] Je prends d'ailleurs ma part de l'erreur [...]. L'intuition que j'avais, c'est qu'on ne pouvait pas abandonner les créateurs. Peut-être que la maladresse a été de donner le sentiment que vous étiez attaqués. »

Nicolas Sarkozy, 27 avril 2011

À l'occasion de l'installation du Conseil national du numérique.

EMMANUEL JOUFFIN
Docteur en droit

FRANÇOIS COUPEZ
Avocat associé, Société d'avocats Caprioli & Associés

La loi HADOPI, première du nom[1], emportait création d'une autorité administrative indépendante dénommée Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI). La mission première de cette autorité est déterminée par l'article 5 de la loi, à savoir la protection des œuvres et objets auxquels est attaché un droit d'auteur ou un droit voisin « *à l'égard des atteintes à ces droits commises sur les réseaux de communications électroniques utilisés pour la fourniture de services de communication au public en ligne* ».

Réécrivant l'obligation de surveillance de son accès à l'Internet contre l'utilisation de celui-ci par un tiers pour la diffusion d'une œuvre auprès du public sans l'accord de ses ayants droit, introduite par la loi DADVSI du 1er août 2006[2] mais non sanctionnée à l'époque[3], cette première loi HADOPI instaurait en outre une sanction administrative punissant spécifiquement le défaut de surveillance.

En particulier, la première loi HADOPI prévoyait la possibilité pour la Commission de protection des droits de la Haute autorité d'ordonner la coupure de l'accès à l'Internet des personnes ayant réitéré cette infraction de défaut de surveillance, voire de proposer des transactions à l'abonné qui s'engageait « *à ne pas réitérer le manquement constaté [...] ou à prévenir son renouvellement* »[4].

Cette loi, partiellement censurée par le Conseil constitutionnel[5] sous le visa des articles 9 et 11 de la Déclaration des droits de l'homme de 1789, s'est ainsi trouvée amputée de toute la partie relative aux sanctions, réduisant à néant son efficacité. Elle a donc donné lieu à un second volet législatif, la loi HADOPI 2, dont l'objet est de définir le cadre répressif des atteintes au droit d'auteur sur le réseau Internet tout en plaçant le juge pénal au centre du dispositif[6].

Sur un plan plus sociologique, le lecteur extérieur à la matière pourrait penser que l'application des textes relatifs à la HADOPI est, comme toujours, susceptible de plusieurs degrés d'empressement de la part du gouvernement. Il convient de l'éclairer particulièrement sur ce point : s'il fallait un mètre étalon de la volonté du gouvernement de faire appliquer ces textes dans toute leur (dé?)mesure, il suffirait de souligner que les dispositions propres à la répression du piratage figurant dans ces deux textes, dont le plus vieux date de moins de deux ans, ont vu au total pas moins de quatorze (!) décrets d'application signés entre le 21 juillet 2009 (5 semaines après la promulgation de la première loi) et le 21 avril 2011[7].

1. Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur Internet.
2. Loi relative au droit d'auteur et aux droits voisins dans la société de l'information (loi DADVSI) transposant en droit interne de la directive européenne 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.
3. Ancien art. L. 335-12 du CPI.
4. Projet d'art. L. 331-27 et L. 331-28 issus du projet HADOPI 1 (et censurés par la suite par le Conseil Constitutionnel).
5. Conseil constitutionnel, décision n° 2009-580 du 10 juin 2009.
6. Pour une étude générale de la question, voir C. Geiger : « "HADOPI", ou quand la répression devient pédagogique – Une analyse critique du dispositif juridique de lutte contre le téléchargement sur les réseaux "de pair à pair" », D. 2011. 773.
7. Décret n° 2009-887 du 21 juillet 2009 pris pour l'application de l'article L. 331-

Par ailleurs, à la suite d'une déclaration en directe du président de la République du 27 avril 2011 (lors de l'installation du Conseil national du numérique) qui pouvait prêter à confusion, un communiqué de l'Elysée du même jour a bien vite recadré les choses, affirmant un soutien fort à la législation adoptée : « *Ni le bien-fondé de l'action de l'Hadopi, ni la nécessité d'une lutte déterminée contre le piratage, n'ont donc été mis en doute par le président de la République [...] la défense du droit d'auteur constituait [...], aujourd'hui comme hier, un impératif catégorique [...] Au moment où l'action de l'Hadopi, six mois après le commencement de son activité, porte ses premiers fruits et où ce modèle novateur suscite dans le monde entier un intérêt croissant, le président de la République tient à réaffirmer son plein et entier soutien à l'Hadopi et souhaite que l'action de cette autorité indépendante puisse poursuivre son déploiement sur une grande échelle* ».

Au titre de cette loi HADOPI 2, pourront désormais être sanctionnés, aussi bien le contrefacteur auteur des téléchargements illicites, que le titulaire de l'abonnement Internet. Pour une entreprise, le risque d'exposition à une suspension de son abonnement est directement proportionnel au nombre de collaborateurs connectés. Les questions sont toutefois celles de l'occurrence et de l'acuité de ce risque, sachant que celui-ci ne doit pas être minimisé.

La loi du 28 octobre 2009 s'attaque aux téléchargements illégaux (entendons par ces termes les téléchargements portant atteinte aux droits d'auteurs ou aux droits voisins) sur deux fronts.

Dans le cadre de cette étude, et pour appréhender les conséquences pratiques de l'application de la loi du 28 octobre 2009, il convient de se concentrer sur les hypothèses où le pirate/contrefacteur aurait opéré la reproduction ou la communication d'objets protégés par les droits d'auteur ou les droits voisins en utilisant des ressources informatiques appartenant à l'employeur. Qu'en est-il alors de la physionomie de cette contrefaçon (I.) ? L'employeur peut-il encourir une suspension de son abonnement à Internet (II.) ? Peut-il enfin, ne serait-ce que pour limiter les risques, encadrer drastiquement, voire interdire, l'usage privé du salarié de son système d'information (III.) ?

I. HADOPI II ET LA CONTREFAÇON

A. Contrefaçon et... contrefaçon

La loi n'innove pas en ce que le délit de contrefaçon trouvera à s'appliquer au travers d'un renvoi exprès aux articles L. 335-2 à L. 335-4 du Code de la propriété intellectuelle (CPI) afin de préciser que ladite contrefaçon est « *commise au moyen d'un service de communication au public en ligne* » (article L. 335-7 du CPI). Ce délit, aux termes de l'article L. 335-2 du CPI, est sanctionné par une peine d'emprisonnement d'une durée maximale de trois ans et une amende de 300 000 euros.

On ne s'étendra pas sur l'opportunité d'un recours à une peine d'une telle ampleur en matière de téléchargements, certes illégaux, mais qui peuvent n'être que de dimension « *domestique* »[8]. L'on sait, depuis Beccaria, que la peine doit être proportionnée à la faute commise, principe énoncé par le Conseil Constitutionnel dans une décision n° 86-215 DC du 3 septembre 1986 (le Conseil avait en l'occurrence estimé qu'il n'y avait pas de « disproportion manifeste »)[9]. Ce principe est également affirmé au travers du principe de « nécessité ».

À l'occasion d'une décision n° 80-127 DC du 20 janvier 1981 relative à la loi « *sécurité-liberté* », le Conseil Constitutionnel avait en effet rappelé « *qu'il ne lui appartient pas de substituer sa propre appréciation à celle du législateur en ce qui concerne la nécessité des peines attachées aux infractions définies par celui-ci* », mais qu'il lui appartient en revanche de censurer « *les dispositions législatives prévoyant des peines manifestement disproportionnées par rapport aux faits reprochés* ».

