

Connectez-moi !

Fabrice Mattatia

préface d'Alain Bobant

INTERNET ET LES RÉSEAUX SOCIAUX :

que dit la loi ?



- Liberté d'expression
- Données personnelles
- Achats en ligne
- Internet au bureau

2^e édition

EYROLLES

2^e édition

INTERNET ET LES RÉSEAUX SOCIAUX :

que dit la loi ?

La loi s'applique aussi sur Internet !

Cet ouvrage de référence vulgarise pour tout internaute le cadre juridique de la publication de contenus et de l'usage des services sur Internet : liberté d'expression, réseaux sociaux, droits d'auteur, licences Creative Commons, données personnelles... Cette nouvelle édition est à jour des dernières jurisprudences ainsi que des nouvelles lois, et explique par de nombreux exemples concrets la protection des données communiquées aux e-commerçants, les transactions e-commerce, l'utilisation d'Internet en entreprise, ou encore les accès frauduleux.

Un livre toujours aussi indispensable pour comprendre ses droits et ses devoirs sur Internet !

Ancien conseiller de la secrétaire d'État au numérique, polytechnicien et docteur en droit, Fabrice Mattatia est expert en confiance numérique. Il intervient dans plusieurs universités, dont Paris I Panthéon Sorbonne et La Rochelle, et dans des grandes écoles comme Télécom ParisTech. Il est également l'auteur de nombreux articles de vulgarisation sur le droit et sur les technologies.

Neutralité du Net • Liberté d'expression • Responsabilité • Données personnelles • Vie privée • E-réputation • Réseaux sociaux • Anonymat • Identité numérique • Droits d'auteur • DRM, téléchargements illégaux et Hadopi • Transactions • Achats en ligne • Ventes entre particuliers • Litiges • Internet au bureau • BYOD et télétravail • Parler de son employeur sur les réseaux sociaux • Cybercriminalité • Phishing • Spam

Connectez-moi !

Démystifier les rouages de la société numérique.

www.editions-eyrolles.com

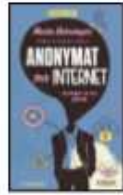
Codex éditeur : 614029
ISBN : 978-2-212-14029-3

Couverture : Studio Eyrolles / Shutterstock © Editions Eyrolles

INTERNET ET LES RÉSEAUX SOCIAUX :

que dit la loi ?

CHEZ LE MÊME ÉDITEUR



Retrouvez aussi nos livres numériques sur
<http://izibook.eyrolles.com>

Connectez-moi !

Fabrice Mattatia
préface d'Alain Bobant

INTERNET ET LES RÉSEAUX SOCIAUX :

que dit la loi ?



EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Remerciements à Anne Bougnoux pour sa relecture, ainsi qu'à Alain Bobant pour sa préface, et à François Coupez, Olivier Itéanu et Marc Lolivier pour leurs contributions.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans l'autorisation de l'Éditeur ou du Centre Français d'exploitation du droit de copie, 20, rue des Grands Augustins, 75006 Paris.

© Groupe Eyrolles, 2015, ISBN : 978-2-212-14029-3

Préface

d'Alain Bobant

À partir de 2005, l'internaute s'est mis à exploiter des usages inédits, a adopté la « Web attitude », et est devenu un « actinaute ». Désormais, il s'enfonce dans l'épaisse végétation du Web de manière active et interactive.

Isolé mais désinhibé, il se montre, il se signale et il se fait connaître ; il s'exprime, il s'exteriorise ; il se singularise et il se fait remarquer, il s'illustre, il influe... Mais en s'agitant et en s'exhibant, il s'expose à des risques de toutes natures.

Fabrice Mattatia a eu la bonne idée d'opérer un traitement méthodique du sujet. Il offre à « l'internaute actif » un ensemble exhaustif de règles applicables au domaine de l'Internet.

Particulièrement riche, le contenu didactique de cet ouvrage peut mettre à l'abri de nombreuses atteintes, apporter un sentiment de sécurité, et protéger de certains effets pervers du Web.

Alain Bobant
Président de la FNNTC
(Fédération nationale des tiers de confiance)

Table des matières

Avant-propos 1

Redécouvrir les concepts d'Internet 2

Rappel sur les abonnements à Internet 3

RAPPEL TECHNIQUE Le débit 3

Triple play, quadruple play 4

JURISPRUDENCE Droit des FAI à proposer des contenus exclusifs 4

Internet mobile 5

DROIT DES CONSOMMATEURS Qu'est-ce qu'un abonnement illimité ? 6

La neutralité du Net 6

DÉFINITION La neutralité du Net 7

Le financement du Net 9

1. La liberté d'expression sur Internet 11

La liberté d'expression, un droit fondamental, mais pas absolu 12

QUI EST CONCERNÉ SUR INTERNET ? Tout le monde ! 13

CONFLIT DE DROITS La liberté d'expression dans la loi américaine 13

Les abus dont la loi vous protège 14

Cas général et cas particulier 14

La diffamation et l'injure 14

LA MISE À JOUR DES LOIS La loi de 1881 modifiée 14

DÉFINITIONS Allégation, imputation, invective 15

EN DÉTAIL Les jurisprudences 16

RAPPEL La hiérarchie des tribunaux 16

Diffamation ou injure, il faut choisir 17

Diffamation et injure publiques envers des personnes 18

EN DÉTAIL Les différentes sanctions financières 18

EN DÉTAIL Le sursis 19

Et envers l'employeur ? 19

Et envers la police ? 19

PROCÉDURE Le référé 20

Et les injures privées ? 20

La codification 20

Jurisprudences concernant Google Suggest 21

Twitter 22

QUESTION Les retweets 23

Des délits que l'on souhaite rares... 23

Le délit d'incitation 23

L'apologie de crimes de guerre ou de crimes contre l'humanité,
l'appel au terrorisme 25

DÉFINITIONS Apologie et négationnisme 26

Le négationnisme 26

Le formalisme 27

La procédure à respecter 27

La possibilité de prouver les faits (exception de vérité) 27

PRÉCISION L'intention malveillante 28

Délai de prescription et droit de réponse 29

Un délai trop court ? 29

DÉFINITION Le délai de prescription 29

Refus du tribunal de contourner la prescription 30

Quel est le point de départ du délai de prescription ? 30

Le droit de réponse 31

Qui peut l'exercer ? 31

Quelles modalités ? 32

Publication de la réponse 33

Condamnation pour non-publication d'un droit de réponse 33

2. Qui est responsable ? 35

La responsabilité de ses actes, un principe 35

Obligation d'identification pour les professionnels, anonymat partiel
toléré pour les particuliers 35

Sites web professionnels 35

Sites web personnels 36

Le directeur de la publication 37

La responsabilité en cascade 37

DÉFINITION	Le producteur	38
	Modérer ou ne pas modérer ?	38
	La responsabilité du producteur	39
EN DÉTAIL	Le Conseil constitutionnel	40
	Confirmation de la limitation de responsabilité du producteur	41
	Jurisprudence sur le directeur de la publication	41
	Responsabilité des mineurs	42
	Comment signaler un contenu illicite ?	42
	Les responsabilités de l'hébergeur	43
DÉFINITIONS	La distinction éditeur/hébergeur	43
DÉFINITION	L'hébergeur	44
	Contrôle de la légalité des contenus	44
PRÉCISION	Avis du Conseil constitutionnel	45
FORMALISME	La notification	45
	Jurisprudences concernant les responsables de forums	46
EXTRAIT DU JUGEMENT	Forum non modéré ou modéré a posteriori	46
	La réapparition de contenus illicites supprimés	47
DÉFINITION	Le droit prétorien	48
À SUIVRE	Portée de l'obligation	49
	Conservation des données de connexion	49
À SUIVRE	La position de la Cour de justice de l'Union européenne (CJUE)	50
	Applicabilité aux services web non européens	51
	Obligation de lutte contre les contenus illégaux	51
	Applicabilité aux services web non européens	51

3. Que deviennent vos données personnelles ? 53

	L'émergence de la vie privée	54
LA VIE PRIVÉE	Une notion récente	54
LA VIE PRIVÉE	Une notion relative	55
DROIT INTERNATIONAL	Les textes fondamentaux	56
	De la vie privée aux données personnelles	57
DÉFINITION	Qu'est-ce qu'une donnée personnelle ?	58
	La valeur des données personnelles	58
PERSPECTIVES	La valeur des données personnelles	60
DÉTAIL	Les propriétés du droit de propriété	61

Les principes fondamentaux de la protection des données
personnelles 61

Information et consentement 62

Droit d'accès, de modification et d'opposition 62

Finalité du traitement 62

Qualité des données 62

Sécurité des données 62

Limitation de la durée de conservation 62

Protection des données « sensibles » 63

CAS PARTICULIER Les associations religieuses, partis politiques, syndicats 63

Limitation de l'exportation hors de l'Union européenne 63

JURISPRUDENCE La diffusion sur Internet 64

Champ d'application de la loi 64

Les traitements concernés par la loi 64

JURISPRUDENCE Accès manuel à des données 65

JURISPRUDENCE Utilisation d'un appareil informatique 66

Le champ territorial de la loi 66

Des conditions de localisation restrictives 66

À RETENIR Un champ territorial restreint 67

Application de la loi française aux services web établis hors de
l'Union européenne 68

JURISPRUDENCE Application à Yahoo! des lois françaises 68

LA LOI Le droit à la vie privée 70

Récents revirements de jurisprudence 70

Les droits de l'internaute 71

Droit de consentement 71

ZOOM Le spam 71

Droit d'opposition 72

EN PRATIQUE Le droit d'opposition, mirage ou épouvantail ? 72

EN PRATIQUE Comment réagir en cas de spam ? 73

Droit d'accès et de rectification 73

EN PRATIQUE Max Schrems et Facebook 74

Droit au déréférencement 75

Comment faire valoir ses droits ? 76

Les devoirs du créateur de site web 76

Formalités administratives 77**ZOOM** Condamné pour non-déclaration de site web 77**Devoir d'information 77****Sécurité des données 78****LIMITATION DE RESPONSABILITÉ** Une obligation de moyens 79**Prospection commerciale 79****ZOOM** Les cas de prospection non encadrés par la loi 80**Les cookies 81****ZOOM** Opt-out et opt-in 82**Conservation des données de connexion et de localisation 83****Sanction encourues en cas de non-respect de la loi 83****ZOOM** Deux voies de sanction 84**ZOOM** Droit d'Internet et droit général 85**Jurisprudences 85****Condamnation pour mise en ligne de photos intimes 85****DISCUSSION** Comment interpréter cette condamnation ? 86**Sanctions pour spam 86****DÉTAIL** Les différentes demandes de la Cnil non satisfaites par JPSM 87**Accès à des données personnelles non sécurisées 87****Sanctions pour défaut de sécurité d'un site 89****Sanction pour non-respect de la loi Informatique et Libertés 90****Perspectives 90****4. La e-réputation 91****L'exposition sur les réseaux sociaux 91****EXEMPLE** La suppression de compte chez Facebook 92**EXEMPLE** Les publications des amis chez Facebook 93**LE DROIT** Les réseaux sociaux sont bien par nature soumis à la loi sur les données personnelles 94**Des conséquences parfois douloureuses 94****Les données divulguées à l'insu de la personne concernée 97****Les recours en cas de publication par un tiers 98****Le cas extrême du happy slapping 99****La collecte de données par les sites web 100****La vie conjugale 101****Avatars et anonymat 102**

Le droit à l'anonymat	102
Le mensonge comme technique de protection	103
Une tendance ancienne...	103
... qui se perpétue	105
L'utilisation de réseaux anonymisés	105
L'identité numérique	106
L'usurpation d'identité	106
Le droit général	106
Le droit face aux défis d'Internet	107
ZOOM Le faux Alain Juppé	109
La preuve d'identité sur Internet	111
Les usages de l'identité numérique	112
ZOOM Les enjeux	113
Les solutions techniques	113
DÉTAIL Et la France ?	115
LE POINT DE VUE DU SPÉCIALISTE Olivier Itéanu, avocat à la cour d'appel de Paris	117

5. Les droits d'auteur 121

À l'origine de la propriété intellectuelle	121
Propriété littéraire et artistique : encadrement de la reproduction	123
Qui est concerné ?	123
Droit d'auteur sur une photo	124
Droit d'auteur sur un tableau	125
Droit d'auteur sur un tweet	125
Les droits de divulgation et d'exploitation	126
Les droits moraux de l'auteur	126
Les droits patrimoniaux	126
Les droits voisins	127
Les exceptions	127
Les copies transitoires	129
Licences, logiciels et données libres	129
ZOOM Les données généalogiques	130
Jurisprudences pour violation des droits d'auteur	131
Les DRM, les téléchargements illégaux et Hadopi	133

Jurisprudences concernant le téléchargement illicite 133

L'encadrement de la copie privée 134

DÉBAT Les barèmes 136

Les DRM 136

DÉBAT Les dés du Blu-Ray 136

DÉBAT Les contradictions du dispositif 137

Les mesures pénales 137

Le téléchargement illégal et Hadopi 138

DROIT Les autorités administratives indépendantes 139

DÉTAIL Le peer-to-peer (P2P) et le streaming 139

TECHNIQUE L'adresse IP 140

BIEN Hadopi 2010-2014 141

Les logiciels, sites web et bases de données 142

DÉTAIL Le cas des auteurs salariés 142

DÉFINITION Le droit prétorien 143

JURISPRUDENCE La paternité d'un logiciel 144

PRÉCISION La limite du droit d'observation 145

Revente de logiciels d'occasion 146

Vente liée de l'ordinateur et du système d'exploitation 146

Les droits sur le développement d'un site web 147

JURISPRUDENCE Le cas des sous-traitants 148

Le nom de domaine 148

TECHNIQUE L'adresse URL 149

Jurisprudences sur les noms de domaine 150

6. Les transactions en ligne 153

RAPPEL Des débuts peu attirants 154

L'achat en ligne 154

NOUVEAU Les pharmacies en ligne 155

Identification du prestataire 156

PRÉCISION Le numéro de téléphone est-il vraiment obligatoire ? 156

Détail de l'offre 157

POLEMIQUE Les prix sont-ils vraiment plus intéressants sur Internet ? 157

DÉTAIL Les réclamations 158

Responsabilité du prestataire 158

PRÉCISION Les places de marché et les sites de vente entre particuliers 159

Délai de livraison 160

Garanties 160

La conclusion de l'achat 161

Information du consommateur 162

Cas du m-commerce 163

Droit de rétractation 163

EXCEPTIONS au droit de rétractation 164

JURISPRUDENCE Contrat d'assurance conclu à distance 165

Courriels publicitaires et offres promotionnelles 165

SANCTION Le spam 166

Après de qui se tourner en cas de litige ? 166

LE POINT DE VUE DU SPÉCIALISTE Marc Lohier, délégué général de la Fevad 167

Le paiement en ligne 169

PRÉCISION Faut-il déclarer son compte PayPal au fisc ? 169

Le paiement par carte bancaire 170

ZOOM Le cryptogramme visuel et le code PIN 170

PRÉCISION Le risque d'abus 171

SÉCURITÉ 3D Secure 172

JURISPRUDENCE Protection du client en cas d'usage du code PIN 173

Les ventes entre particuliers 174

Les obligations du vendeur particulier 175

JURISPRUDENCE Une moindre protection de l'acheteur 175

Le vendeur particulier doit-il déclarer ses ventes au fisc ? 175

Jurisprudences sur les ventes via eBay 176

Les sites de mise en relation 178

Les autres transactions financières en ligne 179

La banque en ligne 179

PRÉCISION La signature électronique 180

La monnaie électronique 181

Les jeux en ligne 181

7. Internet dans la vie professionnelle 183

L'usage d'Internet au bureau à titre personnel 184

PRÉCISION La liste des « favoris » dans le navigateur 185

Le filtrage des accès Internet 185

JURISPRUDENCES La consultation de sites pornographiques au bureau 186

L'accès de l'employeur aux fichiers et aux courriels 186

JURISPRUDENCE L'accès de l'employeur aux documents professionnels du salarié est un droit 188

Comment intituler les éléments personnels ? 189

JURISPRUDENCE Les dossiers « manifestement personnels » 189

L'accès de l'employeur aux documents personnels 190**Travailler chez soi ou avec son matériel ? 191****Le BYOD 191**

PRATIQUE Comment encadrer le BYOD ? 192

LE POINT DE VUE DU SPÉCIALISTE François Coupez, avocat à la Cour 193

Le télétravail 195

JURISPRUDENCE L'employeur ne peut pas imposer la cessation du télétravail 196

Comment parler de son employeur sur les réseaux sociaux ? 197**Diffamation publique de l'employeur 198**

CONCLUSION Facebook, espace public ou privé ? 199

QUESTION Quel droit de regard pour l'employeur sur les tweets personnels ? 200

Divulgateur d'informations confidentielles 200

JURISPRUDENCE Condamnation pour violation du contrat de travail 201

8. La cybercriminalité 203**Les attaques contre les systèmes informatiques 203**

HISTORIQUE La loi Godfrain (1988) 204

Accès ou maintien frauduleux dans un STAD 204

LA LOI L'article 323-1 du Code pénal 205

Condamnation des accès frauduleux, même à des fins ludiques ou de test 206

Condamnation des accès frauduleux à des fins répréhensibles 207

Condamnation pour copie d'un site web 209

LA LOI L'article 323-6 du Code pénal 209

L'accès à un système non sécurisé 210

À RETENIR Que conclure ? 211

La fraude scolaire 212

Entrave au fonctionnement d'un STAD 212

LA LOI L'article 323-2 du Code pénal 212

Condamnations pour entrave volontaire 213

Condamnations pour entrave involontaire 214

Modification frauduleuse des données d'un STAD 215

LA LOI L'article 323-3 du Code pénal 215

Condamnations pour attaques informatiques 216

La répression de la fraude informatique organisée 216

Peut-on chercher et publier des failles de sécurité ? 219

Le vol de données 219

Une qualification juridique incertaine 219

Une évolution des textes 222

Les attaques contre les internautes 223

Le phishing 223

LA LOI Article 313-1 du Code pénal 225

LA LOI Autres articles utiles 225

Condamnation pour escroquerie et accès frauduleux à un STAD 226

Condamnation pour contrefaçon 227

ZOOM Le recours au droit des marques est-il légitime ? 228

L'efficacité de l'arsenal juridique ? 228

Le spam 229

LA LOI L'article L34-5 du CPCE 230

La position de la Cnil 230

Signaler un spam 231

La répression du spam 232

Que faire face à une infraction informatique ? 234

Signaler une infraction 234

Déposer une plainte 235

Index 239

Avant-propos

Internet est-il soumis à un droit spécifique ? Contrairement à ce que l'on entend communément, on constate que le plus souvent, les lois « normales » s'y appliquent. Et c'est une bonne chose, car une loi efficace est une loi qui vaut partout et de tout temps, plutôt que d'être spécifique à un état de la technologie ou à une situation donnée. Par exemple, quand le juriste Ulpien, conseiller de l'Empereur à Rome il y a 1 800 ans, écrivait *Nemo videtur fraudare eos, qui sciunt et consentiunt* (on ne peut être accusé d'avoir trompé quelqu'un qui sait à quoi il s'engage et qui l'accepte), il définissait un principe que nous appliquons toujours lorsque, pour finaliser un achat ou un téléchargement en ligne, nous cochons la case « j'ai lu les conditions d'utilisation [*scio*] et je les accepte [*consentio*] ». Ayant lu et accepté, je renonce à pouvoir me plaindre ultérieurement au motif que les conditions ne me convenaient pas.

Cet ouvrage vise donc à rassembler tous les extraits de loi applicables et à les présenter de manière simple et pratique à l'internaute, car il n'est pas inutile de connaître ses droits et ses devoirs pour surfer en toute sérénité. L'internaute 2.0, celui qui télécharge et qui consomme, celui qui publie et qui met en ligne, celui qui interagit et qui réagit, trouvera dans les pages qui suivent les règles encadrant son activité.

Redécouvrir les concepts d'Internet

Le lecteur, même s'il est familiarisé avec Internet, trouvera ci-dessous un rappel des concepts de base indispensables pour appréhender l'interdépendance entre la technique et le droit.

Si l'on considère Internet comme un service, on peut identifier plusieurs types d'acteurs qui concourent à le produire. Tout d'abord, les fournisseurs d'accès à Internet (FAI) sont les opérateurs qui proposent l'accès physique au réseau : opérateurs télécoms, câblo-opérateurs, voire électriciens ou opérateurs satellite... Il s'agit de tous ceux qui ont des « tuyaux » permettant de se raccorder. Ils constituent le premier point de passage pour entrer dans le Web.

Une fois sur le Net, l'internaute va trouver des offreurs de services, qui peuvent être gratuits ou payants. Certains proposent l'accès à un contenu, que l'on va « consommer » : télévision, presse, information... D'autres réalisent des échanges dématérialisés et transposent sur le Web des transactions qui existaient déjà auparavant dans la « vie réelle » (e-commerce, e-administration, e-banque...). D'autres enfin donnent à l'internaute la possibilité de publier du contenu (photos, pages personnelles, commentaires...).

Rappel sur les abonnements à Internet

RAPPEL TECHNIQUE Le débit

Les contenus qui sont échangés sur Internet représentent une certaine quantité de données, exprimée en mégabits, un bit constituant l'information électronique élémentaire. Les bits sont groupés par huit, pour constituer des octets. Pour donner un ordre de grandeur, un fichier texte simple pèse quelques kilooctets (milliers d'octets) ; un CD avec une heure de musique pèse plusieurs centaines de mégaoctets (millions d'octets), un DVD avec un film quelques gigaoctets (milliards d'octets). Une clé USB contient également jusqu'à plusieurs gigaoctets.

Si l'on a une connexion Internet avec un débit de 50 Mbits/s, télécharger l'équivalent d'un CD musical devrait donc durer dix secondes. Et il faut compter dix fois plus longtemps pour télécharger un film.

Les abonnements proposent plusieurs niveaux de débit.

Le « haut débit » correspond à au moins 100 kilobits par seconde. Il présente l'avantage de passer par le réseau téléphonique et d'être donc disponible partout.

Ce débit étant néanmoins trop limité pour la télévision haute définition ou pour la navigation rapide, les opérateurs passent au « très haut débit » (au moins 30 Mbits/s). Cela nécessite de raccorder l'abonné avec de la fibre optique ou du câble. Le coût pour équiper toute la France se chiffre en dizaines de milliards d'euros, ce qui explique que seules les zones les plus rentables aient été raccordées en priorité. Une offre par satellite est également possible pour les zones mal desservies.

On distingue le débit descendant (de l'opérateur vers l'abonné) du débit montant. En effet, la situation est rarement symétrique : l'abonné a sans doute plus souvent besoin de recevoir chez lui de grosses quantités de données (télévision,

musique...) que d'en exporter de telles quantités. Le débit descendant est donc habituellement supérieur au débit montant.

Triple play, quadruple play

Les opérateurs peuvent proposer un abonnement réduit au seul accès Internet, mais en France prédomine le *triple play* (abonnement couplé Internet + télévision + téléphone fixe, le tout passant dans le même « tuyau »), voire le *quadruple play* (*idem* + téléphonie mobile).

Le 19 novembre 2009, la Cour de cassation a rappelé que les fournisseurs d'accès à Internet sont soumis à une obligation de résultat, sauf cas de force majeure imprévisible. Il leur incombe de vérifier que leur futur client est bien techniquement éligible à une offre avant de la leur proposer. Le fournisseur ne peut pas faire signer un contrat à son client, puis s'apercevoir après coup que le service n'est pas techniquement possible, et ce, même si le contrat prévoyait que l'offre était faite sous réserve de compatibilité technique.

Certains opérateurs comme Orange ou SFR, qui à l'origine sont des possesseurs de « tuyaux », se diversifient en proposant aussi des contenus, par exemple des chaînes de télévision exclusives.

ANALYSE JURISPRUDENCIELLE Droit des FAI à proposer des contenus exclusifs

La cour d'appel de Paris a validé le 14 mai 2009 le droit pour les FAI d'inclure dans leur offre, pour attirer les clients, des contenus exclusifs, qui ne sont donc pas accessibles aux abonnés des autres FAI. En effet, « dans le cadre de la concurrence qu'ils se livrent, tous les FAI s'efforcent d'enrichir le contenu de leurs offres pour les rendre plus attractives, par la mise en place de services innovants ou l'acquisition de droits exclusifs sur des contenus audiovisuels, cinématographiques ou sportifs événementiels. » Cette pratique, dénoncée par SFR et Free qui attaquaient le contrat entre Orange Sports et la Ligue de football professionnel pour la diffusion exclusive de certains matchs, est donc licite.

Du point de vue fiscal, les ordinateurs sont jusqu'à présent exclus du paiement de la contribution à l'audiovisuel public (la « redevance ») : en principe, ce sont les possesseurs de téléviseurs qui y sont assujettis, pas ceux d'un PC sans tuner, même s'il sert à regarder la télévision par Internet *via* une box ou une carte TV.

Toutefois, en 2014, le fisc a estimé qu'un moniteur directement relié à une box constituait un dispositif assimilé à une télévision, et devait donc payer la redevance.

Rappelons que le fisc a accès aux fichiers des abonnés *triple play*.

Internet mobile

En quelques années, l'accès à Internet par mobile s'est généralisé et banalisé. Il y a désormais autant, sinon plus, de mobinautes que d'internautes. L'apparition d'abonnements à bas prix et sans plafond d'usage (Internet « illimité ») n'a pas peu contribué à cette démocratisation.

Or, le passage d'Internet par le mobile (et surtout des applications très demandeuses de ressources comme la télé ou la vidéo) consomme énormément de canaux radio, alors que le spectre radio disponible est très restreint. En clair, il n'y a pas assez de place sur les ondes pour que tous puissent naviguer simultanément avec un haut débit.

