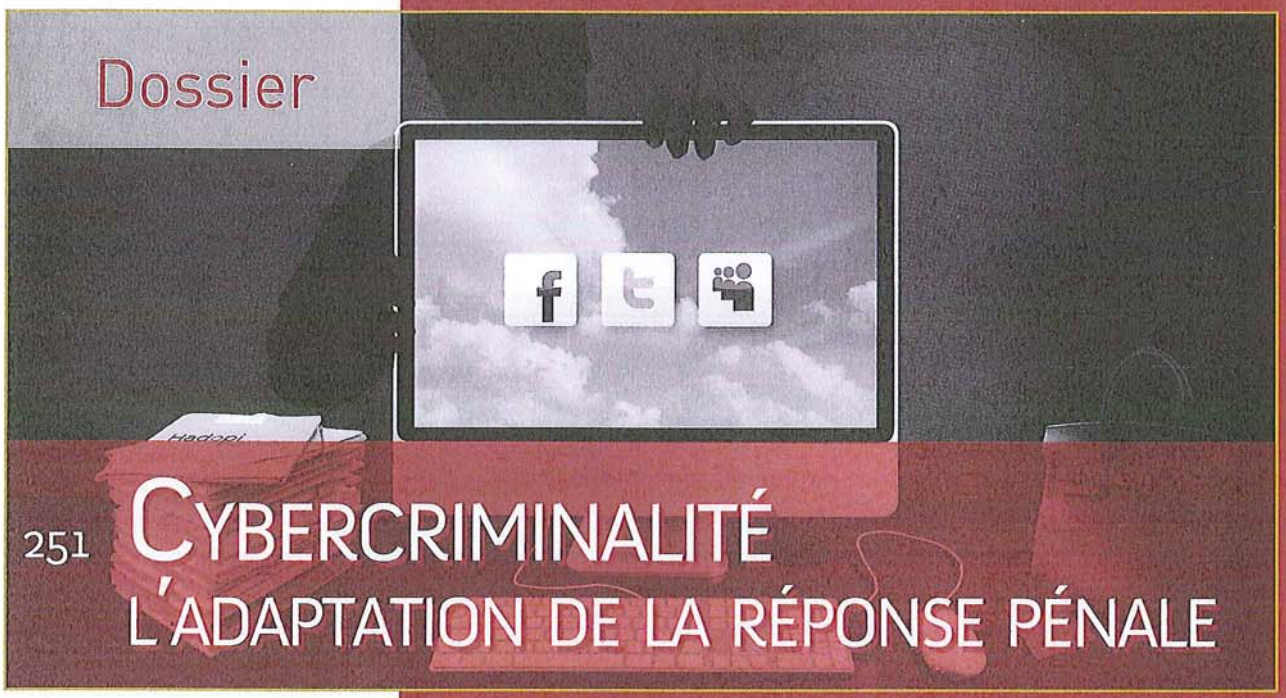
AJ Pénal - mensuel - mai 2012 - pages 241 à 300 - n° 5

AJ Pénal

ACTUALITÉ JURIDIQUE PÉNAL

Dossier



251 CYBERCRIMINALITÉ
L'ADAPTATION DE LA RÉPONSE PÉNALE

272 Le contrôle général des lieux privatifs de liberté : Immersion dans l'ombre de la République
Eric Senna

277 La lutte contre la piraterie maritime
Nouvelles perspectives
Thomas Cassuto

281 Voici venu le temps d'en finir avec la rétention arbitraire des enfants (à propos de l'arrêt *Popov*)
Serge Slama

DALLOZ

ref : 671205

9 782996 712051

Cybercriminalité et réseaux sociaux : la réponse pénale

par Emilie Bailly
et Emmanuel Daoud
Avocats au barreau de Paris

Les réseaux sociaux peuvent être définis comme des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs [1]. Plus de 700 sont recensés dans le monde. Chacun ayant son objectif : partage, discussion, localisation, jeux... Parmi les plus connus il y a évidemment le géant Facebook, mais aussi Twitter, Linkedin, Viadeo, Google+, Copains d'avant, etc.

Ces nouveaux médias partagent tous certaines caractéristiques :

- les utilisateurs sont invités à fournir des données à caractère personnel permettant de donner une description ou un «profil» ;
- les réseaux sociaux mettent également à disposition des outils permettant aux utilisateurs de mettre leur propre contenu en ligne (contenu généré par l'utilisateur tel que des photos, des chroniques ou des commentaires, de la musique, des vidéos ou des liens vers d'autres sites) ;
- les réseaux sociaux fonctionnent grâce à l'utilisation d'outils mettant à disposition une liste de contacts pour chaque utilisateur avec une possibilité d'interaction entre eux.

Pour mémoire, Mark Zuckerberg a créé Facebook en 2004. Seulement six ans après, David Fincher portait son histoire sur grand écran, symbolisant ainsi le bouleversement de nos habitudes occasionné par l'essor de ces plates-formes communautaires. Aujourd'hui, Facebook compte plus de 850 millions d'utilisateurs dans le monde (dont plus de 24 millions en France [2]), est valorisé à 100 milliards de dollars [3] et prépare son introduction en bourse, qui pourrait intervenir en mai 2012 [4].

Après s'être développés sur « la mise en valeur » de nos vies privées et grâce à l'engouement des internautes, les réseaux sociaux ont suscité l'intérêt croissant du monde de l'entreprise. En effet, les entreprises qui se montraient, jusqu'alors, plutôt réticentes à l'utilisation des réseaux sociaux, s'en sont, aujourd'hui, peu à peu emparées comme nouveau vecteur de leur communication institutionnelle et commerciale [5].