À cet égard, on soulignera que la loi DADVSI du 1er août 2006 avait proposé une sanction contraventionnelle des téléchargements illégaux de pair à pair (dits P2P), téléchargements qui sont directement concernés par les lois HADOPI, comme l'ont montré les débats parlementai-

18 du Code de la propriété intellectuelle (*JO* du 23 juill., p. 12308) ; Décret du 23 décembre 2009 portant nomination des membres du collège et de la Commission de protection des droits de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (JO du 26 déc., p. 22372) ; Décret n° 2009-1773 du 29 décembre 2009 relatif à l'organisation de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (JO du 31 déc., p. 23348) ; Décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du Code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur Internet » (*JO* du 7 mars, p. 4680) ; Décret n° 2010-695 du 25 juin 2010 instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique sur Internet (**JO** du 26 juin, p. 11536) ; Décret n° 2010-872 du 26 juillet 2010 relatif à la procédure devant la Commission de protection des droits de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (*JO* du 27 juill., p. 13874) ; Décret n° 2010-1057 du 3 septembre 2010 modifiant le décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du Code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur Internet » (*JO* du 5 sept. 2010, p. 16268) ; Décret n° 2010-1202 du 12 octobre 2010 modifiant l'article R. 331-37 du Code de la propriété intellectuelle (*JO* du 13 oct., p. 18389) ; Décret n° 2010-1267 du 25 octobre 2010 relatif à la « Carte musique » (*JO* du 26 oct., p. 19205) ; Décret n° 2010-1366 du 10 novembre 2010 relatif à la labellisation des offres de services de communication au public en ligne et à la régulation des mesures techniques de protection et d'identification des œuvres et objets protégés par le droit d'auteur (*JO* du 13 nov., p. 20216) ; Décret n° 2010-1630 du 23 décembre 2010 relatif à la procédure d'évaluation et de labellisation des moyens de sécurisation destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne (*JO* du 26 déc. 2010, p. 22739) ; Décret n° 2011-126 du 28 janvier 2011 relatif aux conditions de rémunération du président de la Commission prévue à l'article L. 132-44 du Code de la propriété intellectuelle (*JO* du 30 janv. 2011, p. 1940) ; Décret n° 2011-264 du 11 mars 2011 modifiant le décret n° 2010-236 du 5 mars 2010 relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du Code de la propriété intellectuelle dénommé « Système de gestion des mesures pour la protection des œuvres sur Internet » (*JO* du 13 mars 2011, p. 4561) ; Décret n° 2011-386 du 11 avril 2011 relatif aux indicateurs de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (*JO* du 13 avril 2011, p. 6516). Et encore cette liste n'intègre-t-elle pas la liste des décrets des nominations ou de détachement de ses membres, ni les divers arrêtés d'application.

8. E. Dreyer, « Pour une contraventionnalisation des échanges illégaux de pair à pair », RSC 2007. 57. Pour une approche objective en matière de sanctions pénales : M. Vivant et C. Geiger, *Propr. intell.* 2010, n° 35, p. 747. L. Marino, « La Loi du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur Internet (dite HADOPI 2) », D. 2010. 161. L'auteur évoque la contrefaçon comme « *un délit approprié à la gravité d'une délinquance professionnelle et lucrative* ».

9. Plus récemment, décision n° 96-377 DC du 16 juillet 1996, le Conseil constitutionnel a considéré que le législateur avait entaché son appréciation d'une disproportion manifeste en insérant dans la liste des infractions susceptibles de constituer des actes de terrorisme l'article 21 de l'ordonnance du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France.

res concernant ces deux lois. La mise en place d'une telle sanction avait été censurée par le Conseil constitutionnel pour violation du principe d'égalité devant la loi pénale. La loi incriminait le recours aux logiciels d'échanges de pair à pair, instaurant une distinction selon que les contrefacteurs employaient ou non un tel logiciel, distinction contraire au principe d'égalité[10]. La loi HADOPI 2 n'a pas réitéré cette erreur et, désormais, toutes les technologies permettant la reproduction ou la communication d'objets protégés par les droits d'auteur ou les droits voisins sont concernées. Cette neutralité technologique devrait conduire à englober le streaming[11], qui permet de visionner un film ou d'écouter de la musique sans pour autant télécharger, dans le périmètre de la loi HADOPI.

Dans l'hypothèse considérée de reproduction ou de communication illicite d'œuvres protégées grâce aux moyens informatiques de l'employeur, il n'y a donc rien, en réalité, de différent par rapport aux hypothèses déjà classiques où la responsabilité de l'employeur est mise en cause du fait d'un acte de contrefaçon commis par un de ses salariés.

B. Le délit de contrefaçon et la (très éventuelle) mise en cause de la responsabilité de l'employeur

La recherche de la responsabilité pénale de l'employeur suppose qu'à l'élément légal (la qualification de l'infraction prévue par le texte) soit associé un élément moral, c'est-à-dire la volonté spécifique de commettre l'infraction. Or, en l'occurrence, si l'on pense à la qualification de complicité de contrefaçon pour désigner le fait que les serveurs informatiques ou la connexion à l'Internet soient utilisés pour réaliser les reproductions illicites, l'on bute assez facilement sur la raison pour laquelle ces outils professionnels ont été mis à disposition du salarié.

Si l'on excepte l'hypothèse, fort improbable, où l'employeur aura demandé à son salarié de procéder au téléchargement en connaissance de cause (sa responsabilité pénale ne faisant alors pas débat), l'on se retrouve rapidement en présence de situations où l'utilisateur a utilisé les moyens mis à sa disposition à des fins étrangères aux volontés originelles de l'employeur, surtout si ce dernier a spécifiquement prévu les dispositions adéquates dans son règlement intérieur (et donc en pratique sa charte d'utilisation des ressources informatiques) réprouvant un tel usage. Celui-ci n'ayant donc pas eu la volonté de participer à l'infraction commise par son salarié. Or, cette intention doit être antérieure ou concomitante à la réalisation de l'infraction pour qualifier la conscience de l'aide ainsi apportée à une infraction.

Dès lors, le risque pour l'employeur de voir sa responsabilité pénale mise en cause est donc négligeable, et indépendamment des débats portant sur la qualification du délit de contrefaçon en lui-même comme délit intentionnel ou non intentionnel.

C. Mise en cause de la responsabilité civile de l'employeur

À l'inverse, si l'on regarde les règles et interprétations jurisprudentielles concernant la mise en cause de la responsabilité de l'employeur du fait de son salarié, la déconvenue pour l'employeur risque d'être cruelle. En effet, l'article 1384 alinéa 5 du Code civil a fondé la règle selon laquelle l'employeur est responsable en tant que « commettant »[12] de ses « préposés » (salariés), des fautes commises par ceux-ci dans le cadre de leur vie professionnelle (et donc également en raison de leur utilisation d'Internet et des réseaux sociaux notamment depuis leur lieu de travail). Un arrêt de la Cour de cassation du 19 mai 1988[13] a précisé les conditions de mise en cause de la responsabilité de l'employeur, celui-ci devenant responsable des agissements de son salarié à partir du moment où ce dernier trouve, sur son lieu de travail et pendant son temps de travail, les moyens de sa faute et l'occasion de la commettre.

A contrario, l'employeur n'arrivera à s'exonérer que si trois conditions cumulatives sont remplies : « *si son préposé agit hors des fonctions auxquelles il était employé, sans autorisation, et à des fins étrangères à ses attributions* ». Cela a notamment été jugé pour un directeur d'une agence bancaire qui propose à un commerçant, qui n'était pas client de la banque, des placements a priori très rémunérateurs et qui n'étaient pas proposés par la banque : il n'a pas engagé la responsabilité de son employeur[14]. En revanche, un détournement de fonds commis par un agent général d'assurance sur le lieu et pendant son temps de travail, à l'occasion de ses fonctions, et avec le matériel mis à sa disposition a bien entraîné la mise en cause de la responsabilité civile de son employeur[15].

Or, le principe dégagé par la jurisprudence est identique en matière d'usage de l'Internet et des moyens informatique ; cela a notamment été le cas dans un arrêt du 13 mars 2006[16] rendu par la cour d'appel d'Aix en Provence. En l'espèce, un salarié crée, depuis son lieu de travail, une page personnelle dénommée « ESCROCA » dans le but de dénigrer la société d'autoroute Escota. La société Escota a intenté une action non seulement contre l'auteur du site, mais également contre son employeur, la société Lucent Technologies et contre l'hébergeur du site litigieux. Le Tribunal retient la responsabilité de l'auteur du site pour contrefaçon, et écarte la responsabilité de l'hébergeur. En revanche, le Tribunal retient la responsabilité solidaire de

10. Conseil constitutionnel, décision n° 2006-540 DC, 27 juillet 2006, *RTD civ.* 2006. 791, obs. T. Revet.

11. *Streaming* : diffusion en mode continu selon le dictionnaire de l'AFNIC (http://www.afnic.fr/doc/lexique/d#diffusioncontinue). En pratique, le contenu multimédia est interprété immédiatement sans avoir à attendre le téléchargement complet du fichier et sans que, théoriquement, à l'issue de la lecture complète, l'utilisateur ne puisse obtenir une copie intégrale du fichier sur son ordinateur.

12. Article 1384 al. 5 du Code civil : « *Les maîtres et les commettants du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés* ».