Les opérateurs travaillent à une amélioration de leur débit radio (passage à la nouvelle génération d'appareils « 4G »), mais cette augmentation risque de demeurer inférieure à celle du trafic due à l'explosion simultanée du nombre des utilisateurs et de l'usage de la vidéo mobile. Les embouteillages sur les ondes ont de l'avenir.

En conséquence, les opérateurs sont tentés de restreindre les usages de leurs clients et de brider le caractère « illimité » de leur offre. Cette limitation peut se faire dans la durée

(maximum mensuel autorisé) ou en instantané (maximum de débit instantané offert).

DRÖIT DES CONSOMMATEURS

Qu'est-ce qu'un abonnement illimité ?

En 2010, l'association de défense des consommateurs UFC-Que Choisir a assigné en justice Orange et SFR pour pratiques commerciales trompeuses. Elle leur reprochait « d'utiliser dans leurs publicités la notion d'Internet illimité, alors que dans la pratique le service fourni n'est pas illimité parce qu'il y a des restrictions d'usage ». Ces restrictions étaient précisées en très petits caractères dans les contrats d'abonnement. En 2012, le tribunal de grande instance de Paris n'a pas tranché sur le fond, mais a estimé que puisque les publicités en cause n'étaient plus diffusées, l'action de l'UFC n'était plus fondée.

L'UFC a de nouveau attaqué les opérateurs en juin 2012, cette fois pour « clauses abusives » dans les contrats d'abonnement à l'Internet mobile. L'UFC leur reproche notamment « l'usage des services encore trop souvent limité par des notions floues telles que mauvaise utilisation, utilisation abusive, excessive, envoi en masse ».

Il est donc vivement conseillé de bien analyser son contrat d'abonnement avant de le souscrire et de vérifier que l'usage d'Internet qui y est autorisé correspond bien à ses besoins !

La neutralité du Net

À la base, le fonctionnement d'Internet repose sur un protocole appelé TCP-IP (*Transmission Control Protocol/Internet Protocol*), dont le principe, inventé par le Français Louis Pouzin dans les années 1970, est le suivant : toutes les informations à échanger sur le réseau sont découpées en « paquets » de taille standard, qui sont envoyés sur le réseau de manière indépendante (ils empruntent éventuellement des chemins différents) et sont réassemblés à leur point de destination pour reconstituer l'information de départ. C'est cette standardisation de tous les types d'information qui fait qu'Internet peut transmettre aussi bien du texte que de la voix ou de l'image.

Internet s'est construit sur le principe que l'on pourrait résumer par « tous les paquets naissent et demeurent libres et égaux », c'est-à-dire que le système n'a pas à connaître le contenu des paquets ni à les hiérarchiser, il doit tous les traiter de manière indistincte et uniforme. Cela s'appelle « la neutralité du Net ».

Définition La neutralité du Net

Selon Wikipédia, « la neutralité du Net exclut toute discrimination à l'égard de la source, de la destination ou du contenu de l'information transmise sur le réseau. Ainsi, ce principe garantit que les utilisateurs ne feront face à aucune gestion du trafic Internet qui aurait pour effet de limiter leur accès aux applications et services distribués sur le réseau. La neutralité du Net assure que les flux d'information ne sont ni bloqués, ni dégradés, ni favorisés par les opérateurs de télécommunications, permettant ainsi aux utilisateurs d'utiliser librement l'architecture communicationnelle.

Lors des Rencontres mondiales du logiciel libre de 2009, Benjamin Bayart, pionnier de l'Internet en France, a ainsi proposé quatre principes essentiels à la neutralité du Net :

- transmission des données par les opérateurs sans en examiner le contenu ;
- transmission des données sans prise en compte de la source ou de la destination des données ;
- transmission des données sans privilégier un protocole de communication ;
- transmission des données sans en altérer le contenu. »

Ce principe de neutralité trouve ses limites dans plusieurs types de situation.

- On a mentionné plus haut les risques d'engorgement de l'Internet mobile, qui existe aussi pour l'Internet fixe : les « tuyaux » ne sont pas suffisants pour garantir à chacun, partout et tout le temps, un accès en très haut, ou même en haut débit. Or, certaines applications sont par nature prioritaires sur les autres : téléphonie sur IP (type Skype) ou télé-médecine ont évidemment besoin d'un passage en temps réel, tandis que le téléchargement d'un film peut souffrir quelques minutes de retard.

- Par ailleurs, les clients qui téléchargent beaucoup de vidéos accaparent une grande partie des ressources, au détriment des autres abonnés dont ils ralentissent le débit. Il serait équitable, soit d'allouer le même débit à tous, soit de facturer plus cher ceux qui utilisent plus les infrastructures.
- Les opérateurs sont également soupçonnés de favoriser les connexions à certains services avec lesquels ils ont des accords de partenariat, et de ralentir au contraire les connexions vers les services concurrents.
- Enfin, les autorités voudraient lutter contre la cybercriminalité en repérant et en bloquant certains types de contenus (pédopornographie, incitation au terrorisme...). Cela nécessite de « lire » tous les paquets qui transitent sur le réseau (technologie dite de *Deep packet inspection*, DPI).

Un équilibre doit donc être trouvé entre, d'une part, le principe de neutralité et, d'autre part, les contraintes de gestion des réseaux, les intérêts financiers des opérateurs, ainsi que la lutte contre la criminalité. Les défenseurs de la neutralité du Net souhaitent que celle-ci soit garantie par une inscription dans le cadre législatif. En France, une proposition de loi a été déposée en ce sens en 2012 par la députée Laure de la Raudière. Quant au Parlement européen, il a adopté en première lecture, en avril 2014, un projet de règlement définissant la neutralité du Net. Pour être promulgué, ce texte devra désormais faire l'objet d'un accord avec la Commission européenne et le Conseil de l'Union.



Fig. 1 > Qu'est-ce que la neutralité du Net ?
Sébastien Desbenoit CC BY 3.0

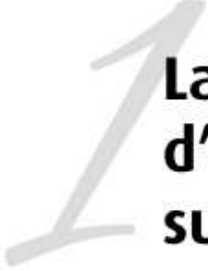
Le financement du Net

Certaines des atteintes au principe de neutralité du Net trouvent leur origine dans le besoin de financement des infrastructures : en effet, les opérateurs doivent investir toujours plus pour proposer à leurs clients des débits plus élevés,

mais les revenus des abonnements ne couvrent pas les investissements nécessaires, tandis que les grands bénéficiaires de la hausse du débit sont les acteurs du Web proposant du contenu qu'ils monétisent par de l'abonnement, du paiement à l'usage (par exemple pour la vidéo à la demande) ou par de la publicité. Pouvoir identifier les paquets permettrait aux opérateurs de faire contribuer financièrement les services web bénéficiaires (paiement en fonction du nombre de paquets émis, ou partenariat global pour une transmission « prioritaire »).

Une autre solution pour faire contribuer les services web au financement des infrastructures serait de lever une taxe sur leurs revenus. L'idée d'une « taxe Google », assise par exemple sur les revenus publicitaires, est en discussion depuis quelques années.

Neutralité du Net et taxation des acteurs web font l'objet de nombreux débats, tant au niveau français qu'au niveau international.



La liberté d'expression sur Internet

*Peut-on tout dire et écrire sur Internet ? Quelles
sont les règles à respecter, quels sont les recours en
cas de problème ?*

Sur Internet, chacun peut enfin s'exprimer et faire connaître au monde entier ses pensées profondes et l'intensité de sa vie privée et sociale. Protégé par l'anonymat de son écran, l'internaute peut-il écrire et publier n'importe quoi ? Bien sûr que non, la liberté n'est pas absolue et des règles sont à respecter, pour se protéger et pour protéger les autres.

La liberté d'expression, un droit fondamental, mais pas absolu

La liberté d'expression a été consacrée en France par la Révolution, lors de la proclamation de la Déclaration des droits de l'homme et du citoyen en 1789. Les articles 10 et 11 de cette Déclaration prévoient ainsi que :

« Nul ne doit être inquiété pour ses opinions, même religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la Loi »,

et que :

« La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté, dans les cas déterminés par la Loi. »

On voit qu'il ne s'agit pas d'une liberté absolue, mais que des limites doivent être respectées. L'article 4 de la Déclaration expliquait ainsi que :

« La liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société, la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi. »

En l'occurrence, la loi du 30 septembre 1986 relative à la liberté de communication précise, pour ce qui concerne l'expression sur Internet :

« La communication au public par voie électronique est libre. L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et

d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale. »

QUI EST CONCERNÉ SUR INTERNET ? **Tout le monde !**

La loi précise que la « communication au public par voie électronique » désigne « toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée ».

Sont donc visés aussi bien les publications commerciales comme les journaux, que les sites politiques ou commerciaux, ou enfin les blogs, sites personnels, commentaires de lecteurs, sites de partage et réseaux sociaux. L'auteur de la publication peut être aussi bien un professionnel (journaliste, commercial) qu'un internaute.

Seuls les courriels, qui constituent une correspondance privée, ne sont pas concernés, à la condition d'être bien « privés » et adressés à un nombre restreint de destinataires, et non pas envoyés globalement à une liste de diffusion.

L'internaute français qui s'exprime en ligne, sur un réseau social, sur un blog ou sur un forum, peut donc profiter de sa liberté d'expression dans les limites prévues par la loi. Ces limites concernent notamment l'injure et la diffamation, le respect de la vie privée d'autrui, l'interdiction des propos racistes, sexistes, homophobes, ou incitant à la violence...

CONFLIT DE DROITS **La liberté d'expression dans la loi américaine**

Comme on le sait, la loi américaine est fondamentalement différente. Le 1^{er} amendement à la Constitution des États-Unis, adopté en 1791, interdit toute restriction à la liberté religieuse, à la liberté d'expression ou à la liberté de la presse.

Lors d'un litige concernant l'utilisation de services américains comme Facebook ou Twitter, l'internaute français risque de se retrouver au centre d'un conflit dû à l'incompatibilité entre le droit américain (liberté absolue d'expression) et le droit français (liberté d'expression encadrée).

Toutefois, le 5 mars 2015, le tribunal de grande instance de Paris s'est estimé compétent pour juger un litige entre Facebook et un de ses utilisateurs.

Les abus dont la loi vous protège

Une fois posé le principe de la liberté d'expression, il reste à voir en pratique dans quelles limites il s'applique.

Cas général et cas particulier

Nous allons exposer dans la suite les règles générales qui encadrent la *liberté d'expression* de l'internaute. Certaines règles supplémentaires peuvent s'appliquer dans des cas particuliers. Par exemple, le Code monétaire et financier interdit la manipulation des cours de bourse par diffusion volontaire de *fausses informations*. L'Autorité des marchés financiers a ainsi condamné le 7 novembre 2013 deux professionnels à des amendes de 10 000 € et de 8 000 € pour avoir publié sur leurs blogs des informations erronées sur une banque, perturbant ainsi les marchés financiers. La protection de la *vie privée* par le Code civil constitue également un moyen puissant. Le tribunal de grande instance de Paris a ainsi condamné le 6 novembre 2013 Google, au nom du droit à la vie privée, à cesser l'affichage sur Google Images de photos divulguant la vie sexuelle d'un dirigeant des circuits de course automobile.

La diffamation et l'injure

La loi du 29 juillet 1881 sur la liberté de la presse précise les règles à respecter pour tout type de publication, y compris « tout moyen de communication au public par voie électronique » (art. 23), c'est-à-dire Internet, qu'il s'agisse des sites web ou des listes de diffusion par courriel.

LA MISE À JOUR DES LOIS La loi de 1881 modifiée

Il ne faut pas s'étonner de voir les publications sur Internet prévues et encadrées par une loi de 1881. En effet, les lois peuvent être régulièrement mises à jour par le Parlement. Si elles ont une importance symbolique, comme la loi de 1881 sur la presse, elles conservent leur titre d'origine, mais sont dites « modifiées ». En l'occurrence, c'est une loi de 2004 pour la confiance dans l'économie numérique (LCEN) qui a inséré dans celle de 1881 la référence à la « communication au public par voie électronique ».

Les jurisprudences pour violation de la loi de 1881 abondent pour la presse traditionnelle, mais on ne citera dans la suite que celles concernant des infractions commises en ligne.

La diffamation est ainsi définie par la loi (art. 29) : « Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible. »

Il faut distinguer la diffamation de l'injure, qui est « toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait ».

DÉFINITIONS **Allégation, imputation, invective**

Allégation : synonyme d'affirmation.

Imputation : action de mettre une action blâmable sur le compte de quelqu'un.

Invective : paroles violentes contre quelqu'un.

Les peines encourues sont les suivantes (art. 30 à 33) :

- diffamation envers un particulier : amende de 12 000 euros maximum ;
- diffamation envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, ou à raison de leur sexe, de leur orientation sexuelle ou de leur handicap : un an d'emprisonnement et/ou 45 000 euros d'amende, ainsi que la publication de la décision dans les journaux aux frais du condamné ;
- diffamation envers les tribunaux, les armées, les administrations, ou, à raison de leurs fonctions, envers les membres du

- gouvernement, parlementaires, fonctionnaires et dépositaires de l'autorité publique : amende de 45 000 euros maximum ;
- injure envers les corps et personnes cités à l'alinéa précédent, ou envers un particulier, lorsqu'elle n'aura pas été précédée de provocations : amende de 12 000 euros maximum ;
 - injure envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée, ou à raison de leur sexe, de leur orientation sexuelle ou de leur handicap, lorsqu'elle n'aura pas été précédée de provocations : six mois d'emprisonnement et 22 500 euros d'amende, ainsi que la publication de la décision aux frais du condamné.

EN DÉTAIL Les jurisprudences

Les jurisprudences sont l'ensemble des décisions des tribunaux, représentatives de la manière dont ils jugent habituellement une question. Leur étude permet de présumer quelle réponse ils donneront dans un cas précis.

Toutefois, la jurisprudence n'est jamais définitive. D'une part, une nouvelle loi peut imposer un changement dans les décisions ; d'autre part, un tribunal, qui a le pouvoir souverain de juger, peut toujours décider de modifier sa jurisprudence.

RAPPEL La hiérarchie des tribunaux

Un litige judiciaire est jugé par un tribunal en première instance (tribunal d'instance [TI] ou de grande instance [TGI]).

Si la décision ne satisfait pas l'une des parties, celle-ci peut faire appel et le litige sera rejugé sur le fond par une cour d'appel (CA).

L'arrêt d'appel ne peut plus être rejugé, sauf s'il comporte un vice de procédure. La partie lésée doit alors introduire un pourvoi auprès de la Cour de cassation. Cette dernière est la juridiction suprême qui peut être saisie pour vérifier si un jugement a bien été rendu dans le plein respect de la loi. Elle ne juge pas sur le fond, mais examine seulement si la cour d'appel a bien appliqué le droit. Si elle estime que ce n'est pas le cas, elle

casse l'arrêt d'appel et renvoie le dossier devant une nouvelle cour d'appel pour un nouveau jugement sur le fond. L'étude des décisions de la Cour de cassation est importante car lorsque les textes de loi sont obscurs ou incomplets, elles contiennent des explications sur la manière dont il faut comprendre la loi. La jurisprudence de la Cour de cassation s'impose à tous les autres tribunaux : ils sont obligés de tenir compte de son interprétation, sous peine de voir leurs décisions systématiquement cassées.

À signaler : depuis 2008, dans le cadre d'un procès, il est possible, pour une personne estimant que la loi applicable est contraire à la Constitution, de déposer une question prioritaire de constitutionnalité (QPC). Si cette question est validée par le Conseil d'État ou par la Cour de cassation, elle est transmise au Conseil constitutionnel. L'examen du litige est alors suspendu dans l'attente de la réponse du Conseil.

Les jurisprudences suivent la hiérarchie des tribunaux : les décisions du Conseil constitutionnel fixent la loi, la jurisprudence de la Cour de cassation s'impose à toutes les juridictions ; les jurisprudences des cours d'appel s'imposent à leurs tribunaux subalternes.

Diffamation ou injure, il faut choisir

On a vu que les définitions de l'injure et de la diffamation étaient différentes : la diffamation suppose d'invoquer un fait précis, pas l'injure. Des propos ne peuvent donc pas constituer à la fois une injure et une diffamation : soit ils font référence à un fait, soit non.

Le 15 février 2013, la Cour de cassation a donc confirmé l'annulation d'une plainte portant sur des propos répétés tenus sur un forum de discussion et que le plaignant qualifiait à la fois d'injure et de diffamation. La Cour a considéré que cette incertitude sur le motif de la plainte était préjudiciable à la défense. Cette position a logiquement été suivie par le tribunal de grande instance de Paris, le 14 janvier 2014, pour repousser une plainte portant sur des propos qualifiés à la fois de diffamation et d'injure.

Diffamation et injure publiques envers des personnes

En bref Les différentes sanctions financières

Lorsqu'une personne est condamnée par un tribunal, elle peut se voir infliger trois types de sanctions financières :

- l'**amende**, encaissée par l'État, sanctionne la violation de la loi. Son montant est proportionnel à la gravité de l'infraction ;
- les **dommages-intérêts**, versés à la victime, visent à réparer le préjudice qui lui a été causé ; ils sont déterminés par le juge au cas par cas ;
- le **remboursement** à la victime de tout ou partie de ses **frais de justice**.

L'amende est une punition, tandis que les dommages-intérêts et le remboursement des frais sont une réparation du dommage causé.

La publication de la décision, aux frais du condamné, dans des journaux ou sur des sites web, vient renforcer la réparation du dommage causé, en contribuant à restaurer publiquement la victime dans ses droits et dans sa réputation.

Le 7 octobre 2009, la cour d'appel de Paris a confirmé la condamnation d'un ancien salarié d'une société, qui avait envoyé aux dirigeants du groupe des courriels injurieux, à 1 euro de dommages-intérêts, auquel elle a ajouté 3 000 euros pour chaque victime au titre des frais.

Le 15 novembre 2012, le tribunal de grande instance de Bobigny a condamné à 1 000 euros d'amende avec sursis et 1 euro de dommages-intérêts une personne qui, après son licenciement, s'était vengée de son ancien supérieur hiérarchique en créant une fausse page Viadeo à son nom, contenant des propos diffamatoires.

Le 12 février 2013, le tribunal correctionnel de Paris a condamné pour diffamation et injure à 400 euros d'amende avec sursis et à 1 euro de dommages-intérêts, un internaute qui avait créé une page Facebook insultant le docteur Delajoux, médecin de Johnny Hallyday, lequel était accusé d'avoir mal soigné son illustre patient.

EN DÉTAIL Le sursis

Lorsqu'une personne est condamnée pour la première fois, le tribunal peut décider d'assortir la peine d'un sursis, c'est-à-dire que cette peine ne sera pas mise à exécution, sauf si la personne récidive dans un délai de cinq années.

Si la personne commet à nouveau la même infraction au cours de cette période, elle encourt une nouvelle condamnation qui cette fois sera ferme (mise à exécution). En outre, cette nouvelle condamnation fera tomber le sursis de la première, c'est-à-dire que celle-ci sera également mise à exécution et viendra s'ajouter à la deuxième.

La diffamation est moralement condamnable et son auteur peut être sanctionné autrement que par un tribunal. En mars 2013, trois jeunes filles ont été définitivement exclues de leur lycée à Limay (Yvelines), pour avoir émis des tweets insultants pour leur professeur de français. Suite à cette décision, des tweets diffamatoires pour le lycée ont été émis. La proviseur a alors déposé plainte contre X pour diffamation.

Et envers l'employeur ?

De nombreux litiges ont opposé des entreprises à certains de leurs salariés qui avaient publié sur Facebook des propos ressentis par leur employeur comme diffamatoires. À chaque fois, les salariés, licenciés, ont contesté leur licenciement.

Voir le chapitre 7, « Internet dans la vie professionnelle ».

Et envers la police ?

Le 14 octobre 2011, suite à la plainte du ministre de l'Intérieur pour injure et diffamation envers la police et l'administration, le tribunal de grande instance de Paris a ordonné en référé aux principaux fournisseurs d'accès Internet français d'empêcher l'accès au site Copwatch, dans l'attente du jugement définitif.

Procédure Le référé

Le référé est une procédure rapide et simplifiée par laquelle on demande à un juge de prendre des mesures pour prévenir un dommage imminent ou pour faire cesser un trouble manifestement illicite (par exemple : la publication de photos pédophiles), sans préjuger du jugement sur le fond qui aura lieu ultérieurement.

Et les injures privées ?

La Cour de cassation a confirmé le 10 avril 2013 que si des propos injurieux sont diffusés sur un réseau social, mais accessibles seulement à un nombre restreint de personnes, alors il ne s'agit pas de propos publics, mais de propos privés : « les propos litigieux [qui] avaient été diffusés [...] tant sur le site Facebook que sur le site MSN, lesquels n'étaient en l'espèce accessibles qu'aux seules personnes agréées par l'intéressée, en nombre très restreint [...] ne constituaient pas des injures publiques ». Ils ne relèvent donc pas de la loi de 1881 qui ne vise que les propos publics.

Toutefois, la Cour ajoute que dans un tel cas de figure l'auteur des injures n'en est pas quitte pour autant : il est passible des sanctions de l'article R621-2 du Code pénal qui réprime les injures non publiques, soit une amende de 38 euros.

La codification

Afin de faciliter la pratique du droit, les différents textes, lois et décrets relatifs à un même domaine peuvent être rassemblés dans des codes, le premier et le plus célèbre étant le Code civil édité sur l'ordre de Napoléon.

Les codes sont généralement divisés en deux parties :

- la partie législative qui rassemble les textes de lois, et dont les articles sont parfois désignés par la lettre L ;
- la partie réglementaire qui rassemble les décrets pris en application de ces lois. Lorsqu'il s'agit de décrets en Conseil d'État, les articles sont désignés par la lettre R ; lorsqu'il s'agit de décrets simples, c'est la lettre D qui est utilisée.

Jurisprudences concernant Google Suggest

Sur Google, lorsqu'un internaute saisit les premières lettres de sa recherche, la fonctionnalité Google Suggest lui propose une liste de requêtes possibles le dispensant d'avoir à taper le libellé complet de sa recherche. Certaines personnes voient ainsi accolés à leur nom des termes peu flatteurs et attaquent Google. C'est alors au tribunal de juger du caractère illicite ou non de la suggestion.

Dans une de ces affaires, cette fonctionnalité accolait au nom d'une personne le mot « secte ». La personne concernée, estimant qu'il s'agit d'une injure, a saisi la justice pour lui demander d'obliger Google à supprimer cette suggestion et de le condamner à 12 000 euros d'indemnité. Le 31 octobre 2012, le tribunal de grande instance de Paris a jugé que le mot « secte », s'il comportait certes une connotation péjorative et s'il pouvait être perçu comme infamant concernant une organisation, ne pouvait cependant constituer une injure selon la définition de la loi de 1881, relativement à une personne physique. Le demandeur a donc été débouté.

Dans un autre cas, Google Suggest accolait les mots « violeur », « prison » et « sataniste » au nom d'une personne. Celle-ci avait donc attaqué Google en diffamation et demandé la suppression des suggestions litigieuses. Le 19 février 2013, la Cour de cassation a confirmé l'arrêt de la cour d'appel de Paris (14 décembre 2011), qui reconnaissait l'aspect diffamatoire de la suggestion, mais qui a accordé à Google l'excuse de la bonne foi, la suggestion résultant d'un algorithme sans que le directeur de la publication (en l'occurrence le directeur de Google) en soit conscient, et les liens suggérés par Google renvoyant à des articles publics relatifs à la condamnation du demandeur pour des faits de viol.

Le 12 juin 2013, le tribunal de grande instance de Paris a refusé une plainte contre Google Suggest sur la base de la loi Informatique et Libertés, au motif que Google Suggest ne

constituait pas un « fichier » au sens de cette loi. Cette décision nous semble procéder d'une mauvaise interprétation de la loi ; en effet, Google Suggest n'est sans doute pas un « fichier », mais il constitue certainement un « traitement automatisé de données personnelles », ce qui relève bien de la loi Informatique et Libertés. En revanche, cette dernière n'étant applicable que pour les traitements effectués sur le territoire français, et Google Suggest étant basé en Californie, cela pouvait constituer une raison légale de ne pas appliquer la loi Informatique et Libertés à Google. Le tribunal pouvait donc estimer que Google Suggest n'était pas soumis à cette loi, mais il se trompait sur la cause : c'est la localisation géographique de Google qui justifierait cette exemption, et non le fait que Google Suggest ne soit pas un fichier (voir le chapitre 3 traitant des données personnelles).

Enfin, le 23 octobre 2013, le tribunal de grande instance de Paris a estimé que la loi de 1881 ne s'appliquait pas à Google Suggest, car cette loi encadre la liberté d'expression, faculté humaine, et non les résultats délivrés automatiquement par un algorithme. En revanche, il a condamné Google sur la base de la responsabilité civile (articles 1382 et 1383 du Code civil) à verser 4 000 € de préjudice moral à une personne au nom de laquelle Google Suggest accolait les mots « escroc » et « secte » : Google est selon le tribunal responsable des dommages causés par son algorithme.

Twitter

Nous avons jusqu'ici considéré uniquement les publications de contenus sur Internet. Mais les mêmes règles s'appliquent sur Twitter.

Le tribunal de commerce de Paris a ainsi condamné le 26 juillet 2011 à 10 000 euros de dommages-intérêts le dirigeant d'une société qui avait dénigré les services d'un prestataire dont il était mécontent sur Twitter.

En 2013, la chaîne de restauration Quick a porté plainte pour diffamation contre un employé qui se plaignait dans des tweets de présumées mauvaises conditions de travail dans son établissement.

En mai 2014, la Fédération française de football et son sélectionneur ont porté plainte pour injure publique contre la compagne d'un joueur qui avait publié un tweet insultant à leur encontre.