Le développement et le succès d'audience des principaux réseaux sociaux (80 % des jeunes européens se connectent entre eux par le biais des réseaux sociaux en ligne) en ont fait des supports marketing et publicitaires indéniables. Cependant, leur utilisation, aussi généralisée et banale soit-elle désormais, n'est pas sans risque. Le succès et l'impact des réseaux sociaux a suscité la convoitise et a donc favorisé l'émergence d'une nouvelle forme de cybercriminalité [6]. Le terme de « cybercriminalité » – ou cyberdélinquance puisqu'il ne s'agit pas toujours de faits susceptibles de relever d'une cour d'assises – a été inventé à la fin des années quatre-vingt-dix, alors qu'internet se répandait en Amérique du Nord. Il n'est l'objet d'aucune définition légale. Selon le ministère de l'Intérieur, « la cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales qui sont commises *via* les réseaux informatiques, notamment, sur le réseau internet » [7].

Cette définition recouvre une grande variété d'infractions. La Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001 [8], distingue quatre types d'infractions :

- les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ;
- les infractions informatiques ;
- les infractions se rapportant au contenu ;
- les infractions liées aux atteintes à la propriété intellectuelle.

Cette typologie n'est pas totalement cohérente, dans la mesure où ces catégories se chevauchent parfois (ainsi, les infractions liées aux atteintes à la propriété intellectuelle peuvent se rapporter au contenu, etc.).

Il nous semble que cette nomenclature pourrait être simplifiée en se limitant à deux formes de cybercriminalité :

- celle qui porte atteinte aux réseaux (piratage, intrusions sur les sites, vol de données...) ;
- celle qui utilise les réseaux pour porter atteinte aux droits des personnes (contrefaçon, usurpation d'identité, escroquerie, pédopornographie, incitation à la haine raciale, propagande terroriste...).

Ce polymorphisme de la cybercriminalité se retrouve sur les réseaux sociaux. En effet, de la simple usurpation d'identité à l'attaque ciblée visant des données protégées les actes de malveillance s'expriment sous différentes formes et touchent tant les personnes, que les biens.

Est-ce à dire que la loi de la jungle règne sur les réseaux sociaux ? Certainement pas. Les réseaux sociaux ne sont pas une zone de non-droit, bien au contraire ; l'arsenal pénal français permet de sanctionner la plupart des infractions rencontrées sur les

(1) Avis 5/2009 sur les réseaux sociaux en ligne, adopté le 12 juin 2009, Groupe de travail « article 29 » sur la protection des données.

(2) www.toutfacebook.fr/statistiques-facebook-france-pour-mars-2012.

(3) N. Rauline, Facebook lance son introduction en Bourse, 1er févr. 2012, Les Echos, www.lesechos.fr/entreprises-secteurs/tech-medias/actu/0201875624724-facebook-lance-son-introduction-en-bourse-283196.php.

(4) Selon une information du Wall Street Journal, online.wsj.com/article/SB10001424052702303404704577309882117568426.html?KEYWORDS=Facebook.

(5) M. Cassaudin, Quand l'entreprise adopte les réseaux sociaux, 3 févr. 2012, Les Echos, lecercle.lesechos.fr/entrepreneur/developpement/221143006/quand-lentreprise-adopte-reseaux-sociaux.

(6) À titre d'exemple, les entreprises spécialisées dans la sécurité informatique n'hésitent pas à affirmer que les réseaux sociaux sont utilisés comme de véritables vecteurs pour les attaques malveillantes et en particulier du pillage à grande échelle des données personnelles de leurs utilisateurs ; voir notamment : Rapport Annuel sur la sécurité informatique de Barracuda Labs, l'enquête intitulée Social Media Protection 2011 de Symantec, la publication de Bitdefender intitulée *Les amis, les ennemis et facebook : La nouvelle lutte contre les escrocs*.

(7) www.interieur.gouv.fr/sections/a_votre_service/votre_securite/internet/cybercriminalite.

(8) conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=FRE. En France, la loi n° 2005-493 du 19 mai 2005 a approuvé la Convention du Conseil de l'Europe sur la cybercriminalité.

réseaux sociaux, qui se situent à la croisée des chemins de plusieurs dispositifs normatifs dont la violation peut entraîner une sanction pénale.
En effet, les réseaux sociaux constituent principalement un média et sont, à ce titre, soumis à la loi du 29 juillet 1881 sur la liberté de la presse qui réprime les infractions de presse (diffamation, injure, incitation à la haine raciale etc.). Ils forment également des traitements de données comportant des informations personnelles (nom, adresse e-mail, etc.) et sont à ce titre soumis à la loi du 6 janvier 1978 dite « Informatique et Libertés » qui réglemente notamment la collecte, la conservation et le transfert de ce type d'informations relatives à la vie privée (articles 226-16 à 226-24 du code pénal). Les contenus « postés » sur les réseaux sociaux sont, quant à eux, soumis au droit d'auteur, au droit à l'image et de manière générale au droit pénal.

***

Dans le cadre de la présente étude, nous nous limiterons aux principaux cybercrimes liés aux réseaux sociaux.
Les infractions portant atteinte aux systèmes informatiques des réseaux sociaux, tel le piratage, n'ont ni fait les gros titres, ni engorgé les tribunaux français bien que la Commission européenne dénombre « jusqu'à 600 000 comptes Facebook [...] bloqués chaque jour après avoir été la cible de plusieurs types de tentatives de piratage » [9].
À peine se souvient-on de l'arrestation, en 2009, d'un jeune internaute français originaire du Puy-de-Dôme pour avoir accédé aux comptes Twitter de personnalités américaines telles que Barack Obama ou Britney Spears. Ce jeune homme âgé de 23 ans et agissant sous le pseudo d'Hacker-Croll avait été recherché par le FBI et l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCT) [10]. Twitter n'avait, en revanche, pas porté plainte. Le 24 juin 2010, le tribunal de grande instance de Clermont-Ferrand l'a condamné à une peine de cinq mois de prison avec sursis. Le jugement est assez laconique et se contente d'affirmer que le jeune homme s'est rendu coupable d'accès frauduleux à un traitement automatisé de données au préjudice de la société Twitter [11].