13. Cour de cassation, Assemblée plénière du 19 mai 1988, n° 87-82.654 : *Juris-Data* n° 1988-000836 ; *Bull. ass. plén.* 1988, n° 5 ; Defrénois 1988, note J.-L. Aubert ; *RTD civ.* 1989, p. 89, obs. P. Jourdain ; D. 1988, p. 513, note C. Larroumet.

14. Cass. 2e civ., 19 nov. 1998, n° 96-15.983 : *Juris-Data* n° 1998-004353 ; *Bull. civ.* 1998, II, n° 279.

15. Cass. 2e civ., 19 juin 2003, n° 00-22.626 : *Juris-Data* n° 2003-019620 ; *Bull. civ.* 2003, II, n° 202.

16. TGI Marseille, 1re ch. civ., 11 juin 2003, *SA Escota c/ Sté Lycos* : *Juris-Data* n° 2003-252159 confirmé par CA Aix-en-Provence 13 mars 2006, *SA Lucent Technologies c/ SA Escota, SA Lycos France, Nicolas B.* : *Juris-Data* n° 2006-299517 ; *JCP G* 2006, II, 10168, note Cl.-A. Maetz.

la société Lucent Technologies en sa qualité d'employeur de l'auteur du site litigieux.

Il s'est appuyé pour cela sur une note synthétique du directeur des ressources humaines (groupe) de l'entreprise précisant que les salariés peuvent désormais utiliser les équipements informatiques mis à leur disposition et les accès réseaux existants 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, s'effectuent en dehors des heures de travail, et respectent les dispositions légales régissant ce type de communication et les règles internes de la société. La cour d'appel en a déduit que les trois conditions étaient réunies : le salarié « *a agi dans le cadre de ses fonctions, avec l'autorisation de son employeur, qui n'a pas proscrit l'utilisation à des fins personnelles de l'outil informatique qui lui avait été confié et qu'il n'a pas agi à des fins étrangères à ses attributions* ». Par conséquent, la société est solidairement responsable avec son salarié.

De même la cour d'appel de Grenoble a-t-elle décidé le 7 septembre 2009 qu'un employeur devait être reconnu responsable du téléchargement et de l'utilisation illégaux par un de ses employés d'une version contrefaite du module d'un logiciel protégé, objet d'un brevet français et international, logiciel déployé sur quarante-neuf ordinateurs du site[17].

En l'occurrence, si une action civile sur le fondement de la contrefaçon alléguée était entamée contre l'employeur, ce dernier pourrait très facilement être considéré comme responsable, charge à lui de se retourner par la suite contre son salarié. Reste que là encore, les nouvelles règles tirées des lois HADOPI ne modifient pas le principe déjà applicable aux actes de contrefaçons que peuvent commettre les salariés via les outils mis à leur disposition à des fins professionnelles, contrairement aux apports de l'article L. 336-3 du Code de la propriété intellectuelle.

Nous verrons ci-après ce qu'il convient d'en déduire du point de vue de la communication auprès des salariés.

II. LE « PIRATAGE » ENTRAÎNANT LA RESPONSABILITÉ DE L'EMPLOYEUR EN TANT QUE TITULAIRE DE LA CONNEXION À L'INTERNET

A. Principes

Face à l'importance du phénomène du téléchargement que le législateur ne pouvait ignorer, et afin de tenter d'éviter les contentieux de masse en matière de contrefaçon qui risquaient de découler d'une application systématique des règles, le législateur a décidé de contourner le problème en ne s'intéressant pas seulement au responsable direct du téléchargement, mais à celui qui l'a rendu possible en donnant accès à son propre abonnement de connexion à Internet.

Ainsi, l'article L. 336-3 du Code de la propriété intellectuelle reprend le principe déjà mis en place par la loi DADVSI, puis repris par la loi HADOPI 1 laquelle prescrivait que l'abonné avait « *l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits* ». La loi HADOPI 1 avait prévu la possibilité pour la Commission de protection des droits de la Haute autorité d'ordonner la coupure de l'accès à l'Internet des personnes ayant réitéré cette infraction de « *défaut de sécurisation* », suivant la procédure que nous exposerons ci-après. C'est cette sanction, invalidée par le Conseil Constitutionnel dans sa décision n° 2009-580 DC du 10 juin 2009, qui s'est transformée, par la grâce de la loi HADOPI 2, en infraction contraventionnelle pouvant également entraîner la suspension de la connexion, si le titulaire de l'accès à l'Internet ne veille pas à ce que « *cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public* » d'œuvres protégées sans l'autorisation des titulaires des droits.

B. La notion de « négligence caractérisée »

1. Un principe clair : l'abonné doit veiller à ce que son accès ne soit pas utilisé pour commettre un acte de contrefaçon…

Le décret du n° 2010-695 du 25 juin 2010, pris en application de la loi HADOPI 2, incrimine ainsi la « *négligence caractérisée* » commise par le titulaire de l'accès[18], laquelle est objet d'une amende de 5e catégorie (1 500 euros) prévue par l'article R. 335-5 du même code applicable à tout titulaire d'un abonnement qui, sans motif légitime, n'a pas « *mis en place* », ou a « *manqué de diligence dans la mise en œuvre* » d'un moyen de sécurisation de l'utilisation dudit abonnement, et ce, malgré deux avertissements préalables de la HADOPI advenus dans une brève période de temps. Qui plus est, l'art. L. 335-7-1 du Code de la propriété intellectuelle prévoit que le titulaire de l'abonnement pourra être condamné par le juge unique du tribunal de police à une suspension de l'accès à l'Internet d'un mois maximum.

Le texte vise les comportements ayant conduit l'absence d'installation de moyens de sécurisation, ou l'installation de moyens insuffisants, mais également une installation n'ayant pas du tout été mise en œuvre, l'ayant été avec retard ou ne l'ayant pas été de façon satisfaisante. Cette disposition vaut pour les personnes physiques et morales[19]. Dans ce dernier cas, la peine d'amende est donc quintuplée en application de l'article 131-41 du Code pénal, ce qui représente dans le cas présent une amende de 7 500 euros.

Dans le temps, cette négligence caractérisée nécessitera que l'abonné ait reçu « *deux coups de semonce* », ce qui sup-

17. CA Grenoble 7 septembre 2009, n° 07/01984.

18. Article L. 335-7-1 du Code de la propriété intellectuelle.

19. En dépit de nombreux amendements en faveur d'une distinction, lesquels ont tous été rejetés. À titre d'exemple : amendements numéros 79, 507 de Patrick Bloche et 84 de Catherine Lemorton proposés lors de la discussion de la loi « HADOPI 2 » et numéros 127, 199, 297 de Patrick Bloche proposés lors de la discussion sur l'article prévoyant une sanction en cas de manquement à l'obligation de surveillance de la connexion Internet dans la loi « HADOPI 1 ».

pose que les faits étayant la négligence caractérisée se soient produits au moins à deux reprises et aient entraîné à chaque fois un avertissement spécifique, le second étant particulièrement formalisé. Le premier avertissement (« *recommandation* » nous dit le texte) peut être adressé par courrier électronique par la HADOPI « *et par l'intermédiaire de la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne ayant conclu un contrat avec l'abonné* »[20]. Ce premier message comporte également une information au sujet de « *l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3* ».

Si le contrevenant est relaps dans un délai de 6 mois suite au premier avertissement, un second lui est adressé, également par courrier électronique, accompagné cette fois-ci d'une lettre remise contre signature ou tout autre moyen propre à établir la preuve de sa date de présentation[21]. Cette seconde recommandation ouvre un nouveau délai d'un an. Ainsi, l'abonné ne commettra la contravention prévue par l'article L. 335-7-1 du Code de la propriété intellectuelle qu'à la condition de se livrer à de nouveaux manquements dans l'année qui suit la présentation de cette dernière lettre. Le terme de riposte graduée a donc été repris pour désigner le processus de sanction mis en œuvre par les lois HADOPI[22].

En effet, l'alinéa 2 de l'article L. 335-7.1 énonce que « *La négligence caractérisée s'apprécie sur la base des faits commis au plus tard un an après la présentation de la recommandation mentionnée à l'alinéa précédent* ». Or, la recommandation visée est celle qui est remise contre signature, ou tout autre moyen propre à établir la preuve de sa date de présentation, donc la seconde recommandation.

2. ...une mise en œuvre qui l'est moins

La question est celle des moyens de sécurisation qui doivent être installés et employés.