QUESTION Les retweets

Lorsque l'on a un compte sur Twitter, on a la possibilité de « retweeter » un message, c'est-à-dire de faire suivre à ses abonnés un tweet qui nous a particulièrement plu ou marqué. Or ce tweet peut avoir un contenu illicite (diffamant, injurieux ou autre), que l'on répand sans obligatoirement s'en rendre compte, voire parfois pour montrer que l'on en est choqué.

La question se pose, juridiquement, de savoir si le fait de retweeter équivaut à une nouvelle publication du contenu, et à une approbation de celui-ci ? Et le cas échéant, expose-t-il aux mêmes sanctions que celles encourues par l'auteur du message initial ?

Par prudence, il conviendra de bien réfléchir, non seulement avant de tweeter, mais également avant de retweeter !

Des délits que l'on souhaite rares...

Le délit d'incitation

L'article 24 de la loi de 1881 prévoit que l'appel « à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une ethnie, une nation, une race ou une religion déterminée », ou « à raison de leur sexe, de leur orientation sexuelle ou de leur handicap », est puni d'un an d'emprisonnement et de 45 000 euros d'amende. Le tribunal peut ordonner la publication de la décision aux frais du condamné.

Recherche des auteurs de tweets antisémites

Par son ordonnance de référé du 24 janvier 2013, le tribunal de grande instance de Paris a ordonné à Twitter de communiquer à des associations de lutte contre le racisme les données en sa possession permettant l'identification de personnes ayant émis des tweets antisémites, en vue de déposer plainte contre ces dernières. Twitter a tout d'abord refusé de s'exécuter, mais en juillet 2013, devant la menace d'un procès pénal pour ses dirigeants, il a finalement fourni à la justice française les éléments demandés.

Condamnation du responsable d'un blog sur lequel des commentaires racistes ont été publiés

Le 30 octobre 2012, la Cour de cassation a confirmé la condamnation à 5 000 euros d'amende, à la publication de la sanction et à 2 750 euros de dommages-intérêts, d'un internaute qui tenait un blog d'information politique sur lequel des commentaires racistes avaient été publiés. La Cour a ajouté à la sanction 2 500 euros à verser à la Ligue internationale contre le racisme et l'antisémitisme en remboursement des frais engagés.

Le même internaute a été condamné en juin 2014 par le tribunal correctionnel de Strasbourg à 3 000 euros d'amende et 500 euros de dommages-intérêts pour publication sur Facebook de propos diffamatoires visant une adversaire politique.

Condamnation des auteurs de pages incitant à la violence contre un handicapé

Le 31 janvier 2013, le tribunal de grande instance de Paris a condamné respectivement à 40 heures de travaux d'intérêt général et à 300 euros d'amende deux jeunes qui avaient créé des pages Facebook appelant à l'euthanasie d'un jeune handicapé nommé désigné. Les deux jeunes devront également verser aux parents de l'enfant handicapé l'euro symbolique de dommages-intérêts et leur rembourser les frais d'huissier.

Condamnations pour incitation à la haine et à la discrimination raciale

Le 28 novembre 2013, la cour d'appel de Paris a condamné à 28 000 euros d'amende l'ancien humoriste Dieudonné, pour des propos et une chanson racistes dans des vidéos publiées sur Internet.

Le 22 avril 2014, deux internautes ont été condamnés par le tribunal correctionnel d'Amiens à cinq mois de prison ferme et 1 000 euros d'amende, pour avoir diffusé sur Internet une vidéo contenant des injures publiques et des provocations à la haine raciale.

Condamnation pour tweets homophobes

Le 20 janvier 2015, le tribunal correctionnel de Paris a condamné les auteurs de tweets homophobes à des amendes allant de 300 euros avec sursis à 500 euros fermes, et à des dommages-intérêts équivalents à verser à une association.

L'apologie de crimes de guerre ou de crimes contre l'humanité, l'appel au terrorisme

L'article 24 de la loi de 1881 punit de cinq ans d'emprisonnement et de 45 000 euros d'amende :

- l'apologie des crimes de guerre ;
- l'apologie des crimes contre l'humanité ;
- l'apologie des crimes et délits de collaboration avec l'ennemi.

Le tribunal peut ordonner la publication de la décision aux frais du condamné.

Jusqu'à récemment, l'appel au terrorisme ou son apologie étaient également réprimés par ce même article 24 de la loi de 1881. Depuis la loi du 13 novembre 2014, cette infraction fait l'objet de l'article 421-2-5 du Code pénal, et est punie de cinq ans d'emprisonnement et 75 000 euros d'amende, portés à sept ans et 100 000 euros si les faits ont été commis sur

Internet. Cette modification a notamment pour conséquence de porter la prescription de ce délit à trois ans (voir ci-après).

Définitions Apologie et négationnisme

Apologie : discours de justification.

Négationnisme : négation, contestation ou minimisation de crimes contre l'humanité.

Peines de prison ferme pour apologie et appel au terrorisme

Sous le régime de la loi de 1881, l'administrateur d'un site web djihadiste a été condamné le 4 mars 2014 par le tribunal correctionnel de Paris à trois ans de prison, dont un ferme, pour apologie et provocation au terrorisme.

Sous le régime du Code pénal, en janvier 2015, plusieurs condamnations à des peines de prison ferme allant jusqu'à deux ans ont été prononcées à l'encontre de personnes ayant publié sur Facebook des apologies des attentats survenus à Paris du 7 au 9 janvier 2015.

Condamnation pour article justifiant un massacre

Le tribunal de grande instance de Tulle a condamné le 9 septembre 2008 à cinq mois de prison ferme et à plusieurs milliers d'euros de dommages-intérêts une personne qui avait publié sur son blog une justification du massacre de Tulle en 1944 (99 personnes pendues et 101 déportées par les Allemands), ce qui constitue le délit d'apologie de crimes de guerre.

Le négationnisme

La loi Gayssot du 13 juillet 1990 « tendant à réprimer tout acte raciste, antisémite ou xénophobe » rappelle que « toute discrimination fondée sur l'appartenance ou la non-appartenance à une ethnie, une nation, une race ou une religion est interdite ». Cette loi a en particulier introduit dans la loi de 1881 un article 24 bis qui interdit également la contestation

des crimes contre l'humanité. Les coupables encourrent un an de prison et 45 000 euros d'amende.

Cet article se distingue du précédent : l'article 24 réprime l'apologie des crimes contre l'humanité, tandis que l'article 24 bis réprime la contestation de leur existence.

Le formalisme

La procédure à respecter

Pour engager une procédure sur la base de la loi de 1881, il est impératif de respecter la procédure prévue par l'article 53 de cette loi, qui prévoit que la plainte doit préciser chaque fait incriminé (bien spécifier où se trouve le contenu litigieux, quel est le passage visé...), et qualifier ce fait (voir par exemple ci-dessus le débat « diffamation ou injure »...).

Pour n'avoir pas respecté ce formalisme, le procureur de la République de Toulouse a été débouté le 11 avril 2014 par le tribunal de grande instance de cette ville, lorsqu'il a voulu demander le blocage d'un site web antisémite et négationniste.

En outre, il est impératif de respecter le délai de prescription (voir ci-après).

La possibilité de prouver les faits (exception de vérité)

Une personne accusée de diffamation a la possibilité de se disculper en prouvant la véracité des faits diffamatoires (article 35 de la loi de 1881), sauf lorsque l'imputation concerne la vie privée de la personne visée.

Jusqu'à récemment, d'une part il était interdit d'apporter une preuve pour des faits datant de plus de dix ans (article 35b de la loi de 1881), et d'autre part toute mention d'une condam-

nation amnistiée, prescrite ou réhabilitée était considérée comme une diffamation, même si ces faits étaient véridiques et que l'on en apportait la preuve (article 35c).

La Cour de cassation a rappelé, le 16 mai 2013, qu'il était interdit de mentionner ou de porter à la connaissance du public des délits commis par des hommes politiques en 1965, même si cette mention était faite par un journaliste de bonne foi dans l'objectif d'informer ses lecteurs.

Toutefois, le Conseil constitutionnel, saisi de questions prioritaires de constitutionnalité (QPC), a estimé que les interdictions de pouvoir apporter une preuve pour des faits de plus de dix ans (décision du 20 mai 2011) ou pour des condamnations amnistiées, prescrites ou réhabilitées (décision du 7 juin 2013) portaient à la liberté d'expression une atteinte disproportionnée et étaient donc contraires à la Constitution.

La seule limite à l'exception de vérité (*exceptio veritatis*) demeure donc la vie privée de la personne visée.

Précision **L'intention malveillante**

Notons toutefois que la publication de faits portant atteinte à l'honneur, même véridiques, demeure répréhensible si elle est effectuée dans un but malveillant. La cour d'appel de Versailles a ainsi condamné le 17 octobre 2013 à 1 000 euros d'amende et 1 000 euros de dommages-intérêts une personne qui avait publié la condamnation pour violence d'un ancien associé devenu son concurrent. Bien que la condamnation en question soit parfaitement véridique, la cour a estimé que c'était l'intention de nuire, et non la seule information du public, qui avait motivé cette publication.

Délai de prescription et droit de réponse

Un délai trop court ?

DÉFINITION Le délai de prescription

Il s'agit du délai au-delà duquel on ne peut plus poursuivre une infraction en justice. La durée de ce délai dépend de la nature de l'infraction : plus celle-ci est grave, plus le délai est long. Les crimes contre l'humanité sont imprescriptibles : les criminels peuvent être poursuivis jusqu'à leur mort.

Selon l'article 65 de la loi de 1881, le délai de prescription pour le non-respect de cette loi est de trois mois révolus.

Ce délai de trois mois se comprenait aisément pour la presse papier : un article sur papier a complètement disparu des kiosques après un tel délai. En revanche, sur Internet, un texte reste en ligne indéfiniment. Cela incite à réfléchir à une prescription différente pour les diffamations sur Internet. Le débat, qui avait eu lieu au Parlement lors du vote de la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), avait abouti au maintien de la durée de trois mois, pour des raisons d'égalité entre les supports papier et électronique.

Toutefois, le délai de prescription a été porté à un an (article 65-3) pour les infractions concernant le négationnisme tel que défini précédemment, ainsi que pour les différentes infractions (discrimination, appel à la haine ou à la violence, diffamation, injure...) commises à l'encontre d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance à une

ethnie, une nation, une race ou une religion déterminée, de leur sexe ou orientation sexuelle, ou de leur handicap.

Le Conseil constitutionnel a validé le 12 avril 2013 cette différence de délai de prescription concernant certaines infractions, cette mesure ayant pour objet de faciliter la poursuite et la condamnation des auteurs de propos ou d'écrits illicites.

Refus du tribunal de contourner la prescription

Le 12 juin 2013, saisi d'une plainte contre Google pour laquelle le délai de prescription était dépassé, le tribunal de grande instance de Paris a refusé de recourir à d'autres textes, en l'occurrence les articles 1382 et 1383 du Code civil consacrés à la réparation des dommages au sens de la responsabilité civile, pour engager des poursuites. Il a souligné que l'on ne peut recourir à des dispositions du droit commun pour contourner les obligations procédurales de la loi de 1881, qui reste la seule voie pour réprimer les abus de la liberté d'expression.

Quel est le point de départ du délai de prescription ?

La Cour de cassation a énoncé le 27 novembre 2001 que pour les textes publiés sur Internet, « le point de départ du délai de prescription de l'action publique prévu par l'article 65 de la loi du 29 juillet 1881 doit être fixé à la date du premier acte de publication ; que cette date est celle à laquelle le message a été mis pour la première fois à la disposition des utilisateurs. »

On notera que si un contenu violent la loi de 1881 (diffamatoire par exemple) se trouve en ligne depuis plus de trois mois, on ne peut plus poursuivre son auteur au titre de la loi de 1881, même si le contenu est toujours accessible au public. Même si la publication est continue, c'est l'acte de publication, lequel est instantané, qui est pris en compte pour le calcul de la prescription.

Toutefois, si le contenu illicite est publié chez un hébergeur, on peut toujours exiger de celui-ci le retrait du contenu, sans délai de prescription, même si on ne peut plus punir l'auteur.

Enfin, en cas de modification du texte par son auteur, un nouveau délai de prescription court à partir de la date de publication de la mise à jour, ainsi qu'il ressort du jugement du tribunal de grande instance de Tulle du 9 septembre 2008, ainsi que de celui du tribunal de grande instance de Bobigny du 15 novembre 2012.

Le tribunal de grande instance de Paris a précisé le 18 mars 2013 que la mise en ligne d'un lien hypertexte renvoyant vers un contenu illicite doit être considérée comme une nouvelle publication de ce contenu et fait donc repartir le délai de prescription à zéro.

En revanche, concernant Google Suggest, la cour d'appel de Paris a indiqué le 15 mai 2013 que le délai de prescription court à partir de la première apparition d'une suggestion injurieuse et que la réapparition ultérieure de cette suggestion ne faisait pas courir un nouveau délai de prescription.

Le droit de réponse

Qui peut l'exercer ?

Le droit de réponse est prévu dans la loi de 1881 pour toute personne nommée ou désignée dans un journal ou un écrit périodique.

Pour ce qui concerne Internet, l'article 6-IV de la LCEN adapte ce droit de réponse à « toute personne nommée ou désignée dans un service de communication au public en ligne ». La demande d'exercice du droit de réponse doit être adressée au directeur de la publication. Lorsque le site auquel le droit de réponse est adressé est géré à titre non professionnel par une personne ayant conservé l'anonymat, le droit de réponse doit être adressé à l'hébergeur du site, qui la transmet sans délai au directeur de la publication.

Si l'hébergeur néglige de transmettre la demande au directeur de la publication dans un délai de 24 heures, il est passible d'une contravention de 4^e classe (750 €).

La demande de droit de réponse doit être présentée au plus tard dans un délai de trois mois à compter de la publication du message justifiant cette réponse.

Le directeur de la publication est tenu d'insérer les réponses dans les trois jours de leur réception, sous peine d'une amende de 3 750 euros. Il peut en outre être condamné aux peines prévues si le message en cause enfreint la loi.

Le droit de réponse est gratuit.

Si le directeur de la publication accompagne la réponse de nouveaux commentaires, un nouveau droit de réponse peut s'exercer dans les mêmes conditions.

Quelles modalités ?

Le décret 2007-1527 du 24 octobre 2007 précise que la demande d'exercice du droit de réponse doit être envoyée par lettre recommandée avec accusé de réception, ou par tout autre moyen équivalent, et doit garantir l'identité du demandeur. Lorsque le service web mis en cause permet de publier des commentaires, c'est par ce moyen que le droit de réponse doit être exercé.

La demande doit indiquer les références du message, ses conditions d'accès sur le service de communication au public en ligne et, s'il est mentionné, le nom de son auteur. Elle précise s'il s'agit d'un écrit, de sons ou d'images. Elle contient la mention des passages contestés et la teneur de la réponse sollicitée.

Quelle que soit la nature du message auquel elle se rapporte (écrit, son, image), la réponse sollicitée doit prendre la forme d'un écrit. Elle est limitée à la longueur du message qui l'a provoquée. Lorsque celui-ci ne se présente pas sous forme de texte (par exemple, une vidéo ou un dessin), la longueur de la

réponse ne doit pas dépasser celle de sa transcription sous forme d'un texte. La réponse ne peut pas être supérieure à 200 lignes.

Publication de la réponse

Le directeur de publication doit publier la réponse dans des conditions similaires à celles du message en cause, et la présenter comme résultant de l'exercice du droit de réponse. Elle est soit publiée à la suite du message en cause, soit accessible à partir de celui-ci. Lorsque le message n'est plus mis à la disposition du public, la réponse est accompagnée d'une référence à celui-ci et d'un rappel de la date et de la durée de sa mise à disposition du public.

La réponse doit demeurer accessible durant la même durée que le message qui la fonde, avec une durée minimale d'un jour.

Lorsque le message est mis à la disposition du public par le biais d'un courrier électronique périodique non quotidien (liste de diffusion), le directeur de la publication est tenu d'insérer la réponse dans la parution qui suit la réception de la demande.

La personne qui adresse une demande d'exercice de droit de réponse peut préciser que sa demande deviendra sans objet si le directeur de publication accepte de supprimer ou de rectifier tout ou partie du message à l'origine de l'exercice de ce droit. La demande précise alors les passages du message dont la suppression est sollicitée ou la teneur de la rectification envisagée. Le directeur n'est pas tenu d'insérer la réponse s'il procède à la suppression ou à la rectification sollicitée dans un délai de trois jours à compter de la réception de la demande.

Condamnation pour non-publication d'un droit de réponse

Le 9 octobre 2009, la cour d'appel de Paris a confirmé l'ordre donné à une société de publier un droit de réponse sous peine d'une astreinte de 200 euros par jour de retard. La société a dû en outre verser 3 000 euros d'indemnité de procédure au plaignant.

Pour sa défense, la société avait soutenu que le délai de prescription de trois mois n'avait pas été respecté par le plaignant. Cependant, comme cette société avait refusé de réceptionner les lettres recommandées qui lui avaient été adressées dans les délais, le juge a estimé qu'on ne peut se prévaloir de ses propres fautes ou négligences pour priver autrui de ses droits.



Qui est responsable ?

La responsabilité de ses actes, un principe

Comme nous l'avons vu, la Déclaration des droits de l'homme et du citoyen de 1789 prévoit que « la libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté, dans les cas déterminés par la Loi ». Le principe de responsabilité est ainsi posé : chacun doit répondre de ses éventuelles infractions.

Obligation d'identification pour les professionnels, anonymat partiel toléré pour les particuliers

Sites web professionnels

L'éditeur d'un service web a l'obligation légale de publier en ligne son identité pour être joignable en

cas d'abus ou d'infraction de sa part. Selon la LCEN, il doit porter à la connaissance du public :

- s'il s'agit d'une personne physique, ses nom, prénoms, domicile et numéro de téléphone. Il doit également indiquer, le cas échéant, son numéro d'inscription au registre du commerce et des sociétés ou au répertoire des métiers (pour les artisans de moins de dix salariés) ;
- s'il s'agit d'une personne morale (entreprise, association, organisme public ou privé...), sa dénomination et son siège social, son numéro de téléphone. S'il s'agit d'une entreprise, son numéro d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, son capital social et l'adresse de son siège social ;
- dans tous les cas, le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction ;
- le nom, l'adresse et le numéro de téléphone de l'hébergeur.

Sites web personnels

Les personnes publiant un site ou un service web à titre non professionnel ont le droit de préserver leur anonymat, en ne publiant sur leur site que le nom et l'adresse de leur hébergeur, sous réserve d'avoir communiqué à celui-ci les éléments d'identification personnelle (voir section précédente).

Les hébergeurs sont tenus au secret professionnel pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée. La violation de cette obligation de secret professionnel est un délit pénal. Ce secret professionnel n'est bien sûr pas opposable à l'autorité judiciaire.

Le directeur de la publication

Les articles 93-2 et 93-3 de la loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle disposent que « tout service de communication au public par voie électronique [site web, service web] est tenu d'avoir un directeur de la publication. »

Le directeur doit être majeur, avoir la jouissance de ses droits civils et n'être privé de ses droits civiques par aucune condamnation judiciaire.

Lorsque le service est fourni par une personne morale (entreprise, association), le directeur de la publication est le président du directoire ou du conseil d'administration, le gérant ou le représentant légal de la société, suivant la forme de la personne morale.

Lorsque le service est fourni par une personne physique, le directeur de la publication est cette personne physique.

La responsabilité en cascade

En cas d'infraction à la loi de 1881 sur la presse, deux cas peuvent se présenter.

- Soit le message incriminé a été rédigé, validé ou modéré par le ou les responsable(s) du site web (la loi dit que le contenu a dans ce cas « fait l'objet d'une fixation préalable ») : c'est alors le *directeur de la publication* qui est poursuivi comme auteur principal de l'infraction. *L'auteur du message* sera poursuivi comme complice.
- Soit le message, qui émane d'un tiers, n'a pas fait l'objet de vérification ou de modération (cas des commentaires sur les blogs par exemple) ; dans ce cas, c'est l'*auteur du message* qui est poursuivi. À défaut de l'auteur, par exemple dans le cas où son identité est inconnue, c'est le *producteur* qui sera poursuivi comme auteur principal de l'infraction (c'est ce qu'on appelle la responsabilité en cascade).

DÉFINITION Le producteur

La notion de « producteur » avait un sens clair dans la loi de 1982 consacrée à l'audiovisuel. Par exemple, dans une émission radio de dialogue en direct avec les auditeurs, un interlocuteur téléphonique non identifié pourrait tenir à l'antenne des propos illicites. C'est alors le producteur de l'émission qui serait tenu pour responsable.

Appliquée à Internet, cette notion de producteur désigne la société qui exploite le site web sur lequel le message incriminé est publié.

L'article 6-I 6° de la loi pour la confiance dans l'économie numérique précise que les fournisseurs d'accès à Internet et les hébergeurs ne sont pas des producteurs.

Jurisprudence

Le 26 mars 2008, la Cour de cassation a confirmé la condamnation pour diffamation publique d'une maire, directrice de la publication du site web de la ville, pour y avoir publié une lettre du sénateur de la ville diffamant un opposant. Le rédacteur de la lettre a été condamné comme complice.

Ils ont dû s'acquitter chacun de 2 500 euros d'amende et 750 euros de dommages (plus 3 000 euros en cassation), plus la publication du jugement.

Modérer ou ne pas modérer ?

La loi précise par ailleurs que lorsque l'infraction résulte du contenu d'un commentaire laissé par un internaute sur un espace de contributions personnelles, le directeur de publication ne peut pas voir sa responsabilité pénale engagée comme auteur principal s'il est établi qu'il n'avait pas effectivement connaissance du message avant sa mise en ligne ou si, dès le moment où il en a eu connaissance, il a agi promptement pour retirer ce message.

Le responsable d'un site web contenant un espace de commentaires non modérés a ainsi pour seule obligation de retirer promptement les messages en infraction, dès qu'il en a connaissance.

En revanche, le responsable d'un site web qui modère les contenus des commentaires endosse une plus grande responsabilité : s'il laisse publier un commentaire illicite, il est considéré comme auteur de l'infraction.

Modérer un forum ou un espace de commentaires fait endosser plus de risques pénaux au directeur de la publication que ne pas le modérer. Cette situation est paradoxale, qui menace de sanction celui qui fait des efforts et qui exonère de toute responsabilité celui qui n'en fait pas.

Le 10 octobre 2013, la Cour européenne des droits de l'Homme (CEDH) a ainsi validé la condamnation par la justice estonienne de l'exploitant d'un portail d'information qui avait, malgré ses filtres, laissé publier des commentaires d'insulte sous un article concernant une entreprise. La Cour a considéré que les auteurs réels des messages ne pouvant être retrouvés, l'exploitant endossait la responsabilité des contenus, qu'il aurait dû faire preuve de plus de prudence, et que la sanction proportionnée prononcée par la justice estonienne ne constituait pas une entrave à la liberté d'expression.

La responsabilité du producteur

Cette exonération de responsabilité en cas de non-modération s'applique-t-elle également au producteur ? En effet, en pratique, si une société exploite un site web sur lequel des internautes peuvent laisser des messages, le responsable de cette société est, comme on l'a vu, considéré comme le directeur de la publication. En cas de message enfreignant la loi de 1881, on recherchera d'abord la responsabilité du directeur de la publication. Si le site est non modéré, on recherchera celle de l'auteur du message. Si celui-ci est introuvable (connu sous un simple pseudo, sans coordonnées personnelles), la justice se retournera vers le producteur... qui n'est souvent autre que le directeur de la publication !

Dans son arrêt du 16 février 2010, approuvé par le Conseil constitutionnel (décision 2011-164), la Cour de cassation a confirmé que si l'auteur du message ne peut être identifié, la personne qui a pris l'initiative de créer un service web non

modéré (donc le directeur de la publication) peut être poursuivie en sa qualité de producteur. Le dispositif de responsabilité en cascade revient à son point de départ !

Le Conseil constitutionnel a de son côté été saisi d'une demande d'examen de la constitutionnalité de ce dispositif de responsabilité en cascade, aux motifs qu'il créerait contre le directeur et contre le producteur une présomption de culpabilité contraire à la Déclaration des droits de l'homme (tout homme est présumé innocent jusqu'à preuve de sa culpabilité) et qu'il traiterait différemment, sans justification, le directeur de la publication et le producteur sur Internet, rompant ainsi l'exigence d'égalité de la loi pour tous.

EN DÉTAIL Le Conseil constitutionnel

Le Conseil constitutionnel a pour mission de vérifier la conformité des lois à la Constitution. Il est saisi, soit à la demande des parlementaires avant la promulgation d'une nouvelle loi, soit, pour les lois déjà en vigueur, à la demande des citoyens dans le cadre d'une « question prioritaire de constitutionnalité » (QPC).

Dans sa décision 2011-164 du 16 septembre 2011, le Conseil constitutionnel a estimé que le mécanisme de responsabilité en cascade était conforme à la Constitution, sous la réserve suivante : pour ne pas instaurer une présomption de culpabilité qui serait inconstitutionnelle, l'article 93-3 de la loi du 29 juillet 1982 ne doit pas être interprété comme permettant que le créateur ou l'animateur d'un site web mettant à la disposition du public des messages adressés par des internautes, voie sa responsabilité pénale engagée en qualité de producteur à raison du seul contenu d'un message dont il n'avait pas connaissance avant la mise en ligne.

Autrement dit, en cas de non-modération, le producteur jouit de la même protection que le directeur de la publication : s'il n'a pas eu connaissance des messages avant leur publication, sa

responsabilité pénale se limite à l'obligation de les retirer promptement dès qu'il en reçoit la demande.