En revanche, les premières affaires liées à des contenus « postés » sur les réseaux sociaux, susceptibles de porter atteinte à l'honneur et à la réputation des personnes ou des entreprises ont été très largement commentées. Il faut dire qu'en France, en 2011, les procédures pour diffamation auraient représenté 49 % des décisions judiciaires liées au web 2.0 [12].
L'arsenal législatif relatif à la protection de ce qu'il est désormais convenu d'appeler l' « e-réputation » a d'ailleurs été récemment complété par la loi dite LOPPSI II [13] pour tenir compte d'une pratique répandue sur les réseaux sociaux : l'usurpation d'identité.
Nous envisagerons, dans une première partie, les principales infractions rencontrées sur les réseaux sociaux portant atteinte à l' « e-réputation », avant d'évoquer les moyens dont disposent les victimes pour lutter contre les atteintes à leur e-réputation *via* les réseaux sociaux.

Il a depuis longtemps été jugé que la diffamation ou l'injure par la voie de l'internet constitue une publication « par voie de presse », et peut, à ce titre, faire l'objet de poursuite sur le fondement de la loi du 29 juillet 1881 sur la liberté de la presse.

Les principales infractions rencontrées sur les réseaux sociaux portant atteinte à l'« e-réputation »

La réputation d'une personne ou d'une entreprise peut se faire ou se défaire par le biais des réseaux sociaux.
Les assureurs n'ont d'ailleurs pas tardé à s'emparer du sujet et une société d'assurance a, tout récemment, diffusé un message publicitaire mettant en scène une jeune fille visiblement victime d'une atteinte à sa réputation sur internet (symbolisée par une tache qui se répand sur le reste de sa famille). Le commentaire qui accompagne cette vidéo est explicite : « Quand votre réputation est salie sur internet, c'est votre famille entière qui est touchée » et propose « une toute nouvelle assurance qui nettoie les informations malveillantes et vous protège également des autres risques d'internet » [14]...
Les principales infractions portant atteinte à l'e-réputation sont les propos injurieux ou diffamatoires et l'usurpation d'identité.

Les propos injurieux ou diffamatoires

La protection de l'e-réputation concerne tant les personnes physiques que les sociétés présentes sur les réseaux sociaux. En effet, il a depuis longtemps été jugé que la diffamation ou l'injure par la voie de l'internet constitue une publication « par voie de presse », et peut, à ce titre, faire l'objet de poursuite sur le fondement de la loi du 29 juillet 1881 sur la liberté de la presse.
L'article 29 de la loi définit la diffamation comme l'allégation ou l'imputation d'un fait précis, portant atteinte à l'honneur ou à la considération d'une personne déterminée ou déterminable, et ce publiquement et de mauvaise foi. En revanche, tous termes de mépris, toute expression outrageante, ou invective qui ne renferme l'imputation d'aucun fait précis est une injure.
Le contentieux relatif à la diffusion de propos diffamatoires ou injurieux sur les réseaux sociaux s'est particulièrement illustré dans le cadre des relations de travail.
Les circonstances de ces premières affaires sont peu ou prou les mêmes : un salarié mécontent « poste » un commentaire injurieux ou diffamant à l'encontre de son employeur qui en est informé d'une manière ou d'une autre.

(9) Communiqué de presse, Un Centre européen de lutte contre la cybercriminalité pour combattre la criminalité sur l'internet et protéger les consommateurs en ligne, du 28 mars 2012, europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317&format=HTML&aged=0&language=FR&guiLanguage=en.
(10) L'OCLCT appartient à la direction générale de la police nationale et dépend de la direction centrale de la police judiciaire. Cet organisme a été créé en mai 2000 afin de lutter contre la délinquance liée aux nouvelles technologies de l'information et de la communication.
(11) www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2982.
(12) Selon le projet de recherche, Les crimes dans le Web 2.0, de B. Dupont, directeur du Centre international de criminologie comparée, et V. Gautrais, titulaire de la Chaire de l'Université de Montréal, en droit de la sécurité et des affaires électroniques (www.ouvertures.net/portail/l_id.asp?doc_id=475).
(13) Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JO 15 mars 2011.
(14) www.youtube.com/watch?v=wJgnzqq3yv0.

C'est ce type de comportement qui a donné lieu à la décision très médiatisée du conseil de prud'hommes de Boulogne-Billancourt du 19 novembre 2010 [15]. Dans cette affaire, le conseil de prud'hommes avait admis la production par l'employeur d'une page Facebook qui était accessible aux « amis des amis », dans la mesure où ce mode d'accès dépassait la sphère privée. Le conseil avait, en outre, jugé fondé le licenciement pour faute grave d'une salariée qui avait « cautionné » des propos dénigrants et « incité à la rébellion contre la hiérarchie ». Il a ainsi jugé que la salariée licenciée « a abusé du droit d'expression visé à l'article L. 1121-1 du code du travail et a nui à l'image de la société [...] ». Le jugement est frappé d'appel.

À l'inverse, la cour d'appel de Rouen a jugé sans cause réelle et sérieuse le licenciement d'une salariée, engagée en qualité d'hôtesse de caisse, qui avait tenu ou soutenu des propos injurieux et calomnieux vis-à-vis de son employeur et de ses supérieurs hiérarchiques sur le réseau Facebook. La cour a estimé qu'en l'espèce, aucun élément ne permettait de dire que le compte Facebook tel que paramétré par la salariée, ou par les autres personnes ayant participé aux échanges, autorisait le partage avec les « amis » de ses « amis » ou toute autre forme de partage avec des personnes indéterminées, de nature à faire perdre aux échanges litigieux leur caractère de correspondance privée [16].