À ce titre, l'article L. 331-26 du Code de la propriété intellectuelle est central. Il confie à la HADOPI le pouvoir d'organiser la mise à disposition de moyens de sécurisation :

– en rendant publiques des spécifications fonctionnelles pertinentes que ces outils doivent présenter ;

– et en établissant la liste des moyens de sécurisation qui auront subis une procédure d'évaluation certifiée (payante) en fonction desdites spécifications. Ils seront alors labellisés[23].

L'entreprise désirant se protéger contre l'éventuelle application de l'infraction de négligence caractérisée dans la sécurité de son accès à Internet, applicable rappelons-le depuis le 27 juin 2010, se tournera alors tout naturellement vers des moyens de sécurisation labellisés par la HADOPI.

Reste qu'en pratique, la chose est impossible, même si certains constructeurs de solutions de sécurité ou de réseaux profitent du phénomène pour vendre des produits « compatibles HADOPI » ou ayant des fonctionnalités listées dans une rubrique « conformité HADOPI ». En effet, la labellisation s'apprécie par rapport à la conformité à des spécifications précises que doit formaliser la HADOPI. Or, la rédaction de celles-ci a donné lieu à une consultation publique qui dure depuis plus d'un an et est toujours en cours fin décembre 2011. Toutefois, une première version, composée de 36 pages, de ce « *Projet de spécifications fonctionnelles des moyens de sécurisation* » (ou SFH pour Spécifications Fonctionnelles HADOPI) a été mise en ligne sur le site de la HADOPI le 20 septembre 2010 [24].

Ce projet visait en grande partie les moyens de sécurisation des particuliers. Or, une nouvelle version, du 31 mars 2011, a été rendue publique par la HADOPI. Cette version a vu sa taille plus que doubler pour s'établir à 77 pages, dont une grande partie, consacrée spécifiquement à la sécurisation des systèmes d'information (SI) des entreprises, s'intitule dorénavant « *Spécifications fonctionnelles des moyens de sécurisation et considérations organisationnelles* »[25]. Le texte précise en effet que les spécifications s'adressent notamment « *aux organismes collectifs : entreprises de toute taille (Grands Groupes, Entreprises avec agences, PME/PMI), administrations collectivités locales, ministères, universités, établissements scolaires, associations, hôpitaux, hôtels, cybercafés, aérogares, hotspots publics, restaurants, etc.* »[26]. Dans ce cadre, le texte énonce d'ailleurs que « *le titulaire de l'accès Internet est le chef d'entreprise ou le chef d'établissement qui peut confier cette responsabilité à sa direction informatique (DSI) ou à un service (interne ou externe) équivalent. Cette Direction désigne en général un Administrateur de la sécurité, quand il n'existe pas de RSSI [...]* »[27].

Surtout, le dernier état du projet de « spécifications fonctionnelles » dépasse largement ce seul cadre en prévoyant maintenant un volet « organisationnel » visant particulièrement ces « organismes collectifs », dont les entreprises. Le texte prévoit ainsi que la problématique du droit d'auteur devrait maintenant être spécifiquement abordée dans leurs chartes, règlements intérieurs et autre PSSI (Politique de sécurité des systèmes d'information) : « *dans les organisations, il est recommandé qu'une charte informatique explicitement mentionne la contrefaçon comme interdite et qu'une session de sensibilisation soit introduite dans le calendrier de l'établissement de façon que les utilisateurs des ressources informatiques soient effectivement prévenus des risques encourus respectivement par le responsable de l'établissement, par le responsable de sécurité et par l'utilisateur, si les ressources informatiques sont utilisées pour capturer illégalement des œuvres. Les utilisateurs de chaque organisme collectif sont informés (et signent une charte) lorsqu'ils accèdent pour la première fois à ces ressources* »[28].

20. Article L. 331-25 1er alinéa du Code de la propriété intellectuelle.
21. Article L. 331-25 alinéa 2 du Code de la propriété intellectuelle.
22. Dans la loi DADVSI, la notion de riposte graduée était utilisée pour désigner une échelle de sanction qui n'était pas graduée temporellement, mais qualitativement, les téléchargements étant considérés – jusqu'à la censure du Conseil constitutionnel déjà mentionnée – comme moins graves qu'une contrefaçon « classique ».
23. La procédure est décrite aux articles R. 331-85 et suivant du Code de la propriété intellectuelle.
24. Disponible sur http://www.hadopi.fr/actualites/agenda/consultation-sur-les-specifications-fonctionnelles-des-moyens-de-securisation.html.
25. Disponible sur http://labs.hadopi.fr/.
26. Spécifications fonctionnelles des moyens de sécurisation et considérations organisationnelles, version du 31 mars 2011, p. 49.
27. *Ibid.*
28. *Ibid.*, p. 52.

Si l'on met en parallèle les règles posées par la loi HADOPI et notamment l'article R. 335-5 du CPI précisant la notion de négligence caractérisée analysée plus haut, il ressort de ce projet de spécifications fonctionnelles du « moyen de sécurisation » que le fait, pour une entreprise, de ne pas avoir mis en place les spécifications organisationnelles décrites (charte, sessions de sensibilisation, etc.) pourrait être considéré par un juge comme le fait de ne pas avoir mis en place ce « moyen de sécurisation »... ou au minimum d'avoir manqué de diligence dans sa mise en œuvre. Ce qui entraînerait nécessairement l'application de l'article R. 335-5 et donc, le cas échéant, les sanctions prévues par ce texte.

Certes, l'article R. 335-5 alinéa premier du Code de la propriété intellectuelle énonce que n'encoure pas de sanction le titulaire de l'abonnement qui peut arguer d'un « *motif légitime* ». Reste que le texte est muet sur ce que peut être un tel motif. Et l'on imagine difficilement, pour une entreprise, que l'absence de rédaction d'une PSSI dans, d'une charte d'utilisation de ses moyens informatiques ou de formations spécifiques de ses collaborateurs puisse s'expliquer par un quelconque « motif légitime », compte tenu des obligations qui pèse sur elle (protection des données concernant ses clients et salariés, obligation de notification des violations de données à caractère personnel imposant un contrôle et une traçabilité accrue en pratique[29], etc.). En tout état de cause, la lecture conjointe de cet article, ainsi que de l'article 121-3 du Code pénal, conduit à penser que seul un cas de force majeure pourrait avoir un effet exonératoire s'agissant d'une amende de 5e catégorie.

Par ailleurs, sachant qu'HADOPI 2 vise, par principe, toutes les formes de partages illégaux de contenus, les termes de l'article L. 336-3 du Code de la propriété intellectuelle étant généraux[30], se pose la question du simple visionnage ou de l'écoute au travers du streaming. Pour la HADOPI, l'affaire semble entendue à la lecture des « *Spécifications fonctionnelles des moyens de sécurisation et considérations organisationnelles* » précitées. Celles-ci prévoient ainsi notamment la mise en place d'un filtrage en temps réel s'intéressant aux types de logiciels, voire au type de protocoles techniques que ceux-ci utilisent (permettant d'aller assez loin dans le contrôle opéré et d'augmenter l'efficacité de celui-ci)[31].

La surveillance étroite, dans une entreprise, de l'usage que les salariés font de l'accès Internet laissé à leur disposition par leur employeur peut s'avérer très délicate, voire impossible selon certains auteurs[32]. Nous verrons *infra* que l'employeur conserve heureusement certaines marges de manœuvre reconnues par la jurisprudence. Ces mesures pourront par exemple être adoptées par la Mairie de Mèze qui a reçu le 4 novembre 2011 une « recommandation » de la HADOPI. En effet, un poste informatique de sa police municipale a été utilisé pour télécharger indûment deux fichiers, soit un film et une chanson, via le logiciel *emule*[33] .

C. Le prononcé de l'amende et coupure de l'accès

1. Le prononcé de l'amende et principes de droit pénal

Tout d'abord, s'agissant d'une contravention, celle-ci est applicable autant de fois que d'infractions constatées et, s'agissant des personnes morales, aux termes de l'article 131-41 du Code pénal, le montant maximum de l'amende est alors égal au quintuple[34] de celui de l'amende encourue par les personnes physiques (soit 7 500 euros au cas d'espèce).

En outre, pour les contraventions de la cinquième catégorie, la peine d'amende peut toujours être remplacée par une ou plusieurs peines prévues à l'article 131-42 du Code pénal dont la confiscation de la chose qui a servi ou était destinée à commettre l'infraction. On n'ose envisager la confiscation d'un serveur dans une entreprise. Si l'article 132-34 dernier alinéa du Code pénal envisage un sursis en pour les personnes morales, ce dernier ne concerne pas la confiscation.