Confirmation de la limitation de responsabilité du producteur

Le 30 octobre 2012, la Cour de cassation a eu l'occasion de se prononcer une nouvelle fois sur le dispositif de responsabilité en cascade, ce qui confirme le manque de clarté des textes concernant le « producteur » d'un site web. Appliquant la décision du Conseil constitutionnel, elle a confirmé que « la responsabilité pénale du producteur d'un site de communication au public en ligne mettant à la disposition du public des messages adressés par des internautes n'est engagée, à raison du contenu de ces messages, que s'il est établi qu'il en avait connaissance avant leur mise en ligne ou que, dans le cas contraire, il s'est abstenu d'agir promptement pour les retirer dès le moment où il en a eu connaissance. »

Jurisprudence sur le directeur de la publication

Le même 30 octobre 2012, la Cour de cassation a confirmé la condamnation à 5 000 euros d'amende, à la publication de la sanction et à des dommages-intérêts, d'un internaute qui tenait un blog d'information politique et qui avait mis plusieurs mois à retirer des commentaires constituant une incitation à la haine raciale. En tant que directeur de la publication, il n'avait donc pas agi promptement. La Cour a ajouté à la sanction 2 500 euros à verser à la Ligue internationale contre le racisme et l'antisémitisme en remboursement des frais engagés.

Il est à noter que l'internaute avait indiqué contrôler les commentaires déposés sur son blog une fois par semaine. La Cour n'a pas trouvé une telle fréquence insuffisante, s'agissant d'un blog personnel, mais elle a sanctionné le fait qu'il avait fallu plusieurs mois à l'internaute pour supprimer les propos illicites. Autrement dit,

elle a admis un contrôle hebdomadaire, mais a sanctionné le fait que les propos aient « passé » plusieurs contrôles.

Responsabilité des mineurs

Les blogueurs et les personnes qui laissent des commentaires sur les pages Facebook ou sur les autres réseaux sociaux sont souvent des mineurs. Il n'existe pas de loi spécifique encadrant la responsabilité des mineurs sur Internet et les textes généraux sont applicables.

- Un jeune de 10 à 13 ans peut être reconnu pénalement responsable et peut subir certaines sanctions, comme la confiscation de ses outils informatiques ayant servi à commettre l'infraction.
- Un jeune de 13 à 18 ans peut se voir condamner à une amende, dont le montant ne peut dépasser la moitié de l'amende encourue, ni excéder 7 500 euros.

Concernant les dommages-intérêts à verser au plan civil, il revient aux parents d'en assurer le règlement si le mineur n'est pas en état de le faire. En effet, conformément à la règle générale du Code civil, les parents sont solidairement responsables des dommages causés par leurs enfants mineurs sur lesquels ils exercent l'autorité parentale.

Comment signaler un contenu illicite ?

Si vous trouvez sur Internet un contenu illicite (appel à la violence ou à la haine raciale, pédopornographie, stupéfiants, injure ou diffamation, escroquerie...), vous pouvez le signaler aux autorités sur le site www.internet-signalement.gouv.fr. Votre signalement sera traité par les brigades spécialisées de la police judiciaire, qui vérifieront l'infraction, puis déclencheront éventuellement une enquête. Si le contenu illicite est publié à l'étranger, Interpol sera saisi.

Il n'est pas obligatoire de donner son identité pour procéder à un signalement, cela peut être fait de manière anonyme. Les dénonciations mensongères sont évidemment interdites.

Les responsabilités de l'hébergeur

La loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) traite de différents thèmes, dont certains relatifs à la protection des données personnelles. Elle définit également les obligations et les responsabilités des éditeurs de contenu et des hébergeurs sur Internet. Ces termes d'éditeurs et d'hébergeurs ne figurent toutefois pas dans la LCEN, mais ils sont couramment utilisés pour plus de commodité.

DÉFINITIONS La distinction éditeur/hébergeur

La distinction entre éditeurs et hébergeurs a, depuis 2004, donné lieu à de nombreux débats et à des jurisprudences contradictoires (qui dépassent notre sujet). Pour simplifier, nous pouvons retenir ce qui suit.

- Les **éditeurs** sur Internet sont les personnes qui mettent en ligne du contenu (texte, images, musique, vidéos...) ou qui ont la mainmise éditoriale sur le contenu créé par d'autres (par exemple, les modérateurs des forums).

Dans son arrêt du 11 septembre 2014, la Cour de justice de l'Union européenne a rappelé que les éditeurs de presse en ligne, même à titre gratuit, relèvent bien du régime des éditeurs.

- Les **hébergeurs** sont les personnes physiques (internauts, gestionnaires de blogs) ou morales (associations, presse en ligne, réseaux sociaux...) qui publient du contenu créé par d'autres sans le contrôler au préalable.

L'internaute qui a un site web personnel, une page Facebook, ou un site de partage, est éditeur du contenu qu'il publie ; il est à ce titre responsable de son caractère légal. Il est de même responsable de ses tweets et des commentaires qu'il dépose sur les blogs ou sur les réseaux sociaux. Dans ces cas de figure, le réseau social,

le site de partage ou celui de micro-blogging ne sont que des hébergeurs. L'internaute est par ailleurs hébergeur au titre des commentaires qu'il accueille sur son blog ou sur sa page Facebook.

DÉFINITION L'hébergeur

D'un point de vue juridique, on appelle hébergeurs les personnes que la LCEN (article 6.1.2) définit ainsi : « les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services. »

Contrôle de la légalité des contenus

Il résulte des articles 6.1.2 et 6.1.3 de la LCEN que les hébergeurs ne peuvent pas voir leur responsabilité civile ou pénale engagée « du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible ».

L'hébergeur Dailymotion a ainsi été condamné le 2 décembre 2014 par la cour d'appel de Paris à 1,2 million d'euros de dommages-intérêts, pour ne pas avoir retiré promptement des vidéos pirates d'émissions de TF1.

L'article 6.1.7 ajoute que les hébergeurs ne sont pas soumis « à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites ».

Ces articles signifient que l'hébergeur qui, par définition et *a priori*, ne connaît pas le contenu qu'il héberge, n'a pas à procéder spontanément à des contrôles et n'est pas responsable du

caractère éventuellement illégal des contenus ; pas plus que, par exemple, La Poste n'est responsable si une lettre contient des injures ou de la diffamation. En revanche, lorsque le caractère illégal du contenu lui est signalé, il a la responsabilité d'agir rapidement pour rendre celui-ci inaccessible.

Précision **Avis du Conseil constitutionnel**

Le Conseil constitutionnel a précisé, dans sa décision 2004-496 DC du 10 juin 2004, que « ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge ».

En pratique donc, lorsque l'illégalité signalée est manifeste (par exemple : pédopornographie), l'hébergeur retirera un contenu sans exiger de formalité ; dans les autres cas, si l'illégalité est discutable, il attendra la décision d'un juge.

Formalisme **La notification**

La notification à l'hébergeur des faits illicites doit respecter les formes prescrites à l'article 6.1.5 de la LCEN :

« La connaissance des faits litigieux est présumée acquise par [les hébergeurs] lorsqu'il leur 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 son représentant légal ;
- 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. »

Comme on le voit, la demande de retrait ne peut être adressée à l'hébergeur qu'après que l'on a contacté (ou essayé de contacter) en vain l'auteur du contenu.

Jurisprudences concernant les responsables de forums

Le 21 juillet 2005, le tribunal de grande instance de Lyon a examiné la plainte d'une société visant le responsable d'un forum de discussion. La société avait relevé sur ce forum des commentaires la concernant qu'elle jugeait diffamatoires. Elle en avait demandé la suppression au responsable du forum qui s'était exécuté. Elle attaquait toutefois ce dernier en diffamation en sa qualité de directeur de la publication.

Le tribunal a indiqué que le forum en question, modéré *a posteriori* par son responsable qui le contrôlait « trois ou quatre fois par semaine », relevait bien du régime de l'hébergeur au sens de la LCEN. Si le responsable du forum n'avait pas eu « son attention spontanément attiré par les messages incriminés » lors de ses contrôles de routine, il n'en avait pas moins retiré les messages litigieux dans les 24 heures après en avoir reçu la demande : il avait ainsi « agi promptement dès qu'il a eu connaissance du caractère illicite du message », conformément aux dispositions de la loi. Le responsable du forum ne pouvait donc voir sa responsabilité engagée et le plaignant était débouté de l'ensemble de ses demandes.

EXTRAIT DU JUGEMENT : Forum non modéré ou modéré *a posteriori*

« Le responsable d'un forum non modéré ou modéré *a posteriori* doit être considéré comme un hébergeur au sein de la loi puisqu'il assure le stockage direct des messages diffusés sans porter de regard préalable sur ces derniers. »

La cour d'appel de Versailles a jugé le 12 décembre 2007 une affaire similaire, dans laquelle une société, s'estimant victime d'un dénigrement commercial, attaquait une association de défense des consommateurs responsable d'un forum. La cour a confirmé que le statut d'hébergeur s'applique aux forums non modérés ou modérés *a posteriori*. Par ailleurs, le plaignant n'ayant pas adressé à l'hébergeur une notification conforme aux exigences de l'article 6.I.5 de la LCEN, s'en tenant à des réclamations « larges, vagues et générales », visant des « propos diffamatoires » sans apporter de précision quant aux faits reprochés et à leur emplacement, la cour l'a débouté de ses demandes et l'a condamné à verser 2 000 euros au responsable du forum, au titre des frais de justice.

La réapparition de contenus illicites supprimés

Nous avons vu que l'hébergeur dégage sa responsabilité s'il retire promptement le contenu qui lui a été signalé comme illicite, mais que se passe-t-il si des internautes remettent en ligne, chez le même hébergeur, le contenu supprimé ?

Le 19 octobre 2007, Google a été condamné par le tribunal de grande instance de Paris à 30 000 euros de dommages-intérêts pour n'avoir pas « accompli les diligences nécessaires » pour rendre impossible la remise en ligne d'une vidéo qui lui avait déjà été signalée comme illicite. Le tribunal a reconnu que Google, au titre de son service Google Video, est un hébergeur et avait effectivement retiré promptement la vidéo en cause la première fois qu'elle lui avait été signalée, dégageant ainsi sa responsabilité. Néanmoins, le tribunal ajoutait qu'il appartenait à la société Google « de mettre en œuvre tous les moyens nécessaires en vue d'éviter une nouvelle diffusion, ce qu'elle ne démontre pas avoir fait, le développement allégué de solutions techniques afin de prévenir et à tout le moins de limiter l'atteinte aux droits des tiers ayant manifestement été en l'espèce inopérant ». Il repoussait également l'argument selon lequel chaque remise en ligne constituerait un fait nouveau et nécessiterait une nouvelle

notification : « si les diffusions successives sont imputables à des utilisateurs différents, leur contenu et les droits de propriété intellectuelle y afférents, sont identiques ». Le tribunal concluait que « faute pour elle de justifier avoir accompli les diligences nécessaires en vue de rendre impossible la remise en ligne du documentaire [...] déjà signalé comme illicite, la société Google Inc ne peut se prévaloir de la limitation de responsabilité prévue à l'article 6-I-2 de la loi du 21 juin 2004. »

DÉFINITION Le droit prétorien

Une telle obligation d'empêcher la remise en ligne d'un contenu retiré ne figure pas dans la loi. Il peut donc sembler surprenant de voir un juge s'y référer et condamner une société sur cette base. Cette pratique existe pourtant et porte le nom de droit prétorien : il s'agit des positions jurisprudentielles retenues par les tribunaux, qui finissent par « prendre force de loi », en l'absence justement d'une loi sur le sujet. Parmi les créations prétoriennes les plus connues, citons le devoir d'information et de conseil de la banque, ou de l'agent immobilier. Dans le cas présent, cette obligation d'empêcher activement la remise en ligne d'un contenu déjà retiré n'aura toutefois « force de loi » que tant que les tribunaux l'appliqueront.

Une décision dans le même sens a été rendue le 14 décembre 2010 par le tribunal de grande instance de Créteil, qui a ordonné à YouTube « d'installer sur son site un système de filtrage efficace et immédiat des vidéos » qui lui ont déjà été signalées, pour éviter leur remise en ligne.

De même, la cour d'appel de Paris a estimé le 16 octobre 2010 que la mise en place par Dailymotion des technologies qui « permettent la détection, entraînant le rejet automatique avant la mise en ligne, de tout contenu » déjà signalé, va dans le sens du respect de ses obligations d'hébergeur.

Ainsi, la cour d'appel de Paris a confirmé le 21 juin 2013 que YouTube n'avait pas engagé sa responsabilité d'hébergeur en ne retirant pas automatiquement des contenus déjà signalés qui avaient été remis en ligne. En effet, YouTube avait mis en place une technologie de reconnaissance vidéo gratuite afin

d'éviter que les vidéogrammes contrefaits soient diffusés sur sa plate-forme. YouTube remplissait ainsi ses obligations. La Société des producteurs de phonogrammes en France (SPPF), qui avait refusé d'adhérer à ce système, ne pouvait dans ce cas exiger un retrait automatique des contenus. Si la SPPF voulait faire retirer une deuxième fois des contenus réapparus, elle devait donc les signaler à nouveau à YouTube.

À SAVOIR Portée de l'obligation

On constate que l'obligation de mettre en place des outils de filtrage pour empêcher la remise en ligne d'un contenu déjà signalé n'a apparemment été appliquée par les juges qu'aux hébergeurs commerciaux : Google, YouTube, Dailymotion. On peut supposer, mais cela reste à confirmer, qu'ils n'imposeront pas les mêmes obligations à des internautes hébergeurs au titre de leur blog personnel ou de leur page Facebook. Il semble également qu'il s'agisse d'une obligation de moyen, et non de résultat. Cela signifie que la mise en place d'outils qui correspondent à l'état de l'art suffira à dégager la responsabilité de l'hébergeur et que l'on ne lui reprochera pas un éventuel insuccès : par exemple, dans le cas de vidéos, si une vidéo déjà retirée est remise en ligne par un internaute qui l'aura légèrement modifiée pour échapper aux filtres.

Conservation des données de connexion

La loi de 2004 pour la confiance dans l'économie numérique (LCEN) impose aux fournisseurs de services de communication au public en ligne et aux hébergeurs de conserver les données permettant l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires, et de les communiquer aux autorités judiciaires à la requête de celles-ci.

Sont également soumises à cette obligation « les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne », c'est-à-dire les fournisseurs d'accès à Internet, les cybercafés, etc., ainsi que « les personnes physiques ou morales qui assurent, même à titre gratuit, pour

mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services », ce qui inclut les responsables de blogs, forums, pages web personnelles...

La durée de conservation prescrite par la loi est d'un an.

La liste des données à conserver fait l'objet du décret n°2011-219 du 25 février 2011, approuvé par le Conseil d'État le 20 novembre 2013. Y figurent notamment :

- l'identifiant de la connexion, l'adresse IP utilisée ;
- les date et heures de début et de fin de la connexion ou de l'opération ;
- l'identifiant utilisé par l'auteur de l'opération ;
- lors d'une création de compte : les nom et prénom de l'utilisateur, ses coordonnées (postales, téléphoniques, courriel), son pseudonyme, son mot de passe et les moyens de le modifier ;
- en cas de compte payant : les informations sur le moyen de paiement et la transaction.

Comme indiqué dans le décret 2011-219, ces données constituent des données personnelles. Le tribunal de grande instance de Paris en a logiquement déduit le 17 juillet 2014 que la personne concernée peut exercer à leur sujet les droits d'accès qui lui sont reconnus par la loi (voir le chapitre 3 sur les données personnelles).

À SAVOIR La position de la Cour de justice de l'Union européenne (CJUE)

Le 8 avril 2014, la CJUE a invalidé la directive européenne de 2006 qui détermine la liste des données de connexion à conserver. La Cour a estimé que la conservation de ces données aurait dû s'accompagner de garanties pour éviter toute atteinte à la vie privée. La situation juridique française est désormais confuse, car la LCEN et le décret de 2011, eux, n'ont pas été invalidés alors qu'ils encourent les mêmes griefs.

Applicabilité aux services web non européens

Par son ordonnance de référé du 24 janvier 2013, le tribunal de grande instance de Paris a estimé « qu'il n'apparaît pas avec l'évidence requise en référé » (c'est-à-dire de manière suffisante pour prendre une décision immédiate) que ces dispositions soient applicables à Twitter. En effet, le décret 2011-219 prévoit que la conservation des données de connexion est soumise à la loi Informatique et Libertés, qui n'est applicable qu'aux responsables de traitements établis sur le territoire français, ou recourant à des moyens situés sur le territoire français. Or Twitter Inc. est une société américaine, dont les serveurs sont situés aux États-Unis ; elle peut donc prétendre ne pas être soumise à la loi Informatique et Libertés et, par suite, au décret 2011-219.

Obligation de lutte contre les contenus illégaux

Si les hébergeurs, comme on l'a vu, n'ont pas à exercer de contrôle sur les contenus et ne sont pas responsables de leur caractère éventuellement illicite, la LCEN (article 6.I.7) a néanmoins prévu qu'ils doivent participer à la lutte contre des types d'infractions particulièrement graves : l'apologie des crimes contre l'humanité, l'incitation à la haine raciale, l'appel au terrorisme ou son apologie, et la pédopornographie. L'hébergeur a ainsi l'obligation de mettre en place un dispositif « accessible et visible permettant à toute personne de porter à sa connaissance ce type de données » (en clair, un bouton « signaler un contenu illicite ») et d'informer promptement les autorités de toute activité illicite relevant des infractions ci-dessus et qui leur serait signalée.

Applicabilité aux services web non européens

Par son ordonnance de référé du 24 janvier 2013, le tribunal de grande instance de Paris a ordonné à Twitter de mettre en place sur sa plate-forme française un dispositif facilement

accessible et visible permettant de signaler les contenus illicites et notamment l'apologie des crimes contre l'humanité et l'incitation à la haine raciale.

Que deviennent vos données personnelles ?

Exposer sa vie en temps réel est grisant, mais pas sans danger. Comment contrôler la diffusion des informations concernant la vie privée ?

Les préoccupations relatives à la protection des données personnelles contre l'informatique ont émergé dans les années 1970, lorsque les progrès technologiques ont donné aux États la capacité de « fliquer » leur population en constituant de gigantesques bases de données informatisées.

Le concept de tels fichiers n'était toutefois pas nouveau : dès 1749, le policier Guillaute, dans son *Mémoire sur la réformation de la police de France*, suggérait à Louis XV de créer un fichier des habitants de Paris et au XIX^e siècle, le fichier (manuel) de la préfecture de Police de Paris regroupait déjà des millions de fiches concernant des criminels.

C'est dans les années 1970 que l'informatique a permis d'industrialiser ces fichiers, de les automatiser et de donner corps au spectre si redouté de *Big Brother*. Or, à la même période, le respect de la vie privée devenait également une priorité, puisque c'est en 1970 que ce principe fut inscrit dans le Code civil.

Ainsi, les notions de données personnelles et de vie privée sont étroitement mêlées. Et dans le but de protéger la vie privée, le législateur a instauré un certain nombre de principes s'appliquant aux données personnelles.

L'émergence de la vie privée

LA VIE PRIVÉE Une notion récente

La vie privée est une invention relativement récente, d'un point de vue sociologique comme d'un point de vue juridique. Inconnue dans les époques antérieures, l'idée d'un droit à l'intimité et à la vie privée prend corps au XIX^e siècle dans les pays industrialisés. Elle est formalisée pour la première fois dans un article de 1890 de Brandeis et Warren dans la *Harvard Law Review*, intitulé « The Right to Privacy ».

En France, si la Déclaration des droits de l'homme de 1789 reconnaît un droit à la sûreté, il faut l'entendre essentiellement comme une protection de l'individu contre les abus du pouvoir. Ce n'est qu'en 1970 que fut inséré dans le Code civil le principe que « chacun a droit au respect de sa vie privée ». Enfin, c'est en 1999, lors de la discussion de la loi sur la couverture maladie universelle, que le Conseil constitutionnel a rattaché le droit à la vie privée à la Déclaration de 1789 (« la liberté proclamée par [cette Déclaration] implique le respect de la vie privée »), lui donnant ainsi une portée constitutionnelle. Le droit à la protection de la vie privée est donc particulièrement récent.

Il reste à donner une définition de la « vie privée ». Or, cette notion n'est pas précisée par la loi. C'est donc par une construc-

tion progressive de la jurisprudence que l'on constate, au gré des jugements, que ce concept peut englober aussi bien le droit à l'intimité et le droit au secret des correspondances écrites, téléphoniques et électroniques, que la protection contre l'informatique, voire le droit à l'image (qui est pourtant plutôt d'ordre patrimonial). Non seulement les jurisprudences ne permettent pas de dégager une définition globale de la vie privée, mais il apparaît que le respect qui lui est dû n'est pas absolu : la liberté d'expression ou l'intérêt général peuvent éventuellement justifier des atteintes à ce droit.

LA VIE PRIVÉE Une notion relative

Comme l'écrit le tribunal de grande instance de Paris dans son jugement du 13 novembre 2013 : « en vertu de l'article 9 du Code civil, toute personne a droit au respect de sa vie privée et est fondée à en obtenir la protection, toute personne dispose également en vertu du même texte, d'un droit exclusif sur son image, attribut de la personnalité, et sur l'utilisation qui en est faite ; ce droit lui permet, en principe, de s'opposer à la diffusion de celle-ci sans son autorisation et d'obtenir réparation du préjudice qui lui aurait été causé de ce fait. »

Mais, poursuit le tribunal, « ces droits peuvent cependant céder devant les nécessités de la liberté d'expression lorsque la diffusion des informations ou des images sont légitimes au regard de ces nécessités, l'appréciation de cette légitimité étant fonction d'un ensemble de circonstances tenant à la personne qui se plaint de l'atteinte aux droits protégés par l'article 9 du Code civil, notamment sa qualité et son comportement antérieur, l'objet de la publication en cause, son contenu, sa forme, l'absence de malveillance et d'atteinte à la dignité de la personne, ainsi que sa participation à un débat d'intérêt général. »

S'il n'existe pas de définition positive de la vie privée, peut-on recourir à une définition négative, en l'opposant à la vie publique ? Relèverait alors du domaine privé tout ce qui n'advient pas dans le domaine public ou qui n'est pas porté à la connaissance du public par la personne concernée. Il ne s'agit pas là non plus d'un critère absolu. La notoriété de la personne concernée, le lieu où se déroulent les faits

concernés, la volonté plus ou moins affichée de communiquer sur sa vie privée ou au contraire de la protéger jouent également leur rôle. Pensons par exemple aux informations concernant la santé, qui forment une part éminemment sensible de la vie privée de chacun ; s'agissant de la santé du Président de la République, un débat oppose depuis des décennies les partisans du secret à ceux de la transparence.

DRONT INTERNATIONAL Les textes fondamentaux

L'article 12 de la Déclaration universelle des droits de l'homme (1948) dispose :

« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

Ce thème est repris par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (1950) :

« Article 8 - Droit au respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »

La jurisprudence de la Cour européenne des droits de l'homme (CEDH) confirme que la protection des données personnelles représente une composante du droit à la vie privée et relève à ce titre de l'article 8 de la Convention.

En Europe, la Charte des droits fondamentaux de l'Union européenne, qui figure à l'article 6 du Traité sur l'Union européenne depuis 2009, énonce un droit au respect de la vie privée et familiale et un droit à la protection des données personnelles :

« Article 7 - Respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

Article 8 - Protection des données à caractère personnel

Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

De la vie privée aux données personnelles

Il convient de souligner la différence entre « vie privée » et « données personnelles ». Toutes les données personnelles ne relèvent pas de la vie privée. Par exemple, les informations concernant l'activité publique d'une personne constituent des données personnelles, mais ne relèvent pas de sa vie privée. Le droit à la vie privée consiste à pouvoir conserver une part d'intimité, ce qui doit certes s'entendre comme le droit à ne pas voir certaines actions surveillées ou divulguées, mais qui recouvre également le droit à ne pas subir des sollicitations ou des discriminations en fonction d'une vie privée que l'on ne souhaite pas divulguer. Si le concept de vie privée existe depuis le XIX^e siècle, c'est seulement avec la généralisation de l'informatique qu'est apparue la nécessité de prévoir également une protection pour les données personnelles.

Jusqu'au début des années 1980, le système informatique se résumait à un ordinateur central avec ses logiciels. Avec l'invention de la télématique, mariage de l'informatique et des télécommunications, apparut une première convergence avec les technologies de la communication (axée sur la circulation de l'information). L'invention d'Internet fut l'occasion d'un changement fondamental en créant un réseau mondial et décentralisé. Dans ce cadre, la protection des données personnelles a pour objectif d'établir un équilibre entre le droit à la vie privée des personnes et le légitime besoin de certains tiers (entreprises, administrations) de traiter des informations concernant ces mêmes personnes.

Historiquement, le droit à la protection des données personnelles s'est donc constitué en accompagnant le développement de l'informatique. Cette protection offerte aux citoyens s'est imposée en réaction aux risques croissants que la puissance de l'informatique – on ne parlait pas encore de nouvelles technologies, mais celles-ci ont confirmé la tendance – faisait courir à la vie privée, en donnant aux États la possibilité technique de

collecter tous les faits et gestes des citoyens. Elle résulte d'une prise de conscience des limites à imposer aux moyens de surveillance pour préserver le droit à la vie privée. Les États ont donc accepté d'encadrer leurs pratiques, en se dotant d'une législation protectrice.

Pour la France, la loi fondatrice est la loi Informatique et Libertés de 1978, modifiée notamment en 2004.

Depuis les années 1970, la situation a encore évolué : d'abord, les entreprises ont acquis elles aussi la capacité de collecter et de traiter les données personnelles de leurs clients ou de leurs prospects. Plus récemment, chacun, muni de son PC, de sa tablette ou de son smartphone, se retrouve dépositaire, sciemment ou inconsciemment, de ses données personnelles et de celles de ses relations.

DÉFINITION Qu'est-ce qu'une donnée personnelle ?

Selon la loi Informatique et Libertés de 1978 (article 2), constitue une donnée personnelle « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement ».

Attention, cette définition est plus large que les seules « données permettant d'identifier une personne », comme on le croit souvent à tort.