Il convient de relever que les victimes potentielles d'usurpation d'identité numérique peuvent être des personnes physiques, comme des personnes morales.

Il ressort de ces décisions que selon que les réseaux sociaux sont « ouverts » ou « fermés » à la communauté des internautes, ou selon le paramétrage du profil (restreint ou non aux amis), la publication de propos injurieux et/ou diffamatoires à l'encontre de l'employeur peuvent justifier – ou non – un licenciement pour faute grave.

Dans tous les cas, de tels propos peuvent entraîner une condamnation pénale, ainsi que le versement de dommages et intérêts pour indemniser l'atteinte portée à l'honneur et à la réputation de la victime. La seule différence est qu'à défaut de publicité, c'est-à-dire lorsque les propos poursuivis sont restreints à un groupe de personnes liées par une communauté d'intérêt, seule la contravention de diffamation ou d'injure non publique peut être retenue (c. pén., art. R. 621-1 et R. 621-2 - contraventions de 1re classe). À l'inverse, lorsque les propos sont considérés comme publics, c'est-à-dire publiés sur un réseau ouvert ou paramétré largement, ils sont constitutifs du délit prévu par l'article 29 de la loi du 29 juillet 1881.

Récemment, le tribunal correctionnel de Paris a condamné un salarié pour avoir publié des injures publique envers son employeur et son supérieur sur sa page Facebook dans les termes suivants : « Journée de merde, temps de merde, boulot de merde, boîte de merde, chef de merde... » « Ben j'aime pas les petits chefaillons qui joue au grand ». Le tribunal a jugé que le passage litigieux comportait « clairement des expressions outrageantes à l'encontre de la direction de l'entreprise » et excédait « les limites de la critique admissible, y compris lorsqu'elle s'exerce dans un cadre syndical » [17].

Au-delà de ce nouveau contentieux relatif aux relations de travail, les infractions d'injure ou de diffamation sont clairement définies par les textes et la jurisprudence et les réseaux sociaux, nouveau média, n'en sont qu'un nouveau vecteur de communication et de diffusion.

Il en va différemment de l'usurpation d'identité, infraction nouvelle qui recouvre une grande diversité de pratiques allant de la création de faux profils Facebook, aux opérations de *phishing*, en passant par les « arnaques nigériennes » (escroquerie consistant à envoyer un mail à une personne lui demandant ses identifiants bancaires afin de lui verser une somme importante) [18].

L'usurpation d'identité

La LOPPSI II, promulguée le 14 mars 2011 [19], a introduit dans le code pénal un délit spécifique d'usurpation d'identité s'étendant aux réseaux numériques. Ainsi, l'article 226-4-1 du code pénal sanctionne « le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ».

Tout d'abord, il convient de relever que les victimes potentielles d'usurpation d'identité numérique peuvent être des personnes physiques, comme des personnes morales.

Par ailleurs, ce n'est plus le seul nom de la victime qui est visé, mais son identité et plus largement n'importe quelle donnée « permettant de l'identifier ». Les informations relatives à l'identité d'une personne physique ou morale susceptibles d'être considérées comme des données « identifiantes » sont nombreuses et variées : nom, prénom, pseudonyme, photographie, dénomination sociale, nom commercial, sigle, marque, logo, enseigne, nom de domaine, adresse IP, adresse e-mail, etc.

Cette nouvelle incrimination comble un vide juridique en permettant de répondre à des actes malveillants qui ne pouvaient jusque-là tomber sous le coup d'aucune qualification pénale.

Certaines décisions avaient néanmoins sanctionné l'usurpation d'identité sur un réseau social sur le fondement de l'article 9 du code civil relatif au respect de la vie privée. À titre d'exemple, un acteur et humoriste avait assigné l'auteur d'une page Facebook créée à son nom (avec des photographies, des commentaires, messages postés où l'auteur du site se faisait passer pour lui...) en lui reprochant une atteinte à sa vie privée et une violation de son droit à l'image. Le tribunal a condamné l'auteur de la page incriminée en rappelant que toute personne, quelle que soit sa notoriété, a droit au respect de sa vie privée et est « fondée à en obtenir la protection en fixant elle-même les limites de ce qui peut être divulgué à ce sujet » et dispose également d'un droit exclusif qui lui permet de s'opposer à la reproduction de son image, sans son consentement préalable [20].

Toutefois, la voie civile était insuffisante pour sanctionner les usurpations d'identité les plus graves. En effet, l'usurpation d'identité est susceptible de

(15) Conseil de prud'hommes de Boulogne-Billancourt, 5e ch., 19 nov. 2010, n° F 09/00343, D. 2011. 2891, obs. P. Delebecque, J.-D. Bretzner et I. Gelbard-Le Dauphin.

(16) CA Rouen, 15 nov. 2011, n° 11/01827.

(17) TGI Paris, 17e ch. cor., 17 janv. 2012, n° d'affaire : 1034008388.

(18) Le délit d'usurpation d'identité au secours de l'e-réputation, Gérard Haas, www.haas-avocats.com/e-reputation/delit-usurpation-identite-au-secours-e-reputation.

(19) Loi n° 2011-267 du 14 mars 2011 d'orientation et programmation pour la performance de la sécurité intérieure.