L'auteur de l'infraction ne pourra pas, afin d'assurer sa défense, arguer de l'absence d'élément intentionnel, le texte de l'article 121-3 du Code pénal ne mentionne en effet, comme cause exonératoire que la survenance d'un cas de force majeure, soit au total une situation de faute présumée[35].

Toutefois, reste un élément qui fait débat, à savoir l'élément légal de l'infraction. Le principe est clairement énoncé : « *Nul ne peut être puni pour un crime ou pour un délit dont les éléments ne sont pas définis par la loi, ou pour une contravention dont les éléments ne sont pas définis par le règlement. Nul ne peut être puni d'une peine qui n'est pas prévue par la loi, si l'infraction est un crime ou un délit, ou par le règlement, si l'infraction est une contravention*[36] ».

L'application de ce principe général interdit la poursuite et la répression d'un comportement n'entrant pas dans le champ des prévisions légales ou réglementaires.

La Cour européenne des droits de l'homme dans une affaire *Pessino c/ France*[37] a jugé, s'agissant de l'article 7 de la CEDH : « *Il s'ensuit que la loi doit définir clairement les infractions et les peines qui les répriment. Cette condition se trouve remplie lorsque le justiciable peut savoir, à partir du libellé de la disposition pertinente et au besoin à l'aide de l'interprétation qui en est donnée par les tribunaux, quels actes et omissions engagent sa responsabilité pénale*[38] ».

29. V. notamment art. 34 et 34 bis nouveau de la loi du 6 janvier 1978, dont la violation est réprimée respectivement par les articles 226-17 et 226-17-1 nouveau du Code pénal.
30. Le titulaire de l'accès Internet a l'obligation de veiller à ce que « *cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public* ».
31. V. notamment « *Spécifications fonctionnelles des moyens de sécurisation et considérations organisationnelles* », version du 31 mars 2011, p. 52 : « *Aide à la prévention de téléchargement illégal et de contrefaçon par l'observation en temps réel, sans enregistrement des flux et protocoles qui transitent par l'accès* ».
32. F. Macrez et J. Gossa, « Surveillance et sécurisation : ce que l'Hadopi rate [...] », *RLDI*, juin 2009, n° 1659.
33. http://www.midilibre.fr/2011/12/20/meze-du-piratage-a-la-police-municipale,433267.php.
34. Article 131-38 du Code pénal.
35. J. Pradel, *Principes de droit criminel*, T. 1, 1999, Cujas, p. 135, n° 120. J.-C. Schmidt, « L'élément intentionnel en matière de contravention », *RPDP* 1932.387.
36. Article 111-3 du Code pénal.
37. Requête n° 40403/02 arrêt du 10 octobre 2006.
38. Voir, notamment, *Cantoni c/ France*, arrêt du 15 novembre 1996, Recueil des arrêts et décisions 1996-V, p. 1627, § 29 et *Achour c/ France* [GC], n° 67335/01, § 41, 29 mars 2006.

On trouve une illustration de ce principe dans une décision du 20 février 2001[39], par laquelle la Chambre criminelle a affirmé la nécessité du respect du principe de légalité. En l'occurrence, il s'agissait de l'article 38 alinéa 3 de la loi du 29 juillet 1881 incriminant « *la publication, par tous moyens, de photographies, gravures, dessins, portraits ayant pour objet la reproduction de tout ou partie des circonstances d'un des crimes ou délits* ».

Les Hauts magistrats ont considéré que ce délit n'était pas conforme à l'exigence de précision des infractions au motif que « *sa formulation introduit une vaste marge d'appréciation subjective dans la définition de l'élément légal de l'infraction et ne permet pas à celui qui envisage de procéder à la publication d'être certain qu'elle n'entre pas dans le champ d'application de l'interdit* ». Cette analyse a été par la suite consacrée par le législateur qui a supprimé la disposition en cause.

Le Conseil constitutionnel veille également au respect du principe de légalité des peines et estime que « *le législateur doit définir des infractions en termes suffisamment clairs et précis pour exclure l'arbitraire*[40] ».

Or, au cas d'espèce, un certain flou environne la question, notamment les conditions de délivrance de son label par la HADOPI. En effet, les spécifications fonctionnelles du « moyen de sécurisation » prévu par les textes n'étant pas encore finalisées, aucun outil ne peut être labellisé par cette dernière. Il n'apparaît dès lors pas possible de s'exonérer de l'application de l'article R. 335-5 du CPI.

2. La sanction redoutée : la coupure de l'accès à l'Internet

Hormis la peine d'amende, la sanction tant redoutée prévue par l'article R. 335-5 du CPI risque d'être autrement plus conséquente si la HADOPI a « recommandé » en vain au titulaire de l'accès de le sécuriser (avec le formalisme vu *supra*) : le magistrat se voit en effet reconnaître le pouvoir de condamner la personne physique ou morale n'ayant pas sécurisé son accès « *à la peine complémentaire de suspension de l'accès à un service de communication au public en ligne pour une durée maximale d'un mois* ».

Deux articles du Code de la propriété intellectuelle précisent les modalités de cette coupure. Tout d'abord, l'article L. 335-7-2 apporte un tempérament à la sanction en précisant que, pour fixer la durée de la suspension de l'accès, « *la juridiction prend en compte les circonstances et la gravité de l'infraction ainsi que la personnalité de son auteur, et notamment l'activité professionnelle ou sociale de celui-ci, ainsi que sa situation socio-économique. La durée de la peine prononcée doit concilier la protection des droits de la propriété intellectuelle et le respect du droit de s'exprimer et de communiquer librement, notamment depuis son domicile* ».

L'entreprise, de par les multiples abonnements à l'Internet qu'elle est susceptible d'utiliser dans le cadre de son activité (abonnements pour les *smartphones* et tablettes, abonnements pour des points de connexion ponctuels, points d'accès sans fil pour ses clients et prospects, voire connexion principale à l'Internet) et la multiplicité des potentiels auteurs de téléchargements illicites est *a priori* une cible toute désignée pour un manquement, considéré comme délibéré, à l'obligation de sécurité de ses accès, et donc… à une coupure.

Ce tempérament apparaît donc pour l'heure la seule protection, pour une entreprise, contre une coupure de son ou de ses accès à l'Internet du jour au lendemain. D'autant que le titulaire de l'accès, condamné à la suspension de son accès, se voit interdire de souscrire, comme palliatif, à un autre abonnement pendant cette période, sous peine d'une amende de 3 750 euros, comme le précise l'article L. 335-7-1 du CPI.

Reste que si l'entreprise venait à être condamnée plusieurs dizaines de fois, par exemple, pour des manquements à la sécurisation de ses accès, la réaction du juge saisi d'une nouvelle affaire pourrait être plus véhémente. Il pourrait ainsi considérer qu'une journée ou deux de coupure serait enfin une mesure de nature suffisamment incitative face à un comportement considéré comme négligent à de multiples reprises. L'hypothèse de ces « manquements » répétés est loin d'être absurde, en pratique, pour une entreprise de plusieurs dizaines de milliers de salariés ayant accès à l'Internet dans le cadre de ses activités, sauf à restreindre plus que drastiquement les conditions de cet accès.

3. Conséquences inattendues de la coupure de la ligne Internet

Les discussions parlementaires sur ces lois HADOPI ont été parfois rocambolesques[41] et surtout exempts de véritable analyse technique sur le fond des sujets évoqués. Dès lors, certaines questions restent entières pour le moment et devront être tranchées par les magistrats.

Il en va ainsi d'une question essentielle, surtout pour les entreprises : *quid* des titulaires d'abonnements disposant de plusieurs accès à l'Internet souscrits auprès de prestataires différents ? La sanction de la suspension/coupure d'accès, quand elle est décidée, doit-elle s'appliquer à tous les abonnements ? Ou seulement à celui qui a été à l'origine de la sanction du fait de sa non-sécurisation ?

En effet, l'interdiction de souscrire à un nouvel abonnement pendant la sanction de la suspension d'accès pourrait laisser penser que le but du législateur est d'empêcher, pendant la période de la sanction, tout accès permettant un téléchargement illicite. L'on pourrait donc en déduire, en conséquence, que tous les abonnements du titulaire condamné pourraient être concernés. Dans le cadre d'une entreprise titulaire d'accès « data » pour les *smartphones* et tablettes de leurs salariés et en cas de téléchargements illicites du fait d'un « défaut de sécurisation » réitéré, ce serait donc potentiellement tous les accès à l'Internet de l'entreprise qui risqueraient

39. D. 2001, Jur. 3001, note P. Wachsmann.

40. Cons. Const. 19-20 janvier 1981, *JCP* 1981.II.19701, note Frank ; D. 1982, *Jur.*, p. 441, note A. Dekeuver ; Cons. Const. 5 mai 1998, n° 98-339 DC, *JO* du 12 mai 1998, p. 7092, D. 1999, Jur. 209, note B. Mercuzot.