En France, l'autorité indépendante chargée de la protection des données personnelles est la Commission nationale de l'informatique et des libertés (Cnil).

La valeur des données personnelles

Pour le travail comme pour les loisirs, il devient difficile d'échapper à l'utilisation des ordinateurs reliés à Internet, des téléphones portables, des cartes bancaires à puce... pour ne citer que les applications dont les utilisateurs sont conscients. Notre smartphone permet de nous localiser en permanence

grâce au GPS intégré, et d'enregistrer tous nos déplacements. Il est désormais question d'un « Internet des objets », dans lequel tous les objets de notre environnement communiqueraient entre eux pour notre plus grand bien : le réfrigérateur deviendrait capable de gérer le stock de yaourts et d'en commander lui-même par Internet lorsque cela lui apparaîtrait nécessaire. Le *quantified self*, qui consiste à porter des objets connectés (montres, bracelets, lunettes...) pour enregistrer sa vie quotidienne, ses activités, le nombre de calories ingérées... se répand également. Ces évolutions ne sont pas sans conséquence sur le droit de la vie privée, car elles nécessitent la multiplication d'échanges de données personnelles.

Bien plus, non seulement l'exploitation des données personnelles est indispensable au fonctionnement même des nouveaux services, qu'il s'agisse des réseaux sociaux, de la relation client personnalisée ou des comptes en ligne proposés par les administrations ou par les banques, mais la connaissance de l'utilisateur ou du client devient un élément essentiel du modèle économique de ces services. La volonté de limiter l'exploitation des données personnelles risque alors d'entrer en conflit avec la créativité des nouveaux services et d'en entraver le développement en empêchant de valoriser ces données.

Le traitement des données personnelles représente désormais un enjeu crucial pour les responsables d'entreprises, d'administrations ou d'associations : qu'il s'agisse des données de leurs employés, de leurs clients, de leurs usagers ou de leurs membres, elles sont omniprésentes et doivent être traitées et protégées dans les formes prescrites par la loi. Or, leur importance économique est croissante : l'exploitation des données personnelles permet non seulement de rendre un meilleur service aux clients, mais parfois aussi de financer à elle seule ce service. Tous les nouveaux géants du Web, les Facebook et les Google, ne sont gratuits que parce qu'ils monétisent les données personnelles de leurs utilisateurs concernant leur profil de consommation, leurs centres d'intérêts ou leur mode de vie.

Perspectives La valeur des données personnelles

Selon une étude du Boston Consulting Group publiée en 2012, « The value of our digital identity », la valeur totale des données personnelles des citoyens européens représenterait 330 milliards d'euros par an pour les organisations publiques et privées (gains de productivité et conquête de nouveaux marchés). La libéralisation de l'usage de ces données amènerait également un gain potentiel de 670 milliards d'euros par an pour les consommateurs (gains de temps et baisses de prix).

Cependant, les responsables des traitements ne peuvent se permettre d'abuser des données qu'ils ont récoltées. Tout d'abord, la loi fixe un cadre strict et des limites précises à l'exploitation qui peut en être faite ; des sanctions administratives et pénales sont prévues en cas d'infraction. Ensuite, le citoyen-client, de plus en plus conscient des risques, est lui-même demandeur de garanties sur l'usage de ses données. Les pressions exercées à de multiples reprises sur Facebook par ses utilisateurs mécontents, qui ont contraint plus d'une fois le réseau social à reculer, témoignent de l'importance croissante de la demande de protection des données personnelles.

Bien plus, le respect des données personnelles et de la vie privée constitue désormais un argument commercial et un avantage compétitif dans la concurrence entre acteurs marchands.

Certains juristes proposent que la loi évolue pour rendre l'individu pleinement propriétaire de ses données. Il pourrait alors à sa guise les louer ou les vendre. Toutefois, une telle évolution serait contraire à l'esprit de la loi actuelle, qui fait de la protection de la vie privée et des données personnelles un droit intangible : on ne peut ni y renoncer ni le vendre. Elle ne correspond pas non plus à ce que l'on entend communément par le concept de « propriété ».

DEJAL Les propriétés du droit de propriété

On considère traditionnellement que le droit de propriété se décline en trois éléments issus du droit romain : le *fructus*, l'*usus* et l'*abusus*. Le *fructus* est le droit de profiter des revenus et produits de sa propriété, l'*usus* est le droit d'utiliser celle-ci et l'*abusus* est le droit de la détruire ou de la vendre. On voit qu'il est difficile d'appliquer ces concepts à des données personnelles : si l'on comprend ce que pourrait être le droit de tirer un profit d'une donnée personnelle, on voit mal comment on pourrait transférer à autrui le droit de l'utiliser à sa place, voire de la détruire. Pourrait-on ainsi vendre une donnée aussi éminemment personnelle que son identité, permettre à autrui de l'utiliser et de la détruire ? Quel sens cela aurait-il concrètement ?

Les principes fondamentaux de la protection des données personnelles

La protection des données personnelles est actuellement assurée dans toute l'Union européenne sur la base d'une directive de 1995 qui harmonise la situation dans tous les États membres.

Le droit européen actuel de la protection des données personnelles résulte d'un équilibre entre deux légitimités : la vie privée d'une part, et le besoin inhérent aux services modernes de manipuler et de conserver les données d'autre part. Il était indispensable de trouver un compromis pour ne pas entraver le développement des usages de l'informatique.

On parle de « traitement » pour désigner toute manipulation des données personnelles (collecte, enregistrement, transfert, analyse...). La loi prévoit des responsabilités particulières pour la personne qui a décidé de la création du traitement, appelée « responsable du traitement ».

Information et consentement

Toute personne doit être informée que les données la concernant vont faire l'objet d'un traitement informatisé et ce traitement ne peut avoir lieu qu'avec son consentement.

Droit d'accès, de modification et d'opposition

Toute personne a le droit d'obtenir du responsable du traitement les données la concernant et de les faire le cas échéant effacer, rectifier ou compléter.

Finalité du traitement

Un traitement de données doit avoir une finalité (c'est-à-dire un objectif) explicite et préalable. Les données recueillies ne peuvent ensuite être utilisées pour une autre finalité.

Qualité des données

Les données traitées doivent être exactes, complètes et à jour.

Sécurité des données

Le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre la destruction accidentelle ou illicite, l'altération, la diffusion ou l'accès non autorisés.

Limitation de la durée de conservation

Les données ne peuvent être conservées que pendant la durée nécessaire à la finalité du traitement.

Protection des données « sensibles »

Le traitement de certaines catégories de données (origine raciale, opinions politiques, philosophiques ou religieuses, santé, sexualité, condamnations pénales...) fait l'objet de mesures particulières de protection. Sauf cas particuliers, ces données ne peuvent être traitées sans autorisation des autorités de protection des données.

CAS PARTICULIER

Les associations religieuses, partis politiques, syndicats

La loi prévoit une dérogation pour les structures comme les associations religieuses, les partis politiques et les syndicats, qui ont évidemment besoin d'avoir un fichier de leurs membres et adhérents. Tant que leur traitement se limite bien à la seule gestion des adhérents (gestion des cotisations, adresses pour envoyer le courrier électronique ou postal...) et que les données ne sont pas communiquées à des tiers, une autorisation de la Cnil n'est pas nécessaire.

Limitation de l'exportation hors de l'Union européenne

Les données personnelles ne peuvent être exportées que dans un pays garantissant un niveau comparable de protection. L'exportation est donc libre à travers toute l'Union européenne, ainsi que vers un certain nombre d'autres pays (Suisse, Canada, Argentine, Norvège, Islande, Nouvelle-Zélande, Israël...).

Pour une exportation de données vers un pays ne figurant pas dans cette liste, une autorisation de la Cnil est nécessaire (pour les États-Unis, cette autorisation n'est pas nécessaire si l'entreprise destinataire s'est engagée à se conformer aux règles de protection dites du *Safe Harbor*).

jurisprudence La diffusion sur Internet

La Cour de justice des communautés européennes a précisé en 2003 que l'interdiction d'exportation des données personnelles ne s'applique pas pour les sites web : la mise en ligne de données personnelles sur un site web hébergé dans l'Union européenne ne constitue pas un « transfert de données », même si ces données deviennent ainsi accessibles à des personnes se connectant depuis des pays tiers.

En effet, selon la Cour, si l'on retenait l'interprétation inverse, cela aboutirait à interdire toute mise en ligne de données personnelles, tant que tous les pays du monde reliés à Internet n'assurent pas un niveau de protection adéquat.

Champ d'application de la loi

Les traitements concernés par la loi

L'article 2 de la loi Informatique et Libertés indique que cette dernière s'applique « aux *traitements automatisés* de données à caractère personnel, ainsi qu'aux traitements *non automatisés* de données à caractère personnel contenues ou appelées à figurer dans des *fichiers*, à l'exception des traitements mis en œuvre pour l'exercice *d'activités exclusivement personnelles*, lorsque leur responsable remplit les *conditions [territoriales] prévues* à l'article 5 [voir plus bas] ».

La loi vise ainsi principalement les traitements automatisés. « Automatisés » n'est pas l'équivalent de « informatisés » : il ne suffit pas d'utiliser un ordinateur lors d'un traitement de données personnelles pour être soumis à la loi. Une utilisation « manuelle » d'un ordinateur n'entre pas dans la catégorie des traitements automatisés ; c'est heureux, car le simple fait d'envoyer un courriel à quelqu'un, en utilisant son adresse, qui est une donnée personnelle, obligerait sinon à respecter toutes les obligations : demander le consentement du destinataire, lui

donner un droit d'accès aux messages envoyés, interdire de conserver les courriels lorsqu'ils ne sont plus d'actualité, etc.

jurisprudence Accès manuel à des données

Dans son arrêt du 13 janvier 2009, la Cour de cassation a indiqué que la loi Informatique et Libertés ne s'applique pas lorsque, sans recourir à un traitement préalable automatisé, on « utilise un appareillage informatique et un logiciel [...] pour accéder manuellement » à des données personnelles.

Notons toutefois qu'une catégorie de traitements non automatisés reste concernée par la loi Informatique et Libertés : il s'agit des fichiers. Qu'il s'agisse de fichiers papier (les bonnes vieilles « fiches ») ou de fichiers informatisés mais pas automatisés, ils doivent se conformer aux obligations définies par la loi.

Enfin, la loi ne s'applique pas aux « activités exclusivement personnelles ». Ce dernier terme est peut-être malheureux, créant une confusion avec les « données personnelles » : il s'agit en fait des activités exclusivement « domestiques », celles que l'on réalise à titre individuel dans sa vie privée. Ainsi, notre bon vieux carnet-répertoire téléphonique constitue sans doute un fichier papier (ensemble structuré et stable de données accessibles selon le critère de l'ordre alphabétique), mais il est à usage strictement domestique. Il n'a donc pas à être déclaré à la Cnil.

ARRÊTÉS Utilisation d'un appareil informatique

En 2004, la Cour de cassation a été saisie d'un pourvoi formulé par un condamné pour association de malfaiteurs et recel. Ce dernier demandait l'annulation des pièces de la procédure, au motif que les officiers de police qui avaient mené l'enquête en avaient consigné les éléments dans des fichiers sur leurs ordinateurs. Selon lui, ces faits violaient le droit à la vie privée des suspects, ils violaient la loi Informatique et Libertés puisqu'ils n'avaient pas été déclarés à la Cnil, que les suspects n'avaient pas été informés de leur droit d'accès, d'opposition et de rectification, et que les fichiers faisaient apparaître l'origine et les opinions politiques des suspects (s'agissant de personnes impliquées dans des mariages mixtes ou ayant déposé une demande d'asile politique). Par son arrêt du 16 mars 2004, la Cour a rejeté le pourvoi, notant que « l'utilisation d'un appareillage informatique ne suffit pas, à elle seule, à caractériser un traitement automatisé au sens [...] de la loi "Informatique et Libertés" ». Cet arrêt rappelle donc que le simple fait d'utiliser un ordinateur, même pour consigner des données personnelles, ne suffit pas à constituer un traitement automatisé de données.

Le champ territorial de la loi

Des conditions de localisation restrictives

La loi Informatique et Libertés ne s'applique en outre qu'aux traitements réalisés selon des conditions géographiques bien précises. En effet, selon l'article 5 de cette loi, seuls y sont soumis les traitements de données personnelles :

- dont le responsable est établi ou exerce une activité sur le territoire français ;
- ou dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État de l'Union européenne, recourt à des moyens de traitement situés sur le territoire français (à l'exclusion, bien entendu, des moyens de télécommunications et de transit des courriels et des connexions Internet sur les réseaux de télécoms).

À RETENIR Un champ territorial restreint

La loi s'applique aux traitements dont le responsable est soit établi sur le territoire français, soit établi hors de France et de l'Union européenne, mais en ayant recours à des moyens de traitements localisés en France.

On note que les responsables de traitements établis dans l'Union européenne et ayant recours à des moyens de traitement en France ne sont pas mentionnés par la loi : c'est parce qu'ils sont soumis à la loi de l'État membre où ils se trouvent, loi assurant grâce à la directive européenne de 1995 une protection équivalente à celle de la loi française.

Lorsqu'un traitement violant la loi est établi dans l'Union européenne, il est possible à la Cnil d'agir en saisissant son homologue du pays concerné. La transposition de la directive européenne de 1995 assure en effet une harmonisation des règles juridiques entre États membres et une coopération entre les autorités de protection des données. Il y a toutefois des différences nationales dans l'implémentation de cette directive. Par exemple, lorsqu'on lit un article sur un site de presse français, il est souvent possible de l'envoyer à un ami en entrant l'adresse mail de ce dernier. L'adresse est censée ne pas être conservée par le site web, le traitement se limitant à l'envoi du courriel. En Espagne, la loi restreint ce type de service d'envoi au seul cas où le destinataire du courriel a donné son accord préalable au site web.

Quant aux responsables établis hors de l'Union et n'utilisant pas de moyens de traitement en France, ils ne sont pas soumis à la loi Informatique et Libertés. Or, avec le développement d'Internet, ce cas devient de plus en plus fréquent.

Application de la loi française aux services web établis hors de l'Union européenne

Cette question resurgit périodiquement lorsqu'une atteinte aux données personnelles met en cause Google, Facebook, Twitter ou tout autre prestataire étranger, notamment américain.

Une telle limitation est propre à la protection des données à caractère personnel. Pour d'autres types de litiges relatifs à Internet et impliquant des sites étrangers, la compétence du juge français est généralement retenue, à partir du moment où le site est accessible sur le territoire français et encore plus s'il vise spécifiquement un public français (par exemple en étant rédigé en français et non dans sa langue d'origine).

JURISPRUDENCE Application à Yahoo! des lois françaises

On se souvient notamment du litige qui a opposé de 2000 à 2005 Yahoo! Inc. à des associations qui lui reprochaient la mise en vente aux enchères, sur son site américain, d'insignes nazis, vente interdite en France par l'article R645-1 du Code pénal. Si le président de Yahoo! a finalement été relaxé le 6 avril 2005 par la cour d'appel de Paris, la compétence de la justice française n'a pas été écartée. Pourtant, dès l'année 2000, Yahoo! avait demandé à la justice californienne de déclarer le jugement français inapplicable aux États-Unis, en vertu de la liberté d'expression garantie par le premier amendement à la Constitution des États-Unis. Cette demande s'est vue rejetée le 12 janvier 2006 par la cour d'appel du 9^e district de Californie.

Concernant le moteur de recherche de Google, le tribunal de grande instance de Paris a eu l'occasion de se prononcer en 2008 sur le cas d'une personne qui souhaitait qu'il soit fait obligation à Google de supprimer de ses archives accessibles en ligne, des messages portant sur sa vie privée et postés par elle sur des forums de discussion, dont certains depuis 1998. Le demandeur s'appuyait sur les articles de la loi Informatique et Libertés garantissant la limitation de la durée de conservation des données, l'obligation de recueillir le consentement de

la personne concernée, et le droit d'opposition de la personne concernée. Pourtant, dans son ordonnance du 14 avril 2008, le tribunal a estimé que la loi Informatique et Libertés n'était pas applicable dans ce cas : en effet, seuls sont soumis à cette loi les traitements dont le responsable est établi sur le territoire français, ou a recouru à des moyens de traitement établis sur le territoire français. Or, les serveurs de Google (y compris le service google.fr) se situent en Californie et sont exploités par la société de droit californien Google Inc. La société Google France n'étant qu'un représentant commercial et non le responsable du traitement, c'est donc le droit californien qui, dans ce cas, s'applique.

Il est à noter que, paradoxalement, si la loi prévoit ainsi une limitation géographique à la protection des données personnelles, elle n'en prévoit pas pour la protection de la vie privée. Cela permet, pour plus de réussite, notamment dans des cas semblables à celui décrit ici, de s'appuyer sur d'autres textes.

Ainsi, en 2006, le tribunal de grande instance de Paris a été saisi par une personne demandant la suspension de la page d'un blog hébergé par Google et contenant des éléments portant atteinte à sa vie privée. Cette demande était basée, non pas sur la loi Informatique et Libertés, mais sur l'article 9 du Code civil et sur l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, qui stipule que l'hébergeur est tenu de retirer les données stockées ou de rendre leur accès impossible à partir du moment où une décision de justice le lui ordonne. Par son ordonnance de référé du 19 octobre 2006, le tribunal avait constaté l'infraction aux dispositions de l'article 9 du Code civil (atteinte à la vie privée) et avait ordonné à Google de retirer les éléments en cause.

De même, c'est sur la base de l'article 9 du Code civil que le tribunal de grande instance de Paris a, le 6 novembre 2013, ordonné à Google de retirer de son moteur de recherche des images portant atteinte à la vie privée d'une personne.

Le droit à la vie privée

L'article 9 du Code civil prévoit que :

« Chacun a droit au respect de sa vie privée.

Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé. »

Récent revirement de jurisprudence

Jusqu'à récemment, pour la grande majorité des demandes fondées sur la loi Informatique et Libertés, la jurisprudence écartait son application aux services établis aux États-Unis en application de l'article 5 de la loi Informatique et Libertés.

Mais la jurisprudence a connu un revirement spectaculaire début 2014. Google s'est vu appliquer la législation sur les données personnelles, successivement par la Cnil (le 3 janvier), puis par la Cour de justice de l'Union européenne (le 13 mai). Reprenant une solution suggérée dès 2008 par l'ensemble des Cnil européennes, mais jamais appliquée jusque-là, ces jugements se basent sur le fait qu'en stockant des cookies sur les terminaux des utilisateurs, Google réalise bien des traitements automatisés de données personnelles sur le territoire européen, ce qui rend la loi Informatique et Libertés applicable. En outre, il a été estimé que via ses filiales Google France, Google Spain, etc., Google est bien « établi » dans l'Union européenne.

Les droits de l'internaute

Droit de consentement

Sur de nombreux sites web, le consentement de l'internaute est recueilli en lui demandant de cocher une case pour indiquer qu'il a pris connaissance des règles de traitement de ses données et qu'il les accepte.

D'un point de vue juridique, il s'agit d'un « consentement éclairé » : celui qui donne son accord le fait en pleine connaissance de cause. On retrouve là un très vieux principe du droit romain. Il y a 1 800 ans, le juriste Ulpien disait déjà « *nemo videtur fraudare eos, qui sciunt et consentiunt* » : on ne peut pas être accusé de tromper quelqu'un qui sait à quoi il s'engage et qui l'accepte.

Pour le démarchage commercial, la loi impose le principe de l'obtention d'un consentement préalable à toute prospection automatisée par courriel (sauf pour démarcher des personnes déjà clientes afin de leur proposer des produits et services analogues, et en leur fournissant un moyen de faire cesser les sollicitations, par exemple un lien à cliquer).

Zoom Le spam

Un démarchage publicitaire par courriel qui ne respecte pas les règles de la directive est un spam. Le spam le plus bénin est une publicité honnête, mais non sollicitée, analogue aux prospectus que l'on trouve dans les boîtes aux lettres. Le spam devient plus dangereux lorsqu'il sert à proposer des marchandises illégales ou contrefaites. Il peut également servir d'appât pour tenter de soutirer à l'internaute ses coordonnées bancaires, ou pour tenter d'infecter son ordinateur avec un virus ou un cheval de Troie.

Droit d'opposition

Le principal droit utile à l'internaute est celui de s'opposer au traitement de ses données. Une personne peut s'opposer à tout moment, pour des raisons légitimes, à un traitement de ses données (sauf évidemment dans le cas d'un traitement prévu par la loi, par exemple le fichier des impôts...).

Dans le cas particulier de la prospection commerciale (publicité en ligne par courriel), toute personne a le droit de s'opposer gratuitement au traitement de données la concernant.

EN PRATIQUE Le droit d'opposition, mirage ou épouvantail ?

La prospection commerciale est le seul cas où le droit d'opposition est absolu et gratuit. Le destinataire doit pouvoir trouver dans le courriel la procédure à suivre pour faire effacer ses coordonnées de la liste.

Dans les autres cas, non seulement le droit d'opposition n'est pas obligatoirement gratuit, mais il doit être motivé par des « raisons prépondérantes et légitimes ». Seule la jurisprudence permet de donner des exemples de telles raisons, sans toutefois en tracer un cadre général.

Afin de protéger les mineurs, certains suggèrent de leur accorder un « droit à l'oubli », consistant en un droit absolu à faire effacer leurs publications. L'État de Californie a adopté une loi en ce sens en 2013.

Le droit d'opposition « pour raison légitime » entre clairement en conflit avec le droit du responsable de traitement, également en vue de son « intérêt légitime », à ne pas demander le consentement de la personne concernée.

En cas de litige, le tribunal devra mettre en balance les deux légitimités concurrentes.

Le tribunal de commerce de Paris a ainsi jugé le 28 janvier 2014 que le fait que Google Suggest propose, suite au nom d'une personne, des mots comportant une connotation négative, crée une atteinte à la réputation de cette per-

sonne et constitue un motif légitime de demander la suppression de la suggestion automatique.

Inversement, le tribunal de grande instance de Paris a estimé le 3 mars 2008 que l'intérêt légitime (en l'occurrence commercial) d'un site web proposant une notation des professeurs ne pouvait justifier que cette notation se fasse sans leur consentement.

EN PRATIQUE Comment réagir en cas de spam ?

Un courriel publicitaire non sollicité est un spam. Cette pratique est réglementée (voir plus loin). Un e-commerçant a le droit de nous envoyer un courriel pour nous proposer des produits ou services analogues à ceux que nous avons déjà achetés chez lui ; il doit toutefois proposer un moyen (lien de désinscription ou adresse mail par exemple) de faire cesser ce démarchage. Si un tel moyen n'est pas proposé, ou si le courriel provient d'un expéditeur inconnu, voire suspect, que faire ?

Si le courriel indésirable contient un moyen de désinscription et semble provenir d'une source suffisamment « sérieuse » pour que ce moyen ne soit pas un leurre, il suffit évidemment de l'utiliser.

Si ce n'est pas le cas, ou si le lien est inopérant, on peut insérer l'adresse mail de l'expéditeur dans la liste des expéditeurs indésirables de son logiciel de messagerie. Les prochains messages de même provenance seront alors automatiquement éliminés par le serveur de messagerie.

Pour agir contre l'expéditeur, deux solutions existent :

- soit porter plainte auprès de la Cnil ;
- soit signaler le courriel sur le site www.signal-spam.fr. Le dossier sera alors transmis aussi bien aux opérateurs télécoms (qui pourront filtrer en amont les courriels abusifs de cet expéditeur) qu'aux autorités (Cnil et police) et aux éditeurs d'antivirus (au cas où le message en question cacheraient des virus ou des chevaux de Troie).

Droit d'accès et de rectification

L'article 39 de la loi Informatique et Libertés prévoit que toute personne peut demander à un responsable de traitement si des données la concernant sont traitées, et obtenir des informations sur le traitement, ainsi qu'une copie sous forme intel-

ligible des données la concernant et toute information disponible sur leur origine.

Ce droit n'est pas absolu : la personne concernée doit justifier de son identité (en pratique, une photocopie de ses papiers d'identité suffit le plus souvent) et la communication de la copie des données n'est pas gratuite : le responsable du traitement peut exiger le remboursement des frais de copie.

EN PRATIQUE **Max Schrems et Facebook**

Un étudiant autrichien, Max Schrems, a voulu en 2011 exercer son droit d'accès auprès de Facebook et a demandé copie de l'intégralité des données le concernant. Il a reçu en retour, au bout de six semaines, 1 222 pages au format PDF. Scandalisé par la quantité d'informations conservées (notamment des données censées avoir été effacées), il a porté plainte contre Facebook et a créé l'organisation europe-v-facebook.org pour soutenir son action. Son association a rapidement rassemblé 25 000 plaignants et a lancé une action collective contre Facebook devant la justice européenne, toujours en cours.



FIG. 3-1 > Max Schrems et le tirage papier des données communiquées par Facebook
© 2011 Dominik Steinmair/europe-v-facebook.org

Le responsable du traitement n'est pas tenu de répondre à des demandes manifestement abusives, notamment par leur caractère répétitif ou systématique.

De même (article 40 de la loi Informatique et Libertés), toute personne peut exiger que les données la concernant soient rectifiées, complétées ou mises à jour ; ou que soient effacées les données inexacts ou dont le traitement est interdit.

Encore une fois, ce droit n'est pas absolu : la personne concernée devra justifier de son identité. En revanche, ce droit de rectification est gratuit. Le responsable doit prouver qu'il a procédé aux opérations demandées et rembourser les frais éventuellement demandés lors de la communication d'une copie des données, si cette communication a entraîné une demande de modification. Il doit également informer de la modification tous les tiers auxquels il aura pu transmettre les données en question.

Les héritiers d'une personne décédée ont également le droit d'exiger une mise à jour gratuite des données du défunt.

Droit au déréférencement

Dans une décision du 13 mai 2014, la Cour de justice de l'Union européenne a indiqué qu'un internaute peut demander aux moteurs de recherche de cesser de référencer certaines pages contenant leur nom, si les informations publiées, même véridiques et collectées de manière licite, apparaissent désormais inadéquates, non pertinentes ou excessives.