(20) TGI Paris, 17e ch. civ., 24 nov. 2010, Comm. com. électr. 2011, comm. 28, note A. Lepage.

nuire gravement à l'e-réputation d'une personne ou d'une entreprise. Un faux profil bien réalisé peut avoir un effet désastreux tant sur l'entourage intime et personnel que sur l'entourage professionnel, les collaborateurs d'une entreprise, ses partenaires sociaux, les clients, les prospects, etc.
L'appréhension et la sanction de tels comportements sur les réseaux sociaux sont donc un enjeu important, tant pour les personnes physiques que pour les entreprises.

La lutte contre les atteintes à l'e-réputation *via* les réseaux sociaux

Deux solutions s'offrent à la victime d'une atteinte à son e-réputation : pour les infractions les moins graves, entraînant un préjudice susceptible d'être réparé par le seul retrait des propos litigieux, la victime peut se contenter de saisir le fournisseur du réseau social, qui en sa qualité d'hébergeur, a l'obligation de supprimer les publications manifestement illicites. En revanche, les atteintes les plus violentes à l'e-réputation qui justifient des poursuites pénales contre l'auteur des propos litigieux, nécessitent souvent des actions précontentieuses afin d'identifier l'auteur de l'infraction poursuivie.

L'action contre les fournisseurs de réseaux sociaux

Les fournisseurs de réseaux sociaux sont des hébergeurs. À ce titre, leur responsabilité peut être engagée à raison des contenus illicites publiés sur leur réseau, si, après en avoir eu connaissance, ils n'ont pas « agi promptement pour retirer ces informations ou en rendre l'accès impossible ». Cette responsabilité reste toutefois limitée.

La procédure de notification de contenu illicite ou *notice and take down*

La procédure de notification de contenu illicite a été instaurée par la LCEN [21]. Elle a pour but d'obtenir le retrait du contenu illicite ou le blocage par l'hébergeur du site internet concerné, et ce, avant toute intervention de l'autorité judiciaire.
Cette procédure est très largement inspirée de la procédure de *notice and take down* introduite aux États-Unis par le Digital Millennium Copyright Act [22] et répond aux exigences de transposition de la directive européenne du 8 juin 2000 [23].
Selon l'article 6, I, 3 de la loi LCEN, l'hébergeur bénéficie d'une limitation de responsabilité si, une fois informé de l'existence d'un contenu manifestement illicite, il « a agi promptement pour retirer ces informations, ou en rendre l'accès impossible ».
Le point 5 du même article précise que « la connaissance des faits litigieux est présumée acquise [...] lorsqu'il [*lui*] est notifié les éléments suivants :
- la date de la notification ;
- si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;
- les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;
- la description des faits litigieux et leur localisation précise ;
- les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;
- la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté ».

Selon la Cour de cassation, « la notification délivrée au visa de la loi du 21 juin 2004 doit comporter l'ensemble des mentions prescrites par ce texte » [24]. À défaut, elle ne sera pas opposable à l'hébergeur.
En revanche, cette notification faite « dans les règles de l'art » crée une présomption d'acquisition de la connaissance du caractère illicite du contenu par le fournisseur d'hébergement.
En tout état de cause, pour que la responsabilité des hébergeurs soit engagée, il faut que « le caractère illicite de l'information dénoncée soit manifeste ou qu'un juge en ait ordonné le retrait ». C'est ce qu'a précisé le Conseil constitutionnel dans sa décision du 10 juin 2004 [25].
En revanche, les Sages n'ont pas jugé utile de préciser ce qu'ils entendaient par « manifestement illicite ». À l'origine, la doctrine s'accordait à dire que cette notion visait « principalement les contenus d'une gravité avérée et dont le caractère illicite ne semble pas discutable [...] par exemple, des contenus à caractère pédopornographique, des écrits faisant l'apologie des crimes de guerre ou qui provoquent directement aux actes de terrorisme » [26] à l'exclusion des cas de diffamation classique. Les juridictions ont, toutefois, retenu une interprétation plus extensive du terme « manifestement illicite » et n'hésitent pas à juger que l'injure et la diffamation publiques « constitue(nt) un trouble manifestement illicite au sens de l'article 809 du code de procédure civile », qui justifie le retrait des textes litigieux [27].
Ainsi, lorsqu'un contenu diffamatoire ou injurieux est notifié à un fournisseur de réseau social, celui-ci doit agir promptement (en général sous 48 heures) pour le retirer ou en rendre l'accès impossible.
En outre, le point 8 de l'article 6, prévoit que « l'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 (FAI) ou, à défaut, à toute personne mentionnée au 1 (hébergeur), toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ».
Ainsi, aux termes de la loi française, rien ne s'oppose à ce que le juge prononce pour l'avenir une ordonnance qui vise à prévenir d'autres atteintes aux droits des personnes.
Les juridictions nationales se sont engouffrées dans cette brèche et, notamment en matière de contrefaçon, ont rendu des décisions qui mettent à la charge de l'hébergeur l'obligation de mettre en œuvre tous les moyens nécessaires en vue d'éviter une nouvelle

(21) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JO 22 juin 2004.
(22) www.copyright.gov/legislation/dmca.pdf.
(23) eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML.
(24) Civ. 1re, 17 févr. 2011, n° 09-13.202, n° 09-67.896 et n° 09-15.857, D. 2011. 669 ; *ibid.* 2164, obs. P. Sirinelli ; *ibid.* 2363, obs. J. Larrieu, C. Le Stanc et P. Tréfigny-Goy.
(25) Cons. const. 10 juin 2004, n° 2004-496 DC.
(26) L. Thoumyre, Les hébergeurs en ombres chinoises. Une tentative d'éclaircissement sur les incertitudes de la LCEN, Rev. Lamy Dr. de l'immatériel, mai 2005, p. 58.
(27) Paris, ch. 14, sect. B, 21 janv. 2005, n° 04/14975.

diffusion d'un contenu illicite précédemment notifié, introduisant ainsi le *notice and stay down* [28].