41. La loi HADOPI 1 avait ainsi été rejetée lors du vote à l'Assemblée nationale le 9 avril 2009 par 21 voix contre 15, les députés socialistes opposés au texte s'étant cachés pour n'apparaître finalement, en supériorité numérique, qu'au moment du vote (affaire dite « des rideaux »).

la suspension… La réponse est donc attendue avec une certaine appréhension…

Par ailleurs, certaines entreprises utilisent un « tuyau » de connexion unique à la fois pour l'accès à l'Internet de leur personnel et à la fois pour la mise en ligne de leurs sites de e-commerce ou de banque en ligne dans le cas d'établissements de crédit. Certes, le législateur a prévu que la coupure de l'accès à l'Internet ne devait pas entraîner la coupure du téléphone ou de la télévision dans le cas des abonnements intégrés dits « *multiple play* » (sans prise en compte des difficultés techniques d'une telle chose). Il convient ainsi de rappeler que la personne sanctionnée se trouve privée de son accès à « *un service de communication au public en ligne* ». Cette notion fait l'objet de l'article 1er § IV, alinéa 4 de la loi n° 2004-575 du 21 juin 2004 dite de confiance dans l'économie numérique. Au sens de ce texte est concernée « *toute transmission, sur demande individuelle, de données numériques n'ayant pas le caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur* ». À cet égard, l'article L. 335-7 alinéa 2 du CPI précise que l'abonnement à la télévision et au téléphone, souscrit par le condamné, accessoirement au service en ligne, continue de fonctionner. La même disposition est prévue pour la téléphonie servie par le fournisseur d'accès à Internet (FAI).

Mais comment établir ce partage dans une la situation ci-dessus décrite, lequel paraît peu réalisable ?

Enfin, qu'il soit permis de poser la question suivante : est-il raisonnable de sanctionner une faute de non-surveillance ayant permis la commission d'un acte de « piratage », alors même que n'a pas été tranchée une question qui apparaît fondamentale, à savoir les échanges sur les réseaux de *pair à pair* sont-ils éligibles à l'exception de copie privée ? Autrement dit, peut-on sanctionner les conséquences d'un piratage qui n'en est peut-être pas un ?

La Chambre criminelle de la Cour de cassation a eu à connaître de cette question, mais n'a pas tranché, se bornant à prononcer une cassation disciplinaire pour défaut de réponse à conclusion[42]. La cour d'appel avait relevé « qu'*aux termes des articles L. 122-3, L. 122-4 et L. 122-5 du code de la propriété intellectuelle, lorsqu'une œuvre a été divulguée, l'auteur ne peut interdire les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* » et que, au cas d'espèce « *le prévenu a déclaré avoir effectué les copies uniquement pour un usage privé et qu'il n'est démontré aucun usage à titre collectif* ».

III. ENCADREMENT DE L'USAGE DES MOYENS INFORMATIQUES MIS À DISPOSITION DU SALARIÉ : LE DROIT À L'USAGE PRIVÉ EXISTE-T-IL DANS L'ENTREPRISE ?

A. L'Internet au travail…

Face à ces exigences toujours plus fortes de sécurisation de ses systèmes d'information, l'entreprise n'est heureusement plus désarmée et s'est vu reconnaître de façon croissante par la jurisprudence la possibilité d'effectuer des contrôles quant à leur utilisation par les salariés.

À partir du moment où elle a posé des règles claires dans son ou ses règlement(s) intérieur(s) par le biais d'une charte d'utilisation des moyens informatiques (ou encore de communications électroniques[43]), la sanction du non-respect de ces règles fondant un certain contrôle de l'employeur apparaît possible, d'autant qu'elle a été validée par la jurisprudence à de multiples reprises.

Certes, le Conseil constitutionnel[44], a énoncé en substance, s'agissant de la loi HADOPI 1, un principe selon lequel les dispositifs de communication en ligne participent à « *la vie démocratique et l'expression des idées et des opinions* » et que la liberté de communication des « *pensées et des opinions est un des droits les plus précieux de l'homme* ». Reste que ce principe n'impose en rien un droit des salariés à se connecter à l'Internet via les moyens mis à disposition par l'employeur à des fins non professionnelles. Ainsi, cette liberté de communication n'est pas totale et ne peut s'exprimer qu'en conformité avec les obligations issues du contrat de travail.

Dans le cadre de cette étude, il convient de distinguer les hypothèses de téléchargement, par le salarié, de contenus illicites au regard du droit d'auteur à partir de ses abonnements propres et sur ses outils informatiques (à son domicile par exemple). En effet, dans ce cadre, un arrêt *Léger* énonce qu'« *en principe, il ne peut être procédé au licenciement d'un salarié pour une cause tirée de sa vie privée…* »[45], un téléchargement dans de telles conditions étant considéré comme relevant de sa vie privée. Pour qu'un employeur décide de sanctionner un salarié s'étant livré à ces actes chez lui et en n'utilisant en rien les moyens de l'employeur (ni pendant son temps de travail), il existe une alternative :

a. Il faudrait que le fait soit considéré comme une faute professionnelle (plutôt réservée aux manquements à la loyauté ou la confidentialité découlant du contrat de travail)…

Ainsi, la Chambre sociale de la Cour de cassation[46], dans un arrêt du 25 février 2003, a retenu la possibilité d'un licenciement disciplinaire pour un fait de vie per-

42. Cass. Crim. 30 mai 2006, D. 2006. 2676, note E. Dreyer, et 2997, obs. P. Sirinelli.

43. L'intitulé précis de tels documents varie suivant les entreprises sans que celui-ci n'altère leur valeur juridique.

44. Conseil constitutionnel 10 juin 2009, n° 2009-580 DC.

45. Cass. Soc 20 novembre 1991, n° 89-44.605.

46. Cass. Soc. 25 février 2003, *Bull. Civ.* V n° 66, p. 62 ; *Dr. soc.* 2003. 625 ; E. Fortis, « Vie personnelle, vie professionnelle », *Dr. soc.* 2004. 44.

sonnelle « *Dès lors que le salarié d'une caisse d'allocations familiales a commis, au préjudice d'une autre caisse à laquelle il était affilié, des faits illicites, à savoir de fausses déclarations pour bénéficier de prestations sociales indues, faits qu'il était chargé de poursuivre dans ses fonctions qui le soumettaient à une obligation particulière de loyauté et de probité, une cour d'appel peut en déduire que ce salarié avait commis une faute grave rendant impossible la poursuite de son contrat de travail pendant la durée du préavis* ».

b. ...ou que ces actes soient considérés comme causant un trouble objectif caractérisé au sein de l'entreprise, ce qui pourrait fonder un licenciement pour motif personnel, le trouble caractérisé étant une alors une cause réelle et sérieuse de licenciement. Dans un arrêt du 16 mars 2004[47] la Chambre sociale de la Cour de cassation énonçait, s'agissant d'un vol commis par un salarié dans un magasin client de l'entreprise, que « *si un fait tiré de la vie personnelle du salarié ne peut constituer une faute, il en est autrement si le comportement de l'intéressé, compte tenu de ses fonctions et de la finalité de l'entreprise a causé un trouble objectif caractérisé au sein de cette dernière* ».

Toute la question est de savoir, hors les cas relevant du trouble évident apporté au fonctionnement de l'entreprise, à partir de quel moment le comportement du salarié doit être considéré comme disciplinairement répréhensible sachant qu'aux yeux de la Chambre mixte de la Cour de cassation[48] « *[...] un trouble objectif dans le fonctionnement de l'entreprise ne permet pas en lui-même de prononcer une sanction disciplinaire à l'encontre de celui par lequel il est survenu* ».

Le comportement du salarié ne doit pas être incompatible avec son contrat de travail, lequel comme tout contrat oblige à ce qui est, « *non seulement exprimé, mais encore à toutes les suites que l'équité, l'usage ou la loi donnent* » à ce contrat.