Pour appliquer cette décision, Google met désormais en ligne un formulaire de suppression. Les demandes de suppression doivent être justifiées. Leur acceptation n'est pas systématique : les moteurs de recherche devront juger de leur pertinence et chercher un équilibre avec le droit du public à accéder à ces informations.

En cas de refus du moteur de recherche d'accéder à la demande de déréférencement, une action devant le tribunal demeure possible. Le 19 décembre 2014, le tribunal de grande instance de Paris a ainsi ordonné en référé à Google Inc. de déréférencer un article vieux de huit ans, concernant une condamnation non portée au casier judiciaire, et dont la persistance dans les résultats nuisait à la recherche d'emploi de la personne concernée.

Comment faire valoir ses droits ?

L'internaute qui veut exercer son droit d'opposition ou son droit d'accès et de rectification doit pouvoir le faire en contactant le responsable de traitement dont les coordonnées sont censées être disponibles dans les courriels ou dans les sites web qu'il gère.

Si aucun moyen de joindre le responsable de traitement n'est disponible, ou si celui-ci ne répond pas, l'internaute peut porter plainte en justice pour violation de la loi Informatique et Libertés. Franchement, sauf si un préjudice financier important résulte de cette violation, il a peu de chances de voir sa plainte déclencher des poursuites. En revanche, il peut porter plainte auprès de la Cnil. Celle-ci contactera elle-même le responsable de traitement et ouvrira éventuellement une enquête. La procédure à suivre pour alerter la Cnil est détaillée sur le site www.cnil.fr.

Les devoirs du créateur de site web

Un site web personnel, un blog ou une page Facebook (ou sur tout autre réseau social), contient très souvent des données personnelles relatives à l'auteur des pages, mais également à ses relations (amis, famille...) ou aux personnes contribuant au site (zone de commentaires par exemple). Le responsable du site ou de la page est libre de divulguer ses propres données

personnelles, en en assumant les conséquences, mais il doit agir avec plus de prudence en ce qui concerne les données d'autres personnes (voir le chapitre 4 sur la e-réputation).

Formalités administratives

Si le site web est personnel, il n'a pas à être déclaré à la Cnil. Son responsable doit néanmoins respecter les autres obligations découlant de la loi Informatique et Libertés.

Zoom Condamné pour non-déclaration de site web

Cette exemption de toute formalité administrative ne découle pas de la loi, mais d'une décision de 2005 de la Cnil (délibération n°2005-285), qui n'avait sans doute pas envie de recevoir des millions de déclarations.

Avant cette décision, une personne avait été condamnée en 2004 à 450 € d'amende avec sursis pour avoir omis de déclarer son site web personnel à la Cnil.

Pour les sites web professionnels ou les applications pour smartphones, s'ils collectent et manipulent des données personnelles, il est nécessaire de consulter le site de la Cnil pour voir quelles sont les formalités à accomplir (selon les cas, exemption de formalités, simple déclaration ou demande d'autorisation).

Devoir d'information

Un site web traitant des données personnelles doit mentionner que les personnes dont les données sont collectées disposent d'un droit d'accès, de mise à jour et d'opposition sur le traitement de leurs données. Un moyen d'exercer ce droit (numéro de téléphone, adresse mail, etc.) doit être indiqué.

En cas de collecte de données personnelles sur le site, doivent également être précisés (article 32 de la loi Informatique et Libertés) :

- l'identité du responsable du traitement ;
- la finalité du traitement auquel les données sont destinées ;
- le caractère obligatoire ou facultatif de la réponse ;
- les conséquences éventuelles d'une absence de réponse ;
- les destinataires des données ;
- l'éventuel transfert des données hors de l'Union européenne.

La loi prévoit également que ces informations doivent être communiquées à la personne concernée, même dans le cas où les données ne sont pas recueillies directement auprès de cette dernière. Toutefois, cette obligation ne s'applique pas lorsque les données sont conservées sous forme anonymisée à des fins historiques, statistiques ou scientifiques. Elle ne s'applique pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible, ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche.

Cette dernière notion ne doit pas s'entendre comme un permis de laxisme accordé au responsable du traitement : en cas de litige, il faudra convaincre le juge ou la Cnil que l'effort dont on a voulu se dispenser était réellement « disproportionné ».

Sécurité des données

Le créateur d'un site web, s'il collecte, traite ou met en ligne des données personnelles, doit prendre les mesures pour assurer un niveau de sécurité approprié. Le choix des mesures à prendre ne figure pas dans la loi ; il doit tenir compte de l'état de l'art et du coût des mesures, en fonction des risques pesant sur les données.

LIMITATION DE RESPONSABILITÉ Une obligation de moyens

L'obligation de sécurité pesant sur le responsable du traitement est clairement une obligation de moyens. En cas par exemple d'accès illicite aux données – typiquement, un vol de numéros de cartes bancaires –, le responsable du traitement sera tenu quitte s'il prouve qu'il avait pris des mesures de sécurité raisonnables et proportionnées. Autrement dit, si un pirate exploite une faille jusqu'ici inconnue pour accéder aux données, le responsable de traitement n'est pas considéré comme coupable. Il l'est en revanche si la faille est connue, que des correctifs sont disponibles et qu'il ne les a pas mis en œuvre.

Lorsque le traitement est confié à un sous-traitant, celui-ci doit apporter des garanties suffisantes quant aux mesures de sécurité et s'engager contractuellement à les mettre en œuvre.

Le fait de ne pas sécuriser les données personnelles peut aboutir à une moindre indemnisation en cas de piratage de celles-ci. En effet, il peut être jugé que le responsable du traitement a contribué à son propre préjudice en ne mettant pas en œuvre les mesures de sécurité adéquates pour protéger des données personnelles. Ainsi, le 21 février 2013, le tribunal de grande instance de Paris a diminué de 30 % les dommages et intérêts à verser à une société dont la base de données clients, mal sécurisée, avait été piratée par un concurrent. Le tribunal a estimé qu'en négligeant de mettre en œuvre des mesures de sécurité suffisantes, la victime avait facilité l'attaque.

Prospection commerciale

Pour réaliser de la prospection commerciale (envoi de courriels publicitaires ou promotionnels), le e-commerçant doit bien sûr avoir collecté les adresses mail de ses prospects d'une manière licite. Il doit par ailleurs obtenir le consentement préalable des destinataires, par exemple en leur faisant cocher une case « j'accepte de recevoir des informations publicitaires... », sauf s'il s'agit de personnes déjà clientes auxquelles il propose des produits ou services analogues à ceux qu'elles avaient précé-

demment achetés. Le e-commerçant doit leur fournir un moyen de faire cesser les envois de courriels (lien de désinscription ou adresse mail à laquelle envoyer la demande pour faire cesser le démarchage).

L'article L34-5 du Code des postes et communications électroniques (CPCE) précise que « on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ».

Le consentement du destinataire doit être « spécifique » : il ne peut y avoir ici, à la différence des cookies, d'*opt-in* général par paramétrage du navigateur.

Zoom Les cas de prospection non encadrés par la loi

Notons que seule la prospection commerciale est interdite, puisqu'il s'agit uniquement de la promotion de biens ou de services. Avis aux amateurs : la loi est muette sur une éventuelle prospection politique, religieuse, syndicale...

Notons également que l'interdiction ne vise que l'utilisation des coordonnées d'une personne physique. Il reste donc possible d'utiliser les coordonnées d'une personne morale, par exemple contact@entreprise.com.

La Cnil a également autorisé le fait d'envoyer de la prospection commerciale à l'adresse professionnelle d'une personne sans le consentement de celle-ci, du moment que le bien ou service en question est en relation avec son activité professionnelle.

La sanction en cas d'infraction est prévue à l'article R10-1 du CPCE : il s'agit d'une contravention de quatrième classe, d'un montant maximal de 750 euros par courriel envoyé.

Un spammeur qui diffuse un million de messages est ainsi passible d'un million de fois 750 euros d'amende. Des condamnations d'un tel montant n'ont jamais été prononcées en France, mais l'ont été aux États-Unis par exemple, bien que sur la base d'un système juridique évidemment différent.

En outre, si l'expéditeur des courriels a collecté les adresses des destinataires de manière illicite, il est également passible des peines prévues à l'article 226-18 du Code pénal pour infraction à la loi Informatique et Libertés, c'est-à-dire 5 ans de prison et 300 000 euros d'amende.

Enfin, il est interdit de dissimuler l'adresse réelle de l'expéditeur d'un message électronique de prospection directe, ou de ne pas indiquer une adresse valable pour faire cesser les sollicitations.

Les cookies

Les cookies sont des petits fichiers stockés dans la mémoire des ordinateurs, gérés par les responsables d'application et conservant une trace des actions de l'utilisateur du terminal sur cette application. Ce sont les cookies qui servent notamment lors d'une navigation sur Internet, pour analyser les préférences d'un utilisateur. L'utilisation des cookies par les prestataires web pour suivre, voire espionner la navigation des internautes, a engendré de nombreux débats pour en déterminer les conséquences sur la vie privée.

Historiquement, les cookies ont d'abord été gérés sous le régime de l'*opt-out* (acceptés par défaut, sauf si l'utilisateur s'y oppose). La tendance est désormais à l'*opt-in* : l'utilisateur doit explicitement accepter les cookies. La directive européenne 2009/136 prévoit que le stockage d'informations, ou l'accès à des informations déjà stockées dans le terminal de l'utilisateur, n'est autorisé que si l'utilisateur a donné son accord après avoir reçu une information claire et complète, entre autres sur les finalités du traitement.

Zoom *Opt-out et opt-in*

Pour signifier le consentement de l'utilisateur, deux démarches étaient en lice.

- L'*opt-out* suppose le consentement par défaut, mais laisse la possibilité de se désinscrire (« cochez la case pour ne plus recevoir la newsletter »).
- L'*opt-in* suppose le refus par défaut, mais demande, pour marquer le consentement, un acte positif d'inscription (« cochez la case pour recevoir la newsletter »).

L'*opt-in* est, depuis 2002, la règle pour la prospection commerciale (même s'il est parfois détourné en précochant la case).

En revanche, les navigateurs Internet ont longtemps été configurés pour accepter par défaut les cookies (*opt-out*). La nouvelle directive, en obligeant à donner une information préalable sur chaque traitement, a conduit à généraliser des mécanismes d'*opt-in*.

Depuis 2011, les règles suivantes s'appliquent aux cookies : l'utilisateur doit être informé de tout accès ou de toute écriture de cookies dans son équipement et de la manière de s'y opposer, et il doit donner son accord. Or, chaque clic sur un lien hypertexte représente un accès aux cookies. En conséquence, pour éviter de devoir « informer » l'internaute et lui demander son accord à chaque changement de page, ce qui deviendrait vite insupportable, l'accord peut être matérialisé *via* le paramétrage par l'utilisateur de son dispositif de connexion. C'est donc en configurant son navigateur que l'internaute pourra matérialiser un *opt-in* général, ou demander à voir chaque cookie en particulier.

Il est évident que ces obligations, qui ont vocation à s'appliquer aux cookies présentant un risque pour la vie privée (cookies de profilage notamment), ne s'appliquent pas aux cookies strictement « techniques » indispensables à la navigation.

Conservation des données de connexion et de localisation

Voir dans le chapitre 2, la section « Les responsabilités de l'hébergeur ».

Sanction encourues en cas de non-respect de la loi

Le non-respect de la loi Informatique et Libertés peut être sanctionné de deux manières :

- par la Cnil, qui dispose d'un pouvoir de contrôle et, depuis 2004, d'un pouvoir de sanction ;
- par les tribunaux, la violation de la loi constituant, selon les cas, un délit ou une contravention.

C'est le Code pénal (articles 226-16 à 226-31 pour les délits et R.625-10 à R.625-13 pour les contraventions) qui fixe les sanctions pénales prévues en cas de non-respect de la loi.

Le non-respect des obligations ou des interdictions prévues par la loi est puni par les tribunaux d'un maximum de cinq ans de prison et 300 000 euros d'amende. Des contraventions de 1 500 euros sont également prévues en cas de non-respect des droits d'information, d'accès ou de mise à jour et de rectification des données.

Quant à la Cnil, elle peut infliger des avertissements ou des sanctions pécuniaires d'un montant maximal de 150 000 euros. Elle peut également ordonner l'interruption d'un traitement non conforme.

Zoom Deux voies de sanction

Lors du vote de la loi Informatique et Libertés en 1978, seul le volet pénal avait été prévu. Le pouvoir de sanction de la Cnil a été instauré lors de la modification de la loi en 2004 et vient se superposer au volet pénal dont il reste parfaitement indépendant. Il est donc possible qu'un même dossier fasse l'objet d'un traitement par les deux juridictions en parallèle et débouche sur deux sanctions pour la même faute. Il s'agit bien d'une violation flagrante du vieux principe du droit romain *Non bis in idem*, selon lequel nul ne peut être condamné deux fois pour les mêmes faits. Cette violation est toutefois encadrée par la loi, qui précise que les deux sanctions cumulées ne peuvent dépasser les maximums prévus dans chacun des textes.

Cela étant, la Cnil et les tribunaux ne sanctionnent pas de la même manière les infractions.

- La Cnil applique une procédure graduée de contrôle, de mise en demeure et seulement en dernier lieu de sanction si la mise en demeure n'est pas respectée.
- Les tribunaux appliquent pour leur part le Code pénal qui réprime les manquements constatés.

Parmi les articles du Code pénal, certains sanctionnent le non-respect des obligations légales (obligation de procéder aux formalités Cnil, d'assurer la sécurité des données personnelles...) ; d'autres sont plus particulièrement consacrés à la protection de la vie privée.

Ainsi, l'article 226-19 du Code pénal réprime le non-respect de l'interdiction de traitement des données sensibles (origine raciale, opinions politiques, philosophiques ou religieuses, santé, sexualité, condamnations pénales...), y compris en cas de traitement manuel (article 226-23).

L'article 226-22 du Code pénal réprime la divulgation sans autorisation d'informations à caractère personnel susceptibles de porter atteinte à la considération de l'intéressé ou à l'intimité de la vie privée d'un tiers. Il prévoit, d'une part un délit de divulgation intentionnelle (cinq ans de prison, 300 000 euros

d'amende), d'autre part un délit de divulgation involontaire par négligence ou par imprudence (trois ans de prison, 100 000 euros d'amende). Rappelons qu'une imprudence se distingue d'une négligence par le fait qu'une action a été volontairement entreprise.

Zoom Droit d'Internet et droit général

On peut également appliquer sur Internet le droit général de protection de la vie privée, notamment l'article 226-1 du Code pénal qui réprime le fait de transmettre « sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé » (un an de prison, 45 000 euros d'amende).

Enfin, délit très répandu, l'article 226-18 du Code pénal réprime la collecte déloyale, frauduleuse ou illicite des données personnelles d'un tiers.

Jurisprudences

Condamnation pour mise en ligne de photos intimes

Un étudiant qui avait scanné et mis en ligne des photos à caractère pornographique de son ex-petite amie, assorties de commentaires désobligeants, a été condamné le 3 septembre 1997 par le tribunal de grande instance de Privas à huit mois d'emprisonnement avec sursis et 5 000 francs d'amende, plus 20 000 francs de dommages et intérêts pour la victime. Le tribunal sanctionnait ainsi le fait d'avoir, en infraction de l'article 226-19 du Code pénal dans sa rédaction de l'époque, « mis ou conservé en mémoire informatique des données nominatives sans l'accord exprès de l'intéressée qui directement ou indirectement fait apparaître ses mœurs » (*sic*).

L'étudiant, le parquet et la victime firent appel. La cour d'appel de Nîmes (6 novembre 1998) confirma le jugement,

mais, tenant compte du fait que le prévenu n'avait jamais été condamné, modifia la peine en une amende de 20 000 francs, les dommages et intérêts déjà alloués étant augmentés de 1 500 francs. Il est à noter que cette décision sanctionne, non pas la diffusion des photos, qui aurait pu relever de l'article 226-1 du Code pénal, mais leur mise en mémoire, c'est-à-dire leur numérisation.

Discussion Comment interpréter cette condamnation ?

Certains auteurs y virent le signe d'une saine mise en garde contre la banalisation de la numérisation :

« En choisissant de sanctionner l'infraction source (la numérisation) et non l'infraction réellement dommageable pour la victime (la diffusion), le tribunal de Privas rappelle donc que la numérisation d'une donnée nominative n'est pas une opération à prendre à la légère. On ne peut y procéder qu'avec l'accord exprès de la personne concernée^a. »

Cette interprétation est discutable. Elle dénote une méfiance envers la numérisation, compréhensible à une époque où les photos étaient encore argentiques. De nos jours, alors que toutes les photos sont numériques et que tous les téléphones portables prennent des photos, cette doctrine assimilant la numérisation à une infraction ferait de chacun un délinquant, dès qu'il prend une photo de plusieurs personnes sans recueillir leurs consentements exprès. Cette interprétation interdirait, en particulier, les photos au sein d'une foule.

En fait, il convient de rappeler que la numérisation de données personnelles n'est pas une infraction en soi, puisque la loi Informatique et Libertés ne s'applique pas tant que le traitement n'est pas automatisé ou qu'il ne concerne pas un fichier ou des données sensibles.

a. Gérard Haas et Olivier de Tissot, *Photographies coquines et propos licencieux sur Internet*, www.juriscorn.net, 20 novembre 1998.

Sanctions pour spam

À partir de février 2005, la Cnil a traité plusieurs dizaines de plaintes émanant de personnes ayant reçu par télécopie des messages publicitaires de la société JPSM, malgré leurs multiples demandes de désinscription envoyées à cette société.

Après avoir rappelé à JPSM ses obligations, et sans réponse de sa part, la Commission a mis en demeure cette société de mettre son traitement en conformité. JPSM a indiqué à la Cnil que des problèmes techniques l'avaient empêchée de prendre en compte toutes les oppositions (8 000 au total) et n'a pas répondu de manière satisfaisante sur les autres points. La Cnil a donc prononcé le 22 novembre 2007 à l'encontre de la société JPSM une sanction de 5 000 euros.

DETAIL

Les différentes demandes de la Cnil non satisfaites par JPSM

La Commission avait demandé en vain à JPSM :

- De « procéder à l'accomplissement des formalités préalables auprès de la Cnil pour tout traitement automatisé de données à caractère personnel mis en œuvre.
- De cesser toute prospection commerciale par télécopie auprès des personnes qui n'auront pas préalablement donné leur accord pour être démarchées [...].
- De supprimer les coordonnées des requérants ayant exercé leur droit d'opposition.
- D'apporter toute garantie que, à l'avenir, les droits des personnes, dont les données à caractère personnel font l'objet d'un traitement automatisé à des fins commerciales, soient respectés ; en particulier le droit d'opposition prévu par l'article 38 de la loi.
- D'indiquer les moyens par lesquels la société JPSM a obtenu les numéros de télécopieurs de ses prospects et apporter toute garantie qu'une telle collecte a été réalisée conformément aux dispositions de la loi Informatique et Libertés. »

Cette décision peut être comparée à l'arrêt de la cour d'appel de Toulouse du 12 janvier 2005 qui, dans une affaire similaire de prospection par télécopie, sans déclaration préalable à la Cnil et sans respecter le droit des destinataires à s'opposer au traitement, avait également prononcé une amende de 5 000 euros.

Accès à des données personnelles non sécurisées

En 1999, Antoine C., journaliste en informatique et administrateur d'un site Internet intitulé *Kitetoo.com*, s'est aperçu en navi-

quant sur le site de la société Tati qu'en utilisant simplement les fonctionnalités du navigateur grand public Netscape, l'ensemble du contenu du serveur s'affichait et qu'il pouvait accéder librement au fichier des clients dans lequel apparaissaient les noms, adresses et autres données personnelles des visiteurs du site. Il envoya alors à l'exploitant du site un message pour l'avertir de cette faille, sans obtenir de réponse. Il répéta l'expérience en juin 2000, obtint le même résultat et envoya un nouveau message d'alerte, qui cette fois fut suivi d'effet, Tati ayant entre-temps changé de prestataire d'administration de site. Néanmoins, Tati porta plainte contre Antoine C. sur la base de l'article 323-1 du Code pénal réprimant l'accès frauduleux à un traitement de données.

Dans son jugement du 13 février 2002, le tribunal de grande instance de Paris reconnut que le traitement de données de la société Tati n'était pas protégé et donc que Tati n'avait pas respecté son obligation de sécurisation des données personnelles. Toutefois, le tribunal estima que ce non-respect n'autorisait pas pour autant un tiers à accéder sans autorisation aux données personnelles, ce qui justifiait la condamnation du journaliste à 1 000 euros d'amende avec sursis. Toutefois, considérant que la société Tati « ne saurait se prévaloir de ses propres carences et négligences pour arguer d'un prétendu préjudice en réalité subi par les personnes victimes éventuelles de violation de leur vie privée », le tribunal la débouta de ses demandes de dommages et intérêts.

Saisie, la cour d'appel de Paris estima le 30 octobre 2002 qu'on ne pouvait reprocher à un internaute d'accéder, en utilisant un navigateur grand public, à des parties de site web qui ne sont ni protégées ni signalées comme confidentielles : l'internaute ne peut deviner que ces données personnelles ne sont pas censées être accessibles et qu'elles ne le sont que suite à une faute du responsable du traitement. En outre, Antoine C. n'avait fait aucune utilisation préjudiciable de ces

données et avait au contraire averti le responsable du traitement. La cour déclara donc Antoine C. non coupable.

Comme on le voit, en première instance, le non-respect par la société Tati de son obligation de sécurisation des données personnelles fut mentionné par le tribunal, sans que la société soit sanctionnée pour ce fait, aucun client n'ayant porté plainte. En appel, ce non-respect constitua la raison principale pour déclarer le prévenu non coupable : en l'absence de sécurisation des données, l'internaute ne peut pas supposer que des pages web accessibles librement sont confidentielles.

En conclusion, cette jurisprudence ne constitue sans doute pas une permission pour les internautes mal intentionnés de rechercher activement sur Internet les données personnelles non protégées, ce qui relèverait dès lors de la collecte illicite de données. Néanmoins, il est à regretter que le manque de protection des données par le responsable du fichier n'ait pas donné lieu à sanction dans cette affaire.

Sanctions pour défaut de sécurité d'un site

Le 19 juillet 2012, la Cnil a adressé à la Fnac un avertissement public pour avoir conservé dans un fichier non chiffré les données bancaires (numéro de carte bancaire, date de validité, cryptogramme visuel) de plusieurs millions de clients. D'une part, une telle conservation de masse n'était pas justifiée ; d'autre part, selon la Cnil, en faisant le choix de ne pas chiffrer le fichier, la société avait délibérément encouru le risque qu'un employé malveillant ou un pirate externe puisse avoir accès à l'ensemble des données bancaires de ses clients, ce qui constituait une violation de son obligation de sécurisation des données.

Le 7 août 2014, la Cnil a de même adressé à Orange un avertissement public, suite à la fuite d'un million de données clients, pour n'avoir pas pris les mesures de sécurité nécessaires lors de l'envoi de ces données à un sous-traitant.

Sanction pour non-respect de la loi Informatique et Libertés

Le 3 janvier 2014, la Cnil a infligé sa sanction maximale de 150 000 euros à Google, lui reprochant de ne pas recueillir le consentement explicite et préalable de ses utilisateurs avant de collecter leurs données, de ne pas fixer une durée maximale de conservation, et de combiner sans autorisation légale les informations collectées sur un même utilisateur *via* ses différents services.

La Cnil a également ordonné la publication de sa décision sur la page d'accueil de Google France.

Google a exercé un recours contre cette sanction devant le Conseil d'État, mais il a été rejeté le 7 février 2014.

Perspectives

En 2012, la Commission européenne a proposé une refonte du cadre législatif européen permettant de mieux protéger les données personnelles des citoyens. Les principes de base demeurent inchangés et la protection des données personnelles est confirmée comme un droit fondamental des personnes. Tous les traitements visant les résidents européens seront soumis à ce nouveau texte, quel que soit leur pays d'origine.

Ce projet a donné lieu à de nombreux débats au niveau du Parlement européen, qui a adopté en 2014 un projet de texte prévoyant notamment un renforcement des contrôles des Cnil et une très forte augmentation des sanctions en cas de violation de la loi (jusqu'à 100 millions d'euros ou 5 % du chiffre d'affaires mondial de l'entreprise concernée, le plus élevé des deux chiffres étant retenu).

Ce texte est désormais discuté dans le cadre du trilogue entre le Parlement européen, la Commission et les gouvernements.



La e-réputation

Au fil de sa participation à des réseaux sociaux, à des forums de discussion, ou à des blogs, chacun construit peu à peu une image de lui qui devient sa réputation sur Internet. L'image d'une personne est également façonnée par ce que les autres publient sur elle, que ce soient ses amis et relations sur les réseaux sociaux, ou des articles de presse ou comptes-rendus professionnels.

Internet a une durée de mémoire illimitée et la réputation numérique d'une personne risque de la suivre toute sa vie. Cela justifie de se préoccuper de la bonne tenue de sa e-réputation.

L'exposition sur les réseaux sociaux

Il est devenu banal de dire que les données personnelles sont le « carburant » du numérique. En tout cas, les services en ligne dits gratuits sont en fait payés par la monétisation, notamment publicitaire,

des données personnelles des utilisateurs et des visiteurs (« si c'est gratuit, c'est que vous êtes le produit »). Certes, les réseaux sociaux permettent parfois de réserver la visibilité des informations à son cercle d'amis. Néanmoins, puisque le succès de leur modèle économique dépend de la pertinence de leur collecte et de la revente des données personnelles des internautes, la base de leur fonctionnement est de demander à l'internaute de dévoiler le maximum d'informations le concernant, seule manière de découvrir de nouveaux « amis » partageant les mêmes goûts, ou de trouver des « relations » utiles.