La Cour de justice de l'Union européenne (CJUE) a approuvé la jurisprudence française en jugeant que les dispositions communautaires en matière de contrefaçon permettent aux juridictions nationales d'enjoindre au prestataire d'un service en ligne, tel que celui mettant à la disposition des internautes une place de marché en ligne, de prendre des mesures qui contribuent de façon effective, non seulement à mettre fin aux atteintes portées au moyen de cette place de marché, mais aussi à prévenir de nouvelles atteintes. Ces injonctions doivent être effectives, proportionnées, dissuasives et ne doivent pas créer d'obstacles au commerce légitime [29].

La fermeture récente de Megaupload est un autre exemple du durcissement du régime de responsabilité des hébergeurs. En effet, l'acte d'accusation reproche à Megaupload le manque d'efficacité de ses procédures de *notice and take down* qui, si on lit entre les lignes auraient dû permettre le*stay down* [30].

La CJUE s'oppose ainsi à une injonction prise à l'encontre d'un intermédiaire technique de mettre en place un système de filtrage généralisé, à titre préventif, à ses frais exclusifs et sans limitation de temps.

Si le glissement de la procédure de *notice and take down* vers une procédure de *notice and stay down* a été initiée en matière de droits d'auteur et de droit des marques, les même exigences devraient pouvoir exister pour assurer la protection des droits des personnes et notamment leur e-réputation. Ainsi, à titre d'exemple, un faux profil (usurpation d'identité) signalé sur un réseau social devrait éviter que de nouveaux faux profils du même type réapparaissent.

En revanche, l'interdiction posée par la directive du 8 juin 2000 d'imposer à un hébergeur une obligation générale de surveillance, interdit de contraindre un réseau social à mettre en place un système de filtrage *a priori*.

Une responsabilité qui reste limitée

La CJUE a tout récemment jugé que l'exploitant d'un réseau social en ligne, en l'espèce Netlog, ne peut être contraint de mettre en place un système de filtrage général, visant tous ses utilisateurs, pour prévenir l'usage illicite des œuvres musicales et audiovisuelles. Selon la Cour, « une telle obligation ne respecterait pas l'interdiction d'imposer à un tel prestataire une obligation générale de surveillance ni l'exigence d'assurer le juste équilibre entre, d'une part, la protection du droit d'auteur et, d'autre part, la liberté d'entreprise, le droit à la protection des données à caractère personnel et la liberté de recevoir ou de communiquer des informations » [31].

La CJUE s'oppose ainsi à une injonction prise à l'encontre d'un intermédiaire technique de mettre en place un système de filtrage généralisé, à titre préventif, à ses frais exclusifs et sans limitation dans le temps.

Cette décision ne remet pas en cause la possibilité pour le juge d'enjoindre aux hébergeurs de prendre des mesures visant non seulement à mettre fin aux atteintes déjà portées aux droits de propriété intellectuelle, mais aussi à prévenir de nouvelles atteintes. En bref, des injonctions pour le futur OUI, mais un filtrage généralisé NON.

On en reste donc au principe du *notice and take down* : si une personne ou une société est informée d'une atteinte manifeste à son e-réputation sur un réseau social, elle en informe le fournisseur du réseau en question qui est tenu d'y mettre un terme.

Du fait de l'interdiction du filtrage, la recherche de l'infraction pèse uniquement sur la victime potentielle. Or, celle-ci peut se trouver confrontée à des difficultés procédurales parfois insurmontables à défaut de réagir promptement. Par exemple la courte prescription qui s'applique en matière d'infractions de presse, ne lui laisse que peu de temps pour réagir [32].

En tout état de cause, pour les atteintes les plus graves à leur e-réputation, les victimes souhaitent le plus souvent se retourner contre l'auteur même des contenus litigieux.

L'identification de l'auteur et les poursuites à son encontre

Tout d'abord, il convient de souligner que l'identification de l'auteur d'une infraction est rendue possible par l'obligation de conservation des données qui incombe aux fournisseurs de réseaux sociaux. Cependant, les fournisseurs de réseaux sociaux ne communiquent ces informations que lorsqu'ils y sont contraints judiciairement.

L'obligation de conservation des données s'impose aux fournisseurs de réseaux sociaux

Les réseaux sociaux qui fournissent à leurs membres un hébergement de données susceptibles d'être consultées par le public doivent être qualifiés d'hébergeurs au sens de la loi pour la confiance dans l'économie numérique (LCEN).

La LCEN et le code des postes et des communications électroniques (CPCE) prévoient, à la charge des fournisseurs d'accès à internet (FAI), des hébergeurs et des opérateurs, l'obligation de conserver les données de connexion et de les communiquer à l'autorité judiciaire, sur demande de cette dernière. La durée de conservation de ces données est fixée à un an.

Ce n'est que sept ans après la publication de la LCEN, que le législateur a adopté le décret n° 2011-219 du 25 février 2011 prévu par l'article 6 de la loi, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, .

Aux termes de ce décret [33], pris non seulement au visa de la LCEN, mais aussi du CPCE, les FAI doivent, pour chaque connexion de leurs abonnés, conserver les données suivantes :

« a) l'identifiant de la connexion ;

(28) Not., TGI Paris, 19 oct. 2007, *SARL Zadig Production, Jean-Robert V. et Mathieu V. c/ Sté Google Inc. et AFA*, www.juriscom.net/documents/tgiparis20071019.pdf ; TGI Créteil, 1re civ., 14 déc. 2010, www.legalis.net/spip.php?article3052.

(29) E. Daoud, Le commerce en ligne : de la loi de la jungle au respect de la morale et du droit, www.journaldunet.com/ebusiness/expert/50055/le-commerce-en-ligne—de-la-loi-de-la-jungle-au-respect-de-la-morale-et-du-droit.shtml.