Ainsi, il a été jugé que le cadre commercial d'une banque, tenu d'une obligation particulière de probité, créait un trouble caractérisé au sein de l'établissement l'employant par sa condamnation pour des délits d'atteinte à la propriété d'autrui[49]. En revanche, l'envoi par maladresse de textes à caractère pornographiques à l'ensemble des salariés n'est pas constitutif d'un fait incompatible avec le fonctionnement de l'entreprise[50]. En l'espèce, une telle qualification pourrait par exemple être appliquée si le délinquant est un cadre supérieur d'un producteur de musique luttant contre le piratage et que la sanction par la HADOPI et par le juge est médiatisée.

Mais *quid* d'un cadre de banque qui se livrerait à des téléchargements illégaux sur ses propres outils personnels et à partir de sa connexion privée à l'Internet ? L'atteinte portée à la protection des œuvres auxquels est attaché un droit d'auteur ou un droit voisin au travers de téléchargements illégaux sur les réseaux de communications électroniques semble constituer une atteinte au droit de propriété laquelle, si l'on en croit la décision du 25 janvier 2006, est incompatible avec la particulière probité attendue de la part d'un cadre de banque. Mais *quid* du personnel non-cadre et *quid*, de manière plus large, du personnel non bancaire ?

En tout état de cause, on peut penser qu'il y aura, *a minima*, une violation des dispositions de la charte d'utilisation des moyens informatiques, violation qui permettrait, à elle seule, d'entamer une procédure disciplinaire.

En revanche, en ce qui concerne l'utilisation par le salarié des outils et connexions informatiques appartenant à l'employeur pour téléchargement des contenus considérés comme illicites par le droit d'auteur, la situation peut être vue de façon différente.

En effet si l'arrêt *Nikon* a énoncé que « *le salarié a droit au respect de sa vie privée, y compris au temps et au lieu de travail* »[51], cette liberté n'est toutefois pas absolue et surtout doit être mise en cohérence avec un autre attendu, moins étudié, de ce même arrêt qui précise que cela est vrai « *et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* ». Ainsi, loin de reconnaître un « droit » du salarié à un usage privé du système d'information de l'employeur, la Cour de cassation a au contraire implicitement reconnu que l'employeur pouvait interdire tout usage privé. Simplement, cette interdiction ne lui permettrait pas en l'espèce de prendre connaissance du contenu de courriers électroniques considérés comme ayant une nature privée et donc protégés par le secret des correspondances.

Même si la CNIL énonce quant à elle depuis 2002 qu'« *une interdiction générale et absolue de toute utilisation d'Internet à des fins autres que professionnelles ne paraît pas réaliste dans une société de l'information et de la communication* »[52], la Cour de cassation n'a jamais validé ou reconnu explicitement cette position.

B. ...et son contrôle

En ce qui concerne le contrôle des activités du salarié, la Chambre sociale de la Cour de cassation a rappelé dans son arrêt du 14 mars 2000, concernant un salarié trader chargé de recevoir et de transmettre par téléphone des ordres d'achat en bourse, que « *l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, l'emploi de procédé clandestin de surveillance étant toutefois exclu* »[53].

47. Cass. Soc. 16 mars 2004, n° 01-45.062.

48. Cass. mixte 18 mai 2007, n° 05-40.803, *Bull. Ch. mixte* n° 3. Il s'agissait de la réception par un salarié d'une revue pornographique qu'il se faisait adresser sur le lieu de son travail.

49. Cass. Soc. 25 janvier 2006, n° 04-44918.

50. Cass. Soc. 21 déc. 2006, n° 05-42.986.

51. Cf. notamment l'arrêt *Nikon* du 2 octobre 2001 ; *Bull. Civ.* V, n° 291 ; *RTD civ.* 2002. 72, obs J. Hauser D. 2001. *Jur.* 3138, note Gauthier ; D. 2002. *Somm.* 2296, obs. Caron ; *JCP* G 2002, I, n° 102, note M. Bourrié-Quenillet et F. Rodhain : *RTD civ.* 2002, p. 72, note J. Hauser ; *RJS* 2001, p. 940, note F. Favennec-Héry ; *Comm. com. électr.* 2001, n° 11, comm. 120, obs. J. Devèze et M. Vivant ; J.-E. Ray, « Courrier privé et courrier personnel », *Dr. soc.* 2001, p. 915 ; P. Alix, « Le contrôle de la messagerie électronique après l'arrêt *Nikon* », *Les cahiers du DRH* 2001, n° 47, p. 2 ; dans le même sens : Cass. Soc. 12 octobre 2004, *Bull.* n° 245. Ces arrêts font suite à des jugements précurseurs, notamment TGI Paris 2 novembre 2000, Expertises 2001, n° 248, p. 190, note X. Furst ; *JCP* E, 2002, n° 36, n° 13, obs. J.-M. Bruguières et M. Vivant ; *Rev. Lamy dr. aff.* 2000, n° 33, n° 2093, obs. L. Costes ; Cons. prud'h. Montbéliard 19 septembre 2000, *Comm. com. électr.*, janvier 2001, p. 14, en annexe à l'article de A. Lepage, « Le secret des correspondances immatérielles dans l'entreprise », chr. n° 2.

52. Rapport présenté par M. Hubert Bouchet, vice-président délégué de la CNIL, partie III : Conclusions, p. 2, adopté par la Commission nationale de l'informatique et des libertés dans sa séance du 5 février 2002.

53. Cass. Soc. 14 mars 2000, *Bull.*, V, n° 101, p. 78 ; *Gazette du Palais*, 28 octobre 2000,

La multiplication des affaires de « cybersurveillance » portées devant elle aidant, la Cour a précisé les modalités de contrôle qu'elle reconnaissant aux employeurs. Compte tenu du volume important des décisions rendues, l'analyse opérée ici sera brève et se concentrera sur les conséquences au regard des exigences des nouvelles lois HADOPI.

Indiquons que, de façon synthétique, la Cour de cassation a opéré une distinction entre courriers électroniques apparaissant comme privés, protégés par le secret des correspondances[54], et les courriers électroniques considérés comme professionnels librement consultables l'employeur hors la présence du salarié[55]. La même distinction a été opérée par la Cour de cassation concernant les fichiers indiqués comme étant « privés » aux conditions d'accès strictes et les autres fichiers, considérés comme professionnels et, partant, librement accessibles par l'employeur[56]. En effet, si les fichiers sont identifiés comme étant personnels, l'employeur ne peut en prendre connaissance que s'il se trouve dans une des trois situations alternatives suivantes : en cas de risque ou d'évènement particulier, si le salarié est présent ou s'il a été dûment appelé[57].

Or, il est très intéressant de noter que la 5e Chambre de la cour d'appel de Versailles a qualifié, pour la première fois, cette notion de « *risque ou d'événement particulier* », permettant la prise de connaissance d'un fichier personnel du salarié hors sa présence dans sa décision sur 31 mars 2011, concernant justement des fichiers multimédias téléchargés via un logiciel P2P. La cour d'appel a ainsi confirmé le licenciement d'un salarié d'une étude d'huissier pour faute grave intervenue en 2007, à la suite de la découverte par l'employeur sur l'ordinateur du salarié du téléchargement illégal de fichiers musicaux via le logiciel de P2P « *e-mule* » qui avait été installé.

Le salarié, à la suite d'un entretien avec son employeur, avait démissionné avant de se rétracter le jour suivant. La cour a considéré que le salarié ne pouvait invoquer l'irrégularité de l'ouverture du fichier identifié comme personnel hors sa présence dès lors que la vérification avait pour but de mettre fin à un téléchargement automatique de données étrangères à l'employeur, mais réalisé à partir de son adresse IP et que cette vérification avait été effectuée à nouveau en sa présence. Cette décision, rendue sous l'empire de la loi ancienne, apporte donc un éclairage bienvenu sur les modalités de contrôle permises à l'employeur à l'heure de l'HADOPI.

Notons également qu'en ce qui concerne l'accès aux sites réalisés à partir de l'infrastructure de l'employeur pendant les heures de travail, la Cour de cassation est là également très claire : l'employeur peut avoir accès à ces informations, hors la présence de l'intéressé et s'en servir pour sanctionner l'utilisateur[58].

En prévoyant une Politique de sécurité des systèmes d'information adaptée, une charte mise à jour au besoin afin de prévoir ces nouveaux impératifs et les règles d'utilisation afférentes, et sous réserve du respect des formalités CNIL nécessaires, celui-ci pourra mettre en œuvre des contrôles stricts et une « chasse » à la fois technique et juridique aux fichiers indûment téléchargés… nouvelles missions qui lui sont dévolues par le législateur, comme nous l'avons vu.