Il peut également se révéler difficile de se désinscrire d'un réseau social et d'en faire disparaître toute trace. Si la suppression d'un compte est possible, l'internaute qui souhaite effacer tous les commentaires qu'il a postés sur les comptes des autres doit le faire manuellement, un par un, ce qui se révèle impossible en pratique. Il devient ainsi parfois difficile de faire disparaître des informations mises en ligne, qui pouvaient être considérées comme amusantes initialement, mais qui se révèlent gênantes par la suite. L'internaute doit alors supporter les conséquences de ces divulgations pendant le reste de sa vie.

Exemple La suppression de compte chez Facebook

Au 27 juin 2013, la politique d'utilisation des données de Facebook indiquait :

« Lorsque vous résiliez un compte, il est supprimé de façon permanente de Facebook. Un délai d'environ un mois est nécessaire pour supprimer un compte, mais certaines informations peuvent rester dans des copies de sauvegarde et dans des journaux d'activité jusqu'à 90 jours. »

Il était précisé que cette suppression ne concernait pas certaines actions :

« Certaines de vos actions sur Facebook, comme lorsque vous publiez dans un groupe ou envoyez un message à quelqu'un (lorsque votre ami peut encore avoir un message que vous avez envoyé même après la suppression de votre compte), ne sont pas enregistrées dans votre compte. Ces informations persistent même après la suppression de votre compte. »

Parfois, les informations n'ont pas été mises en ligne par l'internaute lui-même, mais par un ami, qui seul a le pouvoir éventuel de les faire disparaître du site. Les opinions et participations à des forums restent également en ligne. L'internaute perd ainsi ce que Baudelaire considérait comme deux droits de l'homme « assez importants » et « oubliés » : « le droit de se contredire et le droit de s'en aller »¹.

EXEMPLE Les publications des amis chez Facebook

Au 27 juin 2013, la politique d'utilisation des données de Facebook indiquait :

« Vos amis et d'autres personnes ont la possibilité de communiquer des informations vous concernant. Ils sont par exemple susceptibles de publier des photos ou d'autres informations relatives à votre personne, ou encore de vous identifier dans leurs publications. Si vous n'approuvez pas une de leurs publications, faites-le leur savoir ou signalez la publication. »

Pour montrer à quel point les informations disséminées sur les réseaux sociaux permettent de reconstituer la vie d'une personne, le magazine *Le Tigre* a publié² fin 2008 le portrait d'un internaute inconnu, reconstitué « grâce à toutes les traces qu'il a laissées, volontairement ou non » sur Facebook, YouTube, Flickr, etc. L'article vise à faire prendre conscience « qu'on ne fait pas vraiment attention aux informations privées disponibles sur Internet et que, une fois synthétisées, elles prennent soudain un relief inquiétant ». Il énumère donc toutes les informations glanées sur Marc L., 29 ans, architecte d'intérieur, habitant l'ouest de la France, amateur de voyages et de musique. Ses rencontres amoureuses et ses activités sont narrées par le détail. Comme le conclut le rédacteur, s'adressant à sa victime : « après tout, c'est de ta faute, tu n'avais qu'à faire attention ».

1. Charles Baudelaire, « Edgar Poe, sa vie ses œuvres », préface à la traduction des *Histoires extraordinaires*, 1856.

2. Raphaël Maltz, Marc L***, www.le-tigre.net, décembre 2008.

Le droit Les réseaux sociaux sont bien par nature soumis à la loi sur les données personnelles

Les réseaux sociaux, blogs et autres sites personnels, doivent-ils être considérés comme des « activités purement domestiques » et, à ce titre, être exemptés des obligations prévues par les lois de protection des données personnelles ?

La Cour européenne des droits de l'homme a tranché la question le 6 novembre 2003 en indiquant qu'une telle publication de données personnelles ne peut être considérée comme une activité domestique : en effet, cette exception « vise uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes ».

Des conséquences parfois douloureuses

Les exemples de jeunes surpris par les conséquences d'informations postées, par eux ou par des amis, sont très nombreux.

Quelques anecdotes illustrent comment Facebook peut dévoiler l'intimité de ses membres et de leurs relations, et les conséquences qui peuvent en découler. Par exemple, « mercredi 31 octobre 2007, le jeune Kevin C., stagiaire à l'Anglo Irish Bank, a prévenu ses supérieurs qu'il serait absent le lendemain pour "raisons familiales". Le 1^{er} novembre, son patron lui a envoyé sa réponse : "Mera de nous avoir prévenus. J'espère que tout va bien à New York. (Sympa la robe)." En pièce jointe, une photo de Kevin déguisé en fée en train de fêter Halloween. Son patron l'a trouvée quelques heures après la soirée sur le site communautaire Facebook. »^a

a. Marie-Catherine Bouth, « Facebook rêve de vendre votre vie privée », *Le Figaro*, 7 décembre 2007.

Le Conseil de l'Europe, organisation internationale chargée de veiller aux droits de l'homme a noté en 2008 que « la présence durable de contenus créés par des enfants ou les concernant [est] potentiellement nuisible pour leur dignité, leur sécurité, leur vie privée et leur honneur, maintenant et dans leur future vie d'adultes ». En conséquence, le Conseil « déclare qu'il

convient de veiller à ce qu'aucun historique des contenus produits par des enfants sur Internet, susceptible de porter atteinte à leur dignité, à leur sécurité et à leur vie privée ou de les rendre vulnérables, maintenant ou à un stade ultérieur de leur vie, ne soit accessible de façon durable ou permanente, excepté dans le cadre de la lutte contre les infractions ; [et] invite les États membres à étudier [...] la faisabilité de retirer ou de supprimer ce type de contenu – y compris ses traces (fichiers, journaux, archives, manipulations effectuées) – dans un délai raisonnablement court. »³

Dans le cadre judiciaire, plusieurs cas ont été signalés au Canada, où des photos ou des propos mis en ligne sur Facebook ou MySpace ont été utilisés par les procureurs dans des procès pour cerner la personnalité des accusés et justifier la peine requise.

« [Le procureur] pensait demander le sursis avec mise à l'épreuve pour Lara B., responsable du décès d'un passager de sa voiture dans un accident dû à la consommation d'alcool. Puis il a eu l'idée de consulter la page MySpace de la jeune femme où il découvrit des photos prises après l'accident mais avant le verdict, sur lesquelles Lara pose un verre à la main, plaisantant sur l'alcool. Le procureur a dès lors changé de stratégie et demandé de la prison ferme, photos en main pour appuyer ses propos. La jeune fille de 22 ans a été condamnée à une peine de deux ans. »^a

a. Erik Tucker, « Facebook et MySpace servent aussi aux procureurs », www2.anao.com, 19 juillet 2008.

Les internautes risquent aussi de mauvaises surprises lorsqu'ils cherchent un emploi. En effet, les recruteurs recherchent quasiment systématiquement sur Internet des informations sur les candidats, que ce soit sur des sites professionnels (LinkedIn, Viadeo) ou personnels (Facebook, Twitter...). Des demandeurs d'emploi peuvent alors être écartés à cause de photos

3. Conseil de l'Europe, déclaration du comité des ministres sur la protection de la dignité, de la sécurité et de la vie privée des enfants sur l'Internet, 20 février 2008.

provocantes ou déplacées, ou parce qu'ils ont publié des messages disant du mal de leur précédent employeur ou d'autres personnes, ou divulguant des informations confidentielles... Comme l'indiquait la Cnil dans son 30^e rapport annuel remis en 2010, 45 % des recruteurs américains consultaient les réseaux sociaux personnels ou professionnels (Facebook arrivant bien entendu en tête) pour trouver des informations sur des candidats et 35 % des recruteurs avaient déjà rejeté des candidatures suite à la consultation de leurs profils.

« Le champ des "impairs" numériques est large. Un amateur éclairé a connu des ennuis pour avoir été repéré sur des forums d'armes à feu. Une étudiante a été évincée d'un entretien après avoir été vue, en photo, accrochée à une barre de strip-teaseuse dans une fête de fin d'année. Attention donc, car des commentaires laissés sur des sites de jeu vidéo à l'âge de 14 ans peuvent vous suivre de longues années »^a.

a. Marie-Catherine Bouth, « Facebook rêve de vendre votre vie privée », *Le Figaro*, 7 décembre 2007.

Pour éviter la discrimination que constitue le fait d'écarter une personne d'une procédure de recrutement en se fondant sur un ou plusieurs motif(s) prohibé(s) par la loi, l'association française *À compétence égale* a proposé en 2010 une charte à tous les recruteurs et cabinets d'intérim. Les signataires s'engagent à sélectionner les candidats uniquement sur leurs compétences en excluant tout critère d'ordre personnel ou privé, et notamment à privilégier sur Internet les réseaux professionnels par rapport aux réseaux personnels, et enfin à ne pas utiliser les moteurs de recherche ni les réseaux sociaux comme outils d'enquête pour collecter, ou prendre connaissance d'informations d'ordre personnel, voire intimes, même si elles sont rendues accessibles par les utilisateurs eux-mêmes. Ont signé cette charte Viadeo, le Medef, Monster, l'Apec, Cadremploi, keljob.com, l'association des professionnels de l'intérim, le Syntec, etc.

Afin d'éviter aux jeunes de devoir supporter toute leur vie les conséquences de la mise en ligne de contenus dommageables,

l'État de Californie a adopté fin 2013 une loi permettant à tout mineur d'exiger des prestataires web ou mobiles l'effacement de contenus qu'il a publiés, sans avoir besoin de légitimer sa demande. Toutefois, ce droit n'est ouvert qu'aux internautes de moins de 18 ans, et ne concerne que les contenus qu'ils ont eux-mêmes publiés, pas les contenus publiés par des tiers.

Les données divulguées à l'insu de la personne concernée

Dans les exemples précédents, l'internaute avait lui-même divulgué les données personnelles le concernant. Cependant, il arrive également que certains membres de réseaux sociaux publient des informations concernant d'autres personnes qui ne sont parfois pas membres⁴, ou même que des réseaux revendent les profils de leurs membres à d'autres réseaux. Dans ces situations, les données concernant une personne peuvent se retrouver en ligne sans que celle-ci en soit informée et sans qu'elle ait les moyens de les faire disparaître, n'ayant pas accès aux réseaux en cause.

Le respect de la vie privée des tiers impose de recueillir le consentement de nos relations avant de mettre en ligne des données personnelles les concernant. Inversement, si nous découvrons que des informations personnelles nous concernant ont été publiées par un tiers, la première démarche à effectuer consiste à lui demander de les retirer. Une lettre recommandée avec accusé de réception peut s'avérer un bon moyen de résoudre rapidement le litige.

4. Comme l'indique la politique de confidentialité de Facebook au 2 juillet 2013, « Vos amis et d'autres personnes ont la possibilité de communiquer des informations vous concernant. Ils sont par exemple susceptibles de publier des photos ou d'autres informations relatives à votre personne, ou encore de vous identifier dans leurs publications. (...) Tout le monde peut vous identifier dans n'importe quoi. [...] Si vous ne souhaitez pas que quelqu'un vous identifie, nous vous recommandons de le leur dire. Si cela n'aboutit à rien, vous pouvez bloquer cette personne. Cela l'empêchera de vous identifier à l'avenir. »

Les recours en cas de publication par un tiers

Outre la simple courtoisie, cette demande de retrait peut être basée sur l'article 9 du Code civil, qui dispose que chacun a droit au respect de sa vie privée. Le droit à l'image peut également être invoqué en cas de photographie.

Notons que le Code pénal (article 226-1) punit d'un an d'emprisonnement et de 45 000 euros d'amende « le fait, au moyen d'un procédé quelconque, de porter volontairement atteinte à l'intimité de la vie privée d'autrui » :

1. en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
2. en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé ».

Toutefois, le Code pénal précise que « lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé. »

Rappelons par ailleurs que l'article 6-I de la loi pour la confiance dans l'économie numérique (LCEN) impose aux hébergeurs (et notamment aux réseaux sociaux) de retirer sans délai tout contenu jugé illicite. La personne dont des données personnelles sont publiées par un tiers peut donc demander au juge de constater en référé (c'est-à-dire en urgence) le caractère illicite des données en question (atteinte à la vie privée, ou abus de la liberté d'expression en cas d'injure ou de diffamation) et d'ordonner à l'hébergeur de les retirer.

Il ne faut pas masquer le fait que ces démarches ont un coût non négligeable. Les frais de conseil juridique et de procédure peuvent rapidement atteindre des montants importants, surtout si l'adversaire est une société étrangère, ce qui ajoutera des frais de traduction.

Enfin, en cas d'échec des procédures amiables ou judiciaires, reste le recours aux services d'agences web spécialisées dans le « nettoyage » de la e-réputation. Ces agences vont « noyer » les contenus négatifs sous une quantité importante de contenus positifs. Les informations gênantes ne seront pas supprimées du Web, mais les internautes trouveront en priorité les nouvelles informations, qui seront mieux référencées. Cette technique est appelée « obfuscation ».

Condamnation pour atteinte à la vie privée et au droit à l'image

Le 13 novembre 2013, le tribunal de grande instance de Paris a condamné à 3 000 euros de dommages-intérêts une personne qui, dans le cadre d'un conflit de copropriété, avait mis en ligne la photo de son voisin assortie de commentaires désagréables.

Le cas extrême du happy slapping

Le *happy slapping* est une pratique consistant à filmer une agression avec un smartphone, puis à diffuser le film sur Internet ou entre smartphones.

Jusqu'en 2007, ce délit n'était pas spécifiquement inscrit dans la loi. Cela n'empêchait pas d'en poursuivre les auteurs, par exemple pour non-assistance à personne en danger et (si les faits avaient été commis dans une enceinte privée) atteinte à la vie privée de la victime.

Condamnation pour agression d'un professeur

Le 27 juin 2007, un lycéen qui avait filmé l'agression de sa professeur par un camarade, et diffusé le film à ses condisciples, a été condamné à un an de prison dont six mois avec sursis, 5 000 euros de dommages-intérêts et 2 000 euros de frais de justice, pour non-assistance à personne en danger et atteinte à la vie privée (la salle de classe n'étant pas un lieu public). Le 10 novembre 2008, la cour d'appel de Versailles a confirmé ce

jugement, modifiant toutefois la peine en 18 mois de prison avec sursis et y ajoutant 1 000 euros de frais supplémentaires.

Toutefois, en 2007 a été créé un article 222-33-3 du Code pénal, selon lequel celui qui enregistre les images d'une agression est considéré comme complice, et encourt donc les mêmes peines que l'auteur principal. En outre, la diffusion de l'enregistrement est punie de cinq ans de prison et 75 000 euros d'amende.

Condamnation pour bizutage d'un stagiaire

Le 13 juin 2013, le tribunal correctionnel de Narbonne a condamné trois personnes qui avaient fait subir des humiliations à un stagiaire, avaient filmé la scène et l'avaient publiée sur des réseaux sociaux. Les peines ont été respectivement de douze mois de prison dont deux fermes, six mois avec sursis, et 150 heures de travaux d'intérêt général.

La collecte de données par les sites web

La navigation de l'internaute peut également être espionnée à son insu : Facebook collecte ainsi des informations sur tous les internautes qui visitent des pages comportant son bouton « J'aime », même si ceux-ci ne sont pas membres de Facebook ! Le réseau social recueille ainsi les adresses IP de tous les visiteurs de ces pages et tous les éléments de leur navigation sur le site, cela bien entendu sans leur consentement.

Ces données sont ensuite susceptibles d'être louées sous forme de fichier marketing, voire revendues.

En juin 2013, le fichier clients de l'enseigne culturelle Virgin, placée en redressement judiciaire, a été vendu pour 54 000 € à la Fnac. Ce fichier contenait les données de 1,6 millions de clients.

La situation devient inextricable si les données se retrouvent sur un réseau localisé à l'étranger ou hors de l'Union européenne. Le droit national devenant dès lors inopérant, une régulation devient indispensable pour inciter les acteurs à adopter d'eux-mêmes de bonnes pratiques de protection des données personnelles. C'est pourquoi la Cnil et ses homologues se sont emparés du sujet, au sein du G29 au niveau européen, et au niveau mondial dans le cadre de la Conférence internationale des commissaires à la protection des données et à la vie privée.

La vie conjugale

L'usage du numérique peut également avoir un impact sur la vie conjugale de l'internaute ! La Cour de cassation a ainsi jugé le 30 avril 2014 que la fréquentation intensive de sites de rencontres, en vue de trouver de nouvelles relations, constitue un manquement grave et renouvelé aux obligations du mariage et justifie un divorce aux torts de l'époux fautif.

Dans un autre dossier de divorce pour adultère, la Cour de cassation a indiqué le 17 juin 2009 que, puisque la preuve d'adultère peut se faire par tout moyen, la production de SMS du conjoint était possible, tant que ces SMS n'ont pas été obtenus par fraude ou par violence, ce qui exclut par exemple les mots de passe récupérés par un logiciel espion ou en utilisant à l'insu du conjoint la procédure de récupération de mot de passe, par exemple.

L'utilisation de Facebook peut également se révéler dangereuse. La découverte sur la page de son conjoint de discussions en ligne un peu trop intimes avec une tierce personne est toujours désagréable et conduit à la rupture. Un simple flirt numérique peut être considéré comme une entorse à l'obligation de fidélité qui découle du mariage.

Avatars et anonymat

Pour protéger sa e-réputation, il est recommandé, lorsqu'il n'y a pas d'intérêt à se servir de son identité réelle, d'utiliser un pseudonyme (avatar) ou même de rester anonyme.

 Martin Untersinger, *Anonymat sur Internet*, Eyrolles, 2013

Le droit à l'anonymat

Juridiquement, l'anonymat est un droit « en creux », c'est-à-dire qu'il n'est pas autorisé en toutes lettres par la loi, mais qu'il n'est pas interdit non plus. Plus précisément, la loi énumère un certain nombre de situations dans lesquelles il est obligatoire d'utiliser sa véritable identité (par exemple pour voter), ce qui signifie que dans les autres situations on n'y est pas obligé.

Les associations de protection de l'enfance recommandent notamment aux enfants et aux adolescents, lorsqu'ils font leurs premiers pas (ou leurs premiers clics) sur le Net et sur les réseaux sociaux, de ne pas utiliser leur vraie identité, ou au moins de ne pas divulguer leur nom de famille.

Le pseudonymat et l'anonymat permettent aussi de préserver la réputation de l'internaute, ainsi que sa liberté d'expression. Il peut ainsi librement donner son opinion sur la politique du gouvernement ou celle de son employeur, sans craindre de représailles.

Inversement, le droit à l'anonymat ne signifie pas la possibilité de publier des propos illicites (appel à la haine raciale, au meurtre, au terrorisme, apologie de la pédophilie, etc.) en toute impunité. Le propriétaire d'un blog, par exemple, même s'il reste anonyme pour le grand public, est tenu de déclarer sa véritable identité à son hébergeur et d'assumer ainsi ses éventuelles infractions.

Certains hommes politiques proposent régulièrement d'interdire l'anonymat sur Internet au motif qu'il protège les auteurs d'infractions. En 2010, le gouvernement avait ainsi répondu, par la plume de Nathalie Kosciusko-Morizet, alors secrétaire d'État à l'Économie numérique, à un député de la majorité qui proposait d'interdire l'anonymat sur Internet (réponse publiée au *Journal officiel* du 20 juillet 2010) :

« Une obligation de déclarer sa véritable identité sur Internet serait à la fois inopportune et inefficace. Elle serait en effet inopportune car elle entrerait en conflit avec la liberté d'expression. Pour donner un exemple, un blogueur n'osera plus donner son avis sur la politique de son entreprise ou sur celle du gouvernement, surtout s'il est fonctionnaire. Par ailleurs, une obligation de déclarer sa véritable identité sur Internet méconnaîtrait le fait que l'anonymat ou le pseudonymat sont deux des pratiques permettant la protection de la vie privée sur Internet. En dehors des situations où la vraie identité est indispensable, pour accéder à ses dossiers personnels par exemple, il est déconseillé de toujours utiliser sur Internet son vrai nom. [...] »

Une telle obligation serait d'autre part inefficace. [...] Obliger les internautes à publier leur identité ne les empêcherait pas de mentir s'ils le souhaitent, sauf à contraindre chaque internaute à détenir et à utiliser systématiquement des outils de preuve d'identité. »

Le mensonge comme technique de protection

Les internautes sont conscients des menaces qu'Internet fait peser sur leur vie privée et, pour se protéger, ils adoptent souvent spontanément une stratégie de mensonge calculé.

Une tendance ancienne...

En France, une enquête pionnière effectuée fin 2004⁵ – donc avant le développement des réseaux sociaux – auprès de 1 300 internautes, a mis en lumière leur comportement face aux demandes de données personnelles sur Internet.

Ainsi, cette enquête indiquait que :

- 21 % des internautes refusent de répondre « souvent ou toujours » et 33 % « parfois », aux formulaires en ligne ;

5. Enquête en ligne Vous et votre Identité Numérique, Caroline Lancelot-Milgrom, université Paris-Dauphine, présentation janvier 2006.

- si 14 % indiquent mentir « souvent ou toujours » dans leurs réponses, 69 % ne le font « jamais ou rarement » ;
- toutefois, 86 % ne remplissent pas les champs optionnels ;
- 52 % utilisent « souvent ou toujours » un pseudonyme et 26 % « parfois » ;
- 43 % ne donnent « jamais ou rarement » leur véritable identité et 24 % seulement « parfois ».

Contrairement à l'image d'inconscience propagée par les médias, les internautes interrogés ont donc conscience des risques que la dissémination des données personnelles sur Internet peut représenter pour leur vie privée.

Leur comportement doit être nuancé selon le site visité et la légitimité de la collecte de données. Les internautes acceptent de se dévoiler par ordre croissant dans les contextes suivants : pour entrer sur un site, discuter sur un forum, participer à un jeu-concours, s'abonner à une newsletter, obtenir des informations ou un document, et enfin acheter en ligne. Dans les premiers cas, ils acceptent facilement de dévoiler leur âge ou leur adresse mail et, logiquement, ne donnent leur numéro de carte bancaire que dans le dernier cas.

De manière logique, les internautes font également plus confiance aux sites d'un organisme public ou d'une entreprise qui leur est familière, qu'aux sites peu connus.

En conclusion, cette enquête montre que les utilisateurs des nouvelles technologies sont conscients des risques que celles-ci peuvent faire peser sur leur vie privée et développent en conséquence des stratégies de contournement ou de gestion de ces risques.

... qui se perpétue

Le baromètre ACSEL 2013 de la confiance numérique⁶ confirme que les internautes utilisent toujours cette tactique de camouflage pour protéger leurs données personnelles. Selon cette étude publiée en juin 2013, 92 % des internautes jugent important de limiter la durée de conservation des données personnelles. 78 % d'entre eux pensent que l'enregistrement des données bancaires sur un site marchand présente des risques et 75 % refusent d'être géolocalisés. 77 % ont déjà modifié leurs paramètres de confidentialité sur Facebook. Enfin, 16 % des internautes utilisent des pseudonymes sur les réseaux sociaux et 47 % donnent volontairement de fausses informations en ligne, principalement pour limiter la diffusion d'informations personnelles.

Cette étude confirme par ailleurs une autre tendance qui apparaissait déjà dans les éditions précédentes de ce baromètre : la confiance en Internet s'érode (les réseaux sociaux recueillant sans surprise le taux de confiance le plus bas, mais les sites « sérieux » de l'administration ou des banques sont également affectés par cette baisse de la confiance), ce qui pourtant n'empêche pas les gens de l'utiliser de plus en plus largement. La valeur d'usage des services web est telle que l'on ne peut pas s'en passer, même si l'on n'a pas confiance.

L'utilisation de réseaux anonymisés

Pour protéger leur anonymat vis-à-vis des sites web, et éventuellement pour déjouer la surveillance des échanges électroniques par les États, les internautes peuvent utiliser des réseaux chiffrés. Ces systèmes offrent le triple avantage de protéger l'anonymat de leurs utilisateurs, de cacher l'adresse des services web qu'ils utilisent et de garantir la confidentialité

6. www.acsel.asso.fr

des échanges en les chiffrant. Ils sont très utiles dans les États où le gouvernement cherche à limiter la liberté d'information et d'expression des citoyens en contrôlant leurs navigations ; ils sont évidemment très utiles aussi aux personnes ayant des activités illicites à cacher.

Le plus connu de ces réseaux est TOR (*The Onion Router* : le routage en oignon). Il s'agit d'un réseau mondial décentralisé d'ordinateurs, qui se transmettent les flux Internet de l'un à l'autre en occultant l'adresse IP de l'ordinateur de l'internaute : chaque serveur ne connaît que les identités du serveur qui le précède et de celui qui le suit dans la chaîne de transmission du flux. Les échanges sont chiffrés et donc confidentiels. Toutefois, des chercheurs français ont démontré la possibilité d'attaques visant à casser la confidentialité de TOR, et il semble que des organismes d'État comme la NSA américaine les aient mises en œuvre.

L'identité numérique

L'usurpation d'identité

Le droit général

L'interdiction de l'usurpation d'identité constitue une croyance courante. Et pourtant, le droit français n'interdit pas l'usurpation d'identité en tant que telle. Le fait d'utiliser le nom d'une autre personne ne constitue pas une infraction, si on se borne à l'utiliser. L'article 434-23 du Code pénal réprime certes « le fait de prendre le nom d'un tiers », mais seulement « dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales ». Ce fait « est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende ». L'usurpation d'identité n'est donc visée par la loi que lorsqu'elle sert à couvrir d'autres infractions.