(30) E. Daoud, FBI vs Megaupload + Anonymous : règlements de comptes à OK Corral !, www.journaldunet.com/ebusiness/expert/50846/fbi-vs-megaupload—anonymous—reglements-de-comptes-a-ok-corral.shtml.

(31) CJUE 16 févr. 2012, aff. C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) c/ Netlog NV*, D. 2012. 549, obs. C. Manara ; curia.europa.eu/jcms/upload/docs/application/pdf/2012-02/cp120011fr.pdf.

(32) En application de l'article 65 de la loi du 29 juill. 1881, passé le délai de 3 mois après la publication d'un contenu diffamatoire ou injurieux, aucune action n'est plus envisageable sur le fondement de l'article 29 de la même loi.

(33) Modifié par le décret n° 2012-436 du 30 mars 2012.

b) l'identifiant attribué par ces personnes à l'abonné ;
c) l'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;
d) les dates et heure de début et de fin de la connexion ;
e) les caractéristiques de la ligne de l'abonné ».

Les hébergeurs doivent, quant à eux, conserver pendant un an à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu :

« a) l'identifiant de la connexion à l'origine de la communication ;
b) l'identifiant attribué par le système d'information au contenu, objet de l'opération ;
c) les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;
d) la nature de l'opération ;
e) les date et heure de l'opération ;
f) l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ».

Les FAI et hébergeurs doivent également conserver les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, à savoir :

« a) au moment de la création du compte, l'identifiant de cette connexion ;
b) les nom et prénom ou la raison sociale ;
c) les adresses postales associées ;
d) les pseudonymes utilisés ;
e) les adresses de courrier électronique ou de compte associées ;
f) les numéros de téléphone ;
g) les données permettant de vérifier le mot de passe ou de le modifier, dans leur dernière version mise à jour... ».

En outre, lorsque la souscription du contrat ou du compte avec l'utilisateur est payante, les prestataires sont tenus de détenir et de conserver les données relatives au paiement, telles que :

« a) le type de paiement utilisé ;
b) la référence du paiement ;
c) le montant ;
d) la date et l'heure de la transaction ».

Tout manquement à cette obligation de conservation des données expose aux sanctions visées aux articles 6 VI de la LCEN et L. 39-3 du code des postes et communications électroniques : un an d'emprisonnement et 75 000 euros d'amende, et le quintuple pour les personnes morales (en application de l'article 131-38 du code pénal).

Ce dispositif permet aux instances de répression d'enquêter sur les actes de cybercriminalité et de poursuivre en justice leurs auteurs de façon efficace. Les réseaux sociaux, en leur qualité d'hébergeurs, sont donc soumis à l'obligation de conservation des données.

Ainsi, la victime d'un contenu illicite publié sur un réseau social peut obtenir sur décision judiciaire communication par ce dernier, de l'ensemble des éléments à sa disposition susceptibles d'identifier l'auteur du contenu litigieux.

Cette procédure est le plus souvent engagée sur le fondement de l'article 145 du code de procédure civile.

Les mesures d'instruction *in futurum*

Aux termes de l'article 145 du code de procédure civile, « s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé ». Ces mesures d'instruction, dites *in futurum*, permettent aux parties de s'assurer une meilleure connaissance des éléments du conflit et sont également de nature, parfois, à éviter ou prévenir un procès.

Dans l'affaire précédemment évoquée qui a conduit la 17e chambre correctionnelle du TGI de Paris à condamner pénalement un salarié pour avoir injurié son employeur et son supérieur hiérarchique, l'auteur des propos injurieux avait pris soin de se retrancher derrière un pseudonyme [34]. Afin d'identifier l'auteur des propos, l'employeur avait donc saisi le président du tribunal de grande instance de Paris par voie de requête sur le fondement de l'article 145 du code de procédure civile et avait obtenu de celui-ci une ordonnance enjoignant la société Facebook Inc à lui communiquer l'ensemble des éléments dont elle disposait permettant l'identification éventuelle de la personne à l'origine des propos litigieux. Saisie judiciairement, Facebook Inc avait fait droit à cette ordonnance et communiqué l'adresse e-mail qui avait servi à l'ouverture du profil litigieux.

Dans cette affaire, l'adresse e-mail du titulaire du profil comportait le nom et le prénom du salarié et son identification était évidente. Mais il arrive souvent que l'adresse e-mail ne comprenne aucun élément d'identification. Dans ce cas, il peut être nécessaire de procéder à d'autres mesures d'instruction *in futurum*, par exemple afin qu'il soit ordonné au FAI d'identifier le titulaire de l'adresse e-mail ou des adresses IP.

Bien entendu, avant d'engager toute action même précontentieuse à l'encontre d'un réseau social, il convient de conserver des preuves de l'atteinte que l'on dénonce par la voie d'un constat d'huissier. Car une fois informés d'un éventuel contentieux, les fournisseurs de réseaux sociaux ont tendance à procéder rapidement au retrait des publications litigieuses.

Une fois ces étapes (laborieuses – il faut bien le reconnaître) achevées, la procédure contentieuse classique reprend son cours. De deux choses l'une : soit l'identification de l'auteur des propos a été rendu possible et la victime peut exercer son action devant la juridiction répressive, par le biais d'une citation directe, soit l'identification n'a pas été possible et la victime peut déposer une plainte contre X. Dans cette dernière hypothèse, elle s'en remet aux enquêteurs spécialisés en criminalité informatique dont les pouvoirs d'investigations sont largement plus étendus, mais qui sont eux aussi victimes de l'explosion de la cybercriminalité et en sous-effectif.