Reste qu'il appartient à l'employeur de rester vigilant au fait qu'une cause réelle et sérieuse pouvant justifier un licenciement est définie par la jurisprudence comme un élément nécessairement objectif, existant et d'une certaine gravité et qui consiste en un manquement du salarié suffisant pour donner lieu à une telle mesure définitive[59] : l'échelle des sanctions appliquée aux manquements d'un salarié devra donc rester proportionnée.

Par ailleurs, en pratique, et afin de respecter les exigences des Tribunaux en matière de recueil de la preuve ou encore de la garantie d'imputabilité des faits au salarié, les PSSI et chartes ne peuvent s'affranchir de procédures écrites claires décrivant les conditions des contrôles réalisés, les rôles de chacun (responsable de la sécurité des systèmes d'information, auditeur, manager, etc.), les modalités de réalisation des interventions techniques, propres à chaque cas spécifique (décès du salarié et accès à ses fichiers, suspicion de fraude, suspicion de transmission d'informations confidentielles, accès aux fichiers en l'absence du salarié, etc.) permettant par la suite de prouver la régularité des opérations effectuées.

Subie, la législation HADOPI soulèvera nombre de problèmes que les organisations se devront de gérer dans l'urgence (comment prévoir la remontée d'information des notifications de l'HADOPI, comment (ré)agir ? Comment contrôler ? Comment sanctionner ?).

Défi certain, mais souvent ignoré, cette législation doit au contraire être intégrée dans les problématiques de sécurité informatique de l'organisation afin qu'une réponse adaptée et globale puisse être apportée. À cet égard, les formations au droit d'auteur que semble requérir la HADOPI pourraient être l'occasion d'une formation plus globale sur les règles de sécurité et de comportements dans l'entreprise à l'heure où la sécurité de l'information dans les structures est confrontée à de bien plus importants dangers (approche non maîtrisée des réseaux sociaux, usages des outils personnels dans l'entreprise[60], etc.). ■

n° 302, p. 34, note L. Bérenguer-Guillon et L. Guignot, *Semaine juridique*, 7 février 2001, n° 6, p. 325, note C. Puigelier.

54. Encore que la radicalité du principe dégagé par l'arrêt Nikon ait été quelque peu estompée par un autre arrêt du 17 juin 2009, qui semble aligner désormais le régime d'accès aux messages privés sur celui des fichiers privés : « *sauf risque ou événement particulier, l'employeur ne peut ouvrir les courriers identifiés par le salarié comme personnel contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé* » (Cass. soc. 17 juin 2009, n° 08-40.274, FS-P+B, *SA Sanofi chimie c/ X. et Y.* : *Juris-Data* n° 2009-048669 ; *Comm. com. électr.* 2009, comm. 106, note É. A. Caprioli ; *JCP* S 2009, 1362, E. Jeansen ; *JCP* G 2009, n° 39, 263, p. 22, S. Maillard).

55. Cass. Soc. 18 octobre 2006, *Bull. civ.* V, n° 308, D. 2006, IR, p. 2753 ; É. A. Caprioli, *Comm. com. électr.* 2007, comm. 15.

56. V. notamment Cass. Soc., 30 mai 2007, n° 05-43102 : *Juris-Data* n° 2007-039426, RDBF 2007, comm. 233, p. 59, comm. É. A. Caprioli.

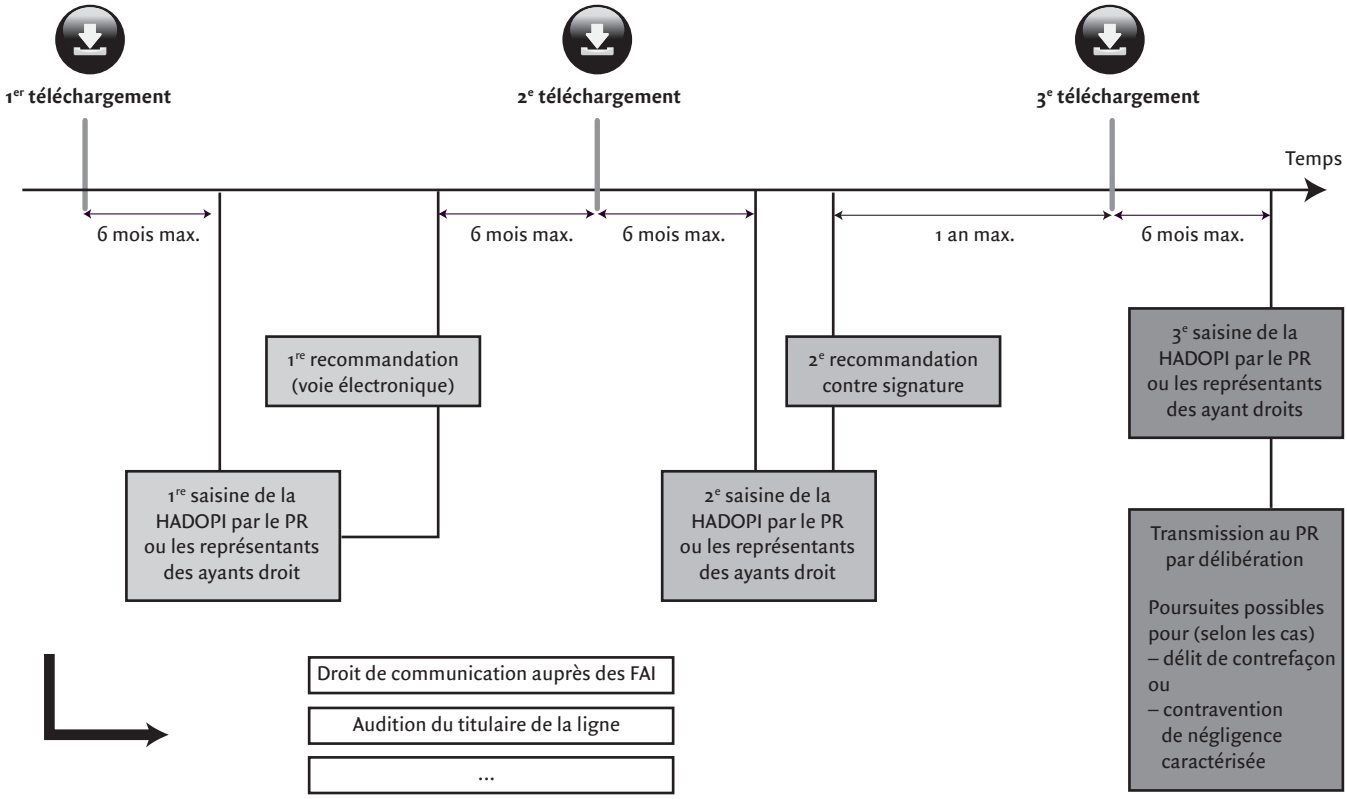
57. Cass. soc. 17 mai 2005, n° 03-40.017, FS-P+B+R+I, *Philippe X. c/ Cathnet-Science* : *Juris-Data* n° 2005- 028449 ; *Bull. civ.* 2005, V, n° 1089 ; *Comm. com. électr.* 2005, comm. 121, note A. Lepage ; *Dr. soc.* 2005, p. 789, note J.-E. Ray.

58. Cass. soc., 9 juillet 2008, n° n° 06-45800, A. Lepage, *Comm. com. électr.* 2008, comm. 128 et É. A. Caprioli, *Comm. com. électr.* 2008, comm. 131.

59. Cass. soc., 29 nov. 1990, n° 87-40.184, P, *Fertray c/ Sté des Éts R Wagner et Cie* : *Juris-Data* n° 1990-003383 ; *Bull. civ.* 1990, V, n° 597 ; *JCP* G 1991, IV, n° 4, p. 33. – Cass. soc. 16 juin 1993, n° 91-45.102, P *Gremillon c/ SA Garon* : *Juris-Data* n° 1993-001208. – Cass. soc. 29 mai 2001, n° 98-46.341 : *Juris-Data* n° 2001-009803 ; *Bull.* civ. 2001, V, n° 183.

60. Ces deux sujets font d'ailleurs l'objet d'une étude par le groupe « Informatique et juridique » du Forum des compétences regroupant les principaux établissements de crédit et entreprises d'assurance de la Place.

Schéma du déroulement de la procédure devant la Commission de protection des droits de la loi HADOPI



Source : Annexe 2 Circulaire du 6 août 2010 relative à la présentation des lois n° 2009-669 du 12 juin 2009, favorisant la diffusion et la protection de la création sur Internet, et n° 2009-1311 du 28 octobre 2009, relative à la protection pénale de la propriété littéraire et artistique sur Internet, ainsi que de leurs décrets d'application : NOR : JUSD1021268C.