***

Il ressort de ce qui précède que l'abus de liberté d'expression sur les réseaux sociaux n'est pas une fatalité. Le caractère anxiogène lié aux réseaux sociaux et à leur impact social et médiatique ne doit pas paralyser les victimes d'atteintes à leur e-réputation, qui doivent au contraire surmonter leurs craintes liées au fonctionnement même d'internet, souvent identifié à une nébuleuse sans visage. Sans aller jusqu'au contentieux, on a vu qu'il existe, dans un premier temps, des procédures efficaces de retrait qui permettent de « nettoyer » les réseaux sociaux et plus généralement l'internet. En outre, la mise en place d'une « veille numérique » permettra

(34) TGI Paris, 17e ch. cor., 17 janv. 2012, préc.

une réaction immédiate en cas de campagne de dénigrement *via* les réseaux sociaux et évitera de tomber dans le piège de la courte prescription applicable aux infractions de presse.
Le risque de réputation doit, en effet, non seulement être pris en considération au stade de la gestion d'une crise, mais aussi au stade de la prévention du risque.
Enfin, le droit positif est certainement perfectible mais en l'état, les victimes des infractions examinées dans la présente étude ont les moyens techniques et juridiques de poursuivre les auteurs des infractions reprochées.

On ne peut à la fois se lamenter des ravages de la cybercriminalité au travers des réseaux sociaux et dans le même temps ne rien faire !
En effet, à une époque où la vie privée des personnes physiques est, à juste titre, sacralisée, et où les entreprises utilisent les réseaux sociaux comme un outil du marketing viral pour assurer une meilleure pénétration de leurs marques, le droit pénal permet d'agir, et donc de protéger la sphère de l'intime et de sauvegarder son e-réputation.

Téléchargement illégal et Hadopi

par Frédérique Chopin
Maître de conférences HDR, Aix-Marseille Université, CDS EA 901

« Tout ce qui augmente la liberté, augmente la responsabilité » V. Hugo

« Hier : l'immatériel survolait la répression. Aujourd'hui : l'immatériel nargue la répression. Demain : l'immatériel transfigurera-t-il la répression » ? [1] Telle est la question qui se pose alors que, fin septembre 2011, la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (HADOPI) a déjà adressé 650 000 premières recommandations et 44 000 secondes recommandations, suite à des téléchargements illicites sur internet.
Face à l'ampleur du phénomène depuis plusieurs années, le législateur est intervenu à diverses reprises pour essayer de l'endiguer [2], mais sans véritable cohérence des politiques publiques en la matière [3]. En effet, ce fut, d'abord, la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) qui, notamment, obligea les fournisseurs d'accès à internet à informer les internautes du caractère nuisible de l'acte de piratage à l'égard de la création. Ensuite, la loi sur les droits d'auteur et les droits voisins dans la société de l'information, dite loi DADVSI du 1er août 2006, continua à privilégier la prévention et l'éducation dans l'utilisation d'internet : elle imposa aux fournisseurs d'accès, d'adresser, à leurs frais, à leurs utilisateurs, des messages de sensibilisation aux dangers du téléchargement et de la mise à disposition illicite pour la création artistique. Dans le même temps, la loi DADVSI s'orienta aussi vers une politique plus répressive en instaurant deux nouvelles mesures : tout d'abord, elle mit en place la responsabilité pénale des éditeurs de logiciels « manifestement destinés à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés » (art L. 335-2-1 CPI). Cette disposition se révèle toujours difficile à mettre en œuvre quand il s'agit d'apprécier le caractère « manifeste » de l'outil. Ensuite, elle imposa aux titulaires d'un accès à internet, une obligation de surveillance de leur accès qui sera au cœur du dispositif mis en place par les lois Hadopi. D'abord, la loi Hadopi 1 du 12 juin 2009 crée une autorité administrative indépendante, l'Hadopi, investie uniquement, suite à la censure du Conseil constitutionnel [4], d'un pouvoir de prévention et d'éducation à l'utilisation de l'internet, notamment par le recours au système de la « réponse graduée ». C'est, ensuite, la loi Hadopi 2 du 28 octobre 2009, relative à la protection pénale de la propriété littéraire et artistique sur internet, qui donne un cadre répressif au téléchargement illégal sur internet, en instaurant non seulement des sanctions, des incriminations nouvelles, mais aussi, une procédure spécifique, désormais confiée au juge judiciaire.
Pourtant, cet arsenal législatif a aujourd'hui du mal à se concilier avec un certain nombre de droits et libertés fondamentaux tels que la liberté d'expression, de communication, d'entreprendre ou encore le droit à l'information. En outre, ce dispositif mis en place par l'Hadopi, avant tout destiné à dissuader les internautes, souffre d'ores et déjà de nombreuses faiblesses face aux nouvelles techniques de partage des œuvres sur internet et cette Haute autorité se trouve de plus en plus confrontée à l'anonymat des utilisateurs, ce qui réduit là encore, l'efficacité du dispositif.

Les faiblesses de l'Hadopi face au partage des œuvres sur internet

Lors de l'adoption des lois DADVSI et HADOPI 1 et 2, le législateur avait essentiellement pour objectif de lutter contre la pratique du téléchargement illégal *via* la pratique du pair à pair (*peer to peer* ou P2P). Aujourd'hui, de nouveaux modes de partage des œuvres sur internet sont utilisés face auxquels la réponse graduée de l'Hadopi semble inadaptée.

(1) G. Vermelle, L'immatériel et la répression, Archives Phil. dr., 1999, Tome 43, p. 213.
(2) 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.
(3) F. Chopin, Les politiques publiques de lutte contre la cybercriminalité, AJ pénal 2009. 101.
(4) Cons. const. 10 juin 2009, n° 2009-580 DC, D. 2009. 2045, point de vue L. Marino.