Par ailleurs, le Code pénal prévoit et réprime :

- le délit d'escroquerie (« le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende », article 313-1) ;
- ainsi que « le fait, dans un acte public ou authentique ou dans un document administratif destiné à l'autorité publique et hors les cas où la réglementation en vigueur autorise à souscrire ces actes ou documents sous un état civil d'emprunt :
 - 1^o de prendre un nom ou un accessoire du nom autre que celui assigné par l'état civil ;
 - 2^o de changer, altérer ou modifier le nom ou l'accessoire du nom assigné par l'état civil » (article 433-19) ;
- et enfin l'usage de faux (« toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit » : trois ans d'emprisonnement et 45 000 euros d'amende, article 441-1).

Le droit traditionnel réprime donc déjà plusieurs types d'infractions basées sur l'usurpation d'identité.

Le droit face aux défis d'Internet

Depuis 2011, a été ajouté au Code pénal un article 226-4-1 qui dispose que « 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, est puni d'un an d'emprisonnement et de 15 000 € d'amende. »

Il complète ainsi la liste des circonstances dans lesquelles l'usurpation d'identité est répréhensible, en y ajoutant les atteintes à la tranquillité et à l'honneur ou à la considération.

Cet article, souvent désigné dans la presse comme le nouveau « délit d'usurpation d'identité sur Internet », vise pourtant les usurpations commises de manière générale, que ce soit dans le monde réel ou dans le monde virtuel.

Notons enfin que ce nouvel article, au-delà de l'usurpation d'identité, vise plus largement l'usage « d'une ou plusieurs données de toute nature ». Il permettra ainsi, sans doute, de réprimer les usurpations de mot de passe, de pseudonyme, d'adresse mail, voire d'adresse IP, qui ne sont pas *stricto sensu* des usurpations d'identité, mais qui peuvent conduire aux mêmes dommages pour la victime. Il aurait d'ailleurs été judicieux de modifier à la même occasion l'article 434-23 pour reprendre la même rédaction.

Toutefois, il n'était pas évident que la création d'un nouveau délit soit indispensable pour réprimer ce type d'usurpation. La jurisprudence a ainsi montré que le vol de mot de passe et le *phishing* (envoi d'e-mails piégés en usurpant le nom et le logo d'expéditeurs légitimes), qui n'existent pas en tant qu'infractions dans le Code pénal, peuvent néanmoins être efficacement réprimés sur le fondement d'autres infractions existantes, par exemple :

- l'escroquerie ⁷;
- l'accès non autorisé à un système automatisé de traitement de données (articles 323-1 et suivants du Code pénal) ⁸;
- la collecte frauduleuse des données personnelles de la victime (article 226-18 du Code pénal) ;

7. TGI Paris, jugement du 2 septembre 2004.

8. TGI Paris, jugement du 2 septembre 2004.

- ou enfin la contrefaçon du site web ou de la marque de la personne morale dont l'identité a été usurpée (en utilisant les délits prévus par le Code de la propriété intellectuelle)⁹.

Dans ces circonstances, l'instauration d'un nouveau délit d'usurpation d'identité sur Internet ne prend tout son sens que si elle sert à sanctionner des comportements moralement répréhensibles, mais qui échappaient encore à la loi. Par exemple, le législateur souhaite-t-il sanctionner un canular comme la création par un farceur d'un profil de Facebook sous le nom d'Alain Juppé en 2007 ? La généralisation des réseaux sociaux donne une actualité forte à cette question, puisqu'il est facile d'y ouvrir une page sous le nom d'une autre personne. Cette usurpation peut être une farce innocente ou, comme dans le cas de l'usurpation d'Alain Juppé, une mise en garde, mais elle peut aussi être l'occasion de recueillir, *via* les contacts obtenus, des informations personnelles sur la personne usurpée (par exemple, dans une autre affaire survenue en 2007, des informations sur l'appartenance de cette personne à la franc-maçonnerie¹⁰).

Zoom Le faux Alain Juppé

« J'ai voulu montrer que sur ce type de site dont l'utilisation est en train d'exploser, on peut facilement se cacher sous un faux profil », a déclaré à Reuters l'internaute [l'auteur de la fausse page Facebook d'Alain Juppé], qui a souhaité garder l'anonymat. [...] L'homme, âgé d'un peu plus de trente ans, a précisé que « (s)on seul but était de montrer les limites de tels sites qui peuvent être utiles par ailleurs ». Pour lui, « le danger vient du fait que les internautes peuvent être trompés et qu'ils doivent être absolument informés que n'importe qui peut se cacher derrière une photo, une signature ou un profil ».^a

a. Reuters, « De faux Alain Juppé et Alain Roussot sur Facebook », 5 décembre 2007.

9. TGI Paris, jugement du 21 septembre 2005.

10. Karine Papillaud, « Identité numérique, bas les masques ! », *Le Monde* 2, 17 novembre 2007, pp. 46-47.

Une telle usurpation du nom d'autrui peut également servir à déconsidérer la personne en question, par exemple en lui attribuant des propos certes honorables et licites, mais contraires à ses convictions ou à ses engagements politiques ou associatifs. Par exemple, publier (que ce soit sur Internet ou sur papier) sous le nom d'Alain Juppé, élu de Bordeaux, un éloge du vin de Bourgogne, constituerait-il réellement une « atteinte à son honneur ou à sa considération », bien que cela constitue sans doute une atteinte à son électorat ? L'affaire aurait sans doute pour conséquence de « troubler sa tranquillité », mais il n'y aurait pas nécessairement eu volonté de créer ce trouble. Bref, le nouvel article 226-4-1 pourrait-il être invoqué dans de telles circonstances ?

Jurisprudences pour usurpation d'identité sur Internet

L'usurpation d'identité sur les réseaux sociaux ou dans des e-mails peut être utilisée pour nuire à la réputation de la victime.

Le tribunal de grande instance de Carcassonne a condamné, le 16 juin 2006, à 10 000 euros d'amende et 18 000 euros de dommages-intérêts divers, une personne qui avait créé un faux profil de sa victime sur des sites de rencontre. La condamnation a été prononcée sur la base de la violence avec préméditation suivie d'une incapacité de travail supérieure à huit jours.

Au Royaume-Uni, la High Court de Londres a condamné à 22 000 £ de dommages-intérêts une personne qui avait créé un faux profil Facebook de sa victime, contenant des informations fausses et diffamatoires sur sa vie privée et sur son honnêteté (24 juillet 2008).

Le 29 mars 2006, la cour d'appel de Colmar a condamné un prévenu à trois mois de prison avec sursis pour avoir utilisé le nom d'une autre personne afin d'envoyer des e-mails susceptibles d'entraîner contre ce dernier des poursuites pénales.

Mais cette décision a été cassée, car la cour n'avait pas précisé en quoi les e-mails pouvaient entraîner des poursuites.

La cour d'appel de Paris a condamné, le 10 octobre 2014, à dix mois de prison avec sursis et 30 000 euros de dommages-intérêts, sur la base de l'article 226-4-1 du Code pénal, une personne qui, par vengeance, avait usurpé l'identité d'un de ses anciens associés pour créer des adresses électroniques et des comptes Facebook contenant des messages diffamatoires et insultants.

Le 18 décembre 2014, le tribunal de grande instance de Paris a condamné sur la même base à 3 000 euros d'amende une personne qui avait piraté pour s'amuser le site web d'une personnalité politique, usurpant ainsi son nom.

Enfin, le tribunal correctionnel de Montbéliard a condamné, le 8 janvier 2015, à quatre mois de prison avec sursis et à 1 000 euros d'amende un homme qui, pour se venger d'avoir été éconduit par une femme, avait créé au nom de celle-ci une page Facebook contenant des messages sexuellement explicites.

La preuve d'identité sur Internet

Ainsi que nous venons de le constater, la notion d'identité n'a pas de définition légale. *A fortiori*, la notion d'identité numérique peut selon les interlocuteurs recouvrir de nombreuses réalités. D'une part, au sens large, l'« identité numérique » peut désigner *l'image que l'individu donne de lui-même sur Internet*. Chacun a le droit d'utiliser des pseudonymes sur le Web et donc de se construire, selon cette définition, autant d'identités numériques qu'il a d'avatars. « Identité numérique » est alors synonyme de « personnage sur le Web » ou de « e-réputation ». D'autre part, au sens régalien, on peut trouver le terme « identité numérique » utilisé par métonymie pour exprimer un « *moyen numérique de preuve de l'identité* ». Cette preuve peut servir uniquement dans le monde réel (par

exemple un passeport électronique), ou bien servir aussi à prouver l'identité sur Internet.

Dans ce qui suit, nous nous restreindrons à cette dernière définition et nous entendrons par « identité numérique » les moyens de *prouver son identité sur Internet*.

Cette preuve de l'identité dans le monde numérique (réseaux, Internet) s'effectue techniquement en deux temps :

1. dire son identité (*identification* proprement dite) ;
2. la prouver (*authentification*).

On distingue « l'authentification faible », lorsque la preuve apportée n'est pas très fiable (mot de passe, par exemple), et « l'authentification forte », lorsqu'elle s'appuie sur des éléments plus difficiles à frauder et demeurant sous le contrôle de leur titulaire (carte à puce, biométrie...).

Une telle démarche n'a aucune raison d'être systématique : l'internaute a toujours le droit de naviguer de manière anonyme ou en adoptant des pseudonymes. La preuve d'identité doit se limiter aux seuls services qui justifient cette exigence, comme l'accès à des dossiers personnels.

Les usages de l'identité numérique

Ainsi, l'authentification est utile pour accéder à de nombreux services à forte valeur ajoutée, qu'il s'agisse de ses propres dossiers (comme le dossier médical personnel ou DMP) ou de ceux des autres (dans le cas du DMP, le médecin traitant a accès au dossier de ses patients, sous réserve de prouver qu'il est bien leur médecin traitant). Dans une entreprise, l'accès à des informations confidentielles doit également être réservé à certains utilisateurs. L'identité numérique peut aussi servir à accomplir en ligne certaines formalités, comme des déclarations administratives, fiscales ou sociales, l'inscription à des concours, l'ouverture de droits sociaux...

Zoom Les enjeux

Les enjeux sont considérables. Une étude de l'Afnor (2008) estime que la généralisation en France de la dématérialisation des échanges des ménages représenterait plusieurs milliards d'euros par an en diminution des coûts et gains de productivité (40 millions pour le commerce en ligne, 1,3 milliard pour le secteur financier, 150 millions pour les assurances, 1,3 milliard pour les administrations...). À lui seul, l'envoi par courriel avec accusé de réception électronique des convocations aux assemblées générales de copropriété représenterait un gain de pouvoir d'achat de 250 M€/an pour l'ensemble des ménages !

Ce besoin d'utiliser l'identité numérique concerne ainsi les entreprises aussi bien que les administrations, les citoyens aussi bien que les clients ou les employés : il s'agit d'un besoin transversal, qui appelle des solutions également transversales.

L'actualité montre quasi quotidiennement que les attaques ne sont pas que théoriques : les comptes de Nicolas Sarkozy et de Barack Obama ont été piratés, ainsi que les systèmes informatiques du ministère des Finances ou de Sony... Les campagnes de phishing se multiplient, alors que les moyens de protection actuels, basés principalement sur les mots de passe, atteignent leurs limites : toutes les études montrent qu'un nombre toujours important d'internautes choisit des mots de passe trop simples (« 123456 » et « azerty » restent des classiques).

Les solutions techniques

Plusieurs technologies servent à prouver en ligne que l'on est bien qui l'on prétend être.

- Le mot de passe : simple mais notoirement dépassé, les gens ayant tendance à choisir des mots trop simples et à les utiliser trop longtemps et sur trop de sites à la fois.
- Le mot de passe à usage unique : la personne est en possession d'une liste de codes utilisables une seule fois. Cette solution est utilisée en France par des banques (groupe Cré-

dit Mutuel-CIC). Au Danemark, le système NemID sert aussi bien aux banques qu'à l'administration électronique.

- Des codes à usage unique (OTP : *One-time password*) envoyés par SMS ou générés par une mini-calculatrice dédiée.
- La biométrie (empreintes digitales, iris de l'œil...). Depuis 2013, l'iPhone et l'iPad comportent ainsi un dispositif de reconnaissance de leur propriétaire par empreinte digitale.
- Des clés numériques logées dans une puce (carte à puce, clé USB sécurisée, carte SIM du smartphone...).

Dans cette dernière catégorie, on compte les identités numériques distribuées par certains États. Par exemple, en Europe, plusieurs pays ont décidé depuis une quinzaine d'années de doter leurs citoyens d'identités numériques implantées dans la carte d'identité. Cette dernière devient ainsi une carte à puce, au format d'une carte bancaire, contenant des clés que l'internaute peut utiliser en connectant la carte à l'ordinateur grâce à un lecteur.

La Finlande propose ainsi des cartes d'identité électroniques facultatives à ses citoyens depuis 1999 : 444 000 ont été distribuées. L'Italie, la Suède et Monaco l'ont imitée. En Belgique et en Estonie, où ces cartes sont obligatoires, toute la population en est équipée, soit respectivement 8,3 et 1,1 millions de personnes. En Espagne et au Portugal, où elles sont obligatoires également, le déploiement est en cours avec respectivement 38 et 4 millions de cartes distribuées en 2013. L'Allemagne a distribué 21 millions de cartes depuis 2010. La Lituanie, la Lettonie et la République tchèque ont également commencé à distribuer les leurs. Ainsi, plusieurs dizaines de millions de citoyens européens disposent déjà d'outils d'identité numérique émis par les États.

DEJÀ. Et la France ?

En France, un projet semblable a été lancé en 2004 par le ministère de l'Intérieur. Plusieurs fois repoussée, une loi créant une carte d'identité électronique a été adoptée par le Parlement en 2012. Cependant, le Conseil constitutionnel a censuré les dispositions concernant les fonctionnalités d'identité numérique utilisables sur Internet (« puce e-services »). En l'état actuel des textes, la carte nationale d'identité électronique française, si elle est lancée, serait donc seulement un titre d'identité et de voyage. L'insertion éventuelle de fonctionnalités d'identité numérique dans cette carte nécessiterait un nouveau texte de loi.

Pour faciliter l'usage de l'identité numérique dans toute l'Union européenne, celle-ci a adopté en 2014 un règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur. Ce texte instaure, à partir de juillet 2016, des règles communes dans toute l'Union pour l'authentification forte. Chaque État pourra notifier à la Commission des systèmes nationaux d'identité numérique.

Les autres États membres de l'Union devront alors reconnaître les identités électroniques notifiées inscrites sur la liste publiée par la Commission, et les accepter pour leurs services d'administration électronique. Ce texte ne crée toutefois aucune obligation pour un État de l'Union de délivrer ou de faire délivrer des identités numériques, ni de notifier à la Commission celles qu'il délivre ou fait délivrer.

Toutefois, il n'y a pas que l'État qui puisse vérifier l'identité d'une personne et lui remettre une puce électronique utilisable sur Internet. Des entités parapubliques ou privées sont également en capacité de le faire. C'est ainsi qu'en Europe existent d'autres systèmes, où les émetteurs des identités numériques ne sont pas l'État. Parfois, ces systèmes coexistent avec une carte d'identité électronique, comme en Suède où les entreprises et les universités peuvent équiper leurs salariés ou leurs étudiants de cartes reconnues officiellement dans tout

le pays. En Finlande, en Estonie, en Norvège et de nouveau en Suède, banques et opérateurs mobiles équiper leurs clients ; en Italie, ce sont les régions et les chambres de commerce qui développent des offres. Parfois, ces systèmes non étatiques constituent la seule solution d'identité numérique disponible, comme en Suisse, en Autriche ou en Norvège, où la loterie nationale représente le principal émetteur... Les outils remis aux internautes sont toujours basés sur la même technologie que les cartes d'identité électroniques, mais le format du support peut varier (clé USB sécurisée, téléphone mobile...). Ces formats facilitent l'utilisation de l'identité numérique pour des navigations en situation de nomadisme, que ce soit sur un ordinateur portable, sur une tablette ou sur un smartphone, et sont donc en phase avec l'importante augmentation de l'Internet mobile, qui est sur le point de dépasser l'Internet fixe. Au total, le nombre d'internautes européens dotés de ces outils non étatiques est du même ordre de grandeur que celui des porteurs de cartes d'identité électroniques.

Enfin, les grands acteurs américains d'Internet se lancent eux aussi sur le marché de l'identité numérique. En effet, Facebook, Google, Apple, PayPal... comptent des centaines de millions de clients qu'ils connaissent très bien et dont ils peuvent sécuriser facilement l'identité en la reliant à un compte bancaire ou à une puce (carte SIM d'un iPhone par exemple). Ils ont ainsi la capacité de proposer rapidement à des millions d'internautes une identité numérique facile à utiliser, qu'ils pourront valoriser en vendant aux sites web le « service » constitué par la vérification d'identité. Facebook Login (authentification faible puisque Facebook ne vérifie pas si l'internaute s'inscrit sous son vrai nom) est déjà accepté par plus de 7 millions de sites dans le monde. PayPal (identité consolidée par l'existence du compte bancaire associé) est accepté comme identité numérique des internautes par l'administration électronique britannique. Google+ et Microsoft Account ont lancé en 2013 leur authentification « à deux

facteurs », en couplant le mot de passe habituel à l'envoi d'un SMS sur le téléphone portable de l'internaute (identité consolidée par l'existence de l'abonnement mobile). Google a annoncé travailler à la distribution de certificats sur clés USB sécurisés, ce qui serait l'équivalent des systèmes non étatiques décrits précédemment, mais à l'échelle mondiale. Apple a lancé en 2014 TouchID qui permet aux applications mobiles d'utiliser le lecteur d'empreinte de l'iPhone. PayPal expérimente un système de paiement en boutique avec un compte PayPal, en communiquant au commerçant la photo du titulaire du compte à des fins de vérification d'identité. Enfin, au Nigéria, la distribution des cartes d'identité électroniques se fait depuis 2014 sous l'égide de Mastercard. Ces acteurs globaux, qui disposent déjà de comptes pour presque tous les internautes et qui peuvent valider les identités de ces derniers à un coût marginal très faible, ont de fortes chances de dominer le monde de l'identité numérique dans les années à venir.

LE POINT DE VUE DU SPÉCIALISTE **Olivier Itéanu, avocat à la cour d'appel de Paris, chargé d'enseignement aux universités de Paris I et de Paris XI, représentant européen auprès de l'ICANN**

Peut-on agir de manière anonyme sur Internet ?

L'anonymat absolu n'existe pas sur Internet. Il vaudrait mieux parler de pseudonymat, c'est-à-dire d'une identification empruntant des identifiants non répertoriés par les autorités publiques et autogérés. Pourquoi répondre non à l'anonymat ? Parce que les obligations de traçabilité sont désormais bien ancrées dans la loi ; elles signifient que toutes traces laissées sur les réseaux doivent être collectées et enregistrées. Elles concernent en premier lieu les opérateurs de communications électroniques, ex-« opérateurs de télécoms », plus généralement les intermédiaires techniques, parmi lesquels au premier chef les hébergeurs, qui ont une obligation légale de procéder à cette traçabilité en conservant toute trace pendant un an à compter de son enregistrement. Ces opérateurs et intermédiaires répondent quotidiennement ensuite à des centaines de demandes présentées par les autorités publiques ou par des personnes privées

ayant obtenu une injonction de la justice. À cela s'ajoute que ces traces sont exploitées au sein des organisations dans le cadre de la cybersurveillance, dont la légalité est étroitement surveillée par la justice. Enfin, si on ajoute encore à tout cela, les interceptions et captations de sécurité de tous les services de police et agences de renseignements d'un bon nombre d'États avancés dans le monde, on se rend compte qu'il est difficile de parler d'un anonymat absolu sur Internet.

Quelles sont les limites légales au choix et à l'usage d'un pseudonyme ?

Le pseudonyme est destiné à s'afficher en public. Il doit donc, comme tout message public, respecter l'ordre public (lutte contre le racisme, l'antisémitisme et l'homophobie principalement) et le droit des tiers (injure ou diffamation de tiers). En outre, comme le pseudonyme peut servir à des tas de choses d'ordre commercial ou pas, son titulaire doit, en fonction de cet usage, s'interroger sur le respect du droit des marques. Par ailleurs, il faut s'inquiéter de vérifier qu'on ne se trouve pas sur un cas d'usurpation d'identité. Tout cela paraît au final un catalogue de droits privatifs difficile à appréhender par le simple internaute. En réalité, derrière ces règles, il y a beaucoup de bon sens paysan que chacun ressent. J'ajouterai enfin, qu'à l'inverse, on peut imaginer qu'un pseudonyme se trouve dans le commerce juridique, c'est-à-dire qu'il donne lieu à vente (cession) ou location (concession). Ces opérations seront facilitées si le pseudonyme est déposé à titre de marque, ce qui est tout à fait possible.

Quel est le statut juridique des avatars ?

À ce jour, il n'existe pas de statut juridique des avatars. Pour autant, l'avatar n'est pas totalement absent de notre corpus juridique. Par exemple, on en trouve trace dans les dispositions particulières relatives à la pédophilie, soit l'article 227-23 du Code pénal. Les textes punissent « l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique », ce qui clairement s'applique au cas de l'avatar. Le dernier alinéa prévoit même que « les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur ». La jurisprudence a ainsi déjà dit en 2007 que les dispositions que nous rappelons sur la pédophilie s'étendent « aux images non réelles représentant un mineur imaginaire, telles que des dessins ou des images résultant de la transformation d'une image réelle^a ». Elle a condamné une société pour avoir diffusé des dessins animés mettant en scène un jeune enfant ayant des relations sexuelles avec des femmes adultes. La diffusion d'images représentant un avatar d'apparence mineur, en pleine activité sexuelle, alors même qu'aucun enfant n'est impliqué, devrait tomber sous le coup de ce texte. Au-delà de ce cas encore isolé, il n'est pas du tout exclu que le droit s'intéresse à l'avatar dans les années à venir. Le droit n'est pas réservé aux êtres faits de chair et de sang. L'exemple des personnes morales et des sociétés est là pour le confirmer.

a. Cour de cassation, chambre criminelle, 12 septembre 2007 : Dalloz 2008 n° 2 p.827.

Comment protéger sa vie privée, y compris sur les réseaux sociaux ?

Il y a au moins trois mesures à prendre. En premier lieu, être le stratège de son identité, c'est-à-dire limiter la révélation de cette identité et des éléments qui la composent seulement lorsque c'est pertinent, et uniquement à des personnes de confiance. Réagir à toute atteinte à votre identité, dès connaissance d'une tentative d'atteinte telle qu'une usurpation. Il existe désormais un ensemble de règles juridiques en vigueur qui permettent de réagir dès la tentative. Par exemple, pour l'usurpation d'identité, l'article 226-4-1 du Code pénal qui réprime « 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 », en le punissant « d'un an d'emprisonnement et de 15 000 € d'amende ». Cette démarche consistant à porter plainte auprès d'un commissariat, d'une brigade de gendarmerie ou par courrier adressé au parquet du tribunal de grande instance dont on dépend, est défensive ; elle tend à prévenir les conséquences de l'atteinte à l'identité, par exemple des créanciers qui poursuivraient celui qu'ils croiraient être le débiteur. Il faut donc se placer tout de suite en victime, la plainte y aidera. Enfin, il ne faut pas hésiter à rechercher l'origine de cette atteinte, alerter ses proches, car c'est souvent là que se trouve le fauteur.

📖 Olivier Itéanu, *L'identité numérique en question*, Eyrolles, 2008

5 Les droits d'auteur

La lutte contre le téléchargement illégal a fait largement connaître la problématique du droit d'auteur sur Internet et a reposé la question de l'équilibre entre les intérêts des auteurs, de leurs producteurs et du public.

L'informatique donne à chacun la capacité de recopier un contenu à l'identique en quantité illimitée. Quelles sont les conséquences sur la rémunération des auteurs de ces contenus ? Quelles sont les limites à respecter ?

À l'origine de la propriété intellectuelle

Tout travail mérite salaire. Il est souhaitable que celui qui crée une œuvre ou une invention puisse en tirer des bénéfices et que la reproduction et l'exploitation de cette création soient encadrées. L'hypothèse de départ, pragmatique, est que sans l'incitation que constitue l'espoir d'une récom-

pense, l'auteur d'une création n'aurait pas fait l'effort de mener celle-ci à son terme. Et même si un artiste peut créer pour le plaisir (encore qu'il doive tout de même gagner sa vie, lui aussi), il va de soi que les éditeurs, imprimeurs et distributeurs ne vont pas travailler gratuitement. Le principe de légitime rétribution de ceux qui ont contribué à créer et à faire connaître une œuvre matérialise le respect de leur travail.

Le droit de propriété intellectuelle n'est toutefois pas absolu. La loi va instaurer un équilibre entre les droits de l'auteur et ceux du public.

La propriété intellectuelle sur une œuvre ou sur un produit consacre les droits de son créateur à contrôler l'exploitation qui en est faite et à jouir des revenus de celle-ci. Cette propriété peut prendre plusieurs formes :

- la propriété littéraire et artistique, pour les œuvres de l'esprit (littérature, sculpture, peinture, musique...), leur reproduction et leur interprétation éventuelles ;
- les logiciels et bases de données ;
- la propriété industrielle, qui recouvre les marques, logos, secrets de fabrication, brevets, dessins et modèles, etc.

Un internaute qui souhaite publier des photos, des textes, des images, télécharger ou mettre en ligne des vidéos ou des musiques, copier ou utiliser un logiciel, ou utiliser une base de données, peut le faire en respectant les règles de la propriété intellectuelle.

Les différents droits, les procédures à suivre pour les assurer et les sanctions en cas d'infraction, font l'objet du Code de la propriété intellectuelle (CPI).

Propriété littéraire et artistique : encadrement de la reproduction

Le Code de la propriété intellectuelle prévoit que « l'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. »

Notons qu'aucun dépôt ni aucune formalité ne sont nécessaires : le seul acte de création suffit à établir les droits de son auteur.

Ce droit est incorporel car il n'est pas lié à la possession de l'objet matériel (par exemple : sculpture ou tableau) : par le seul fait d'avoir créé l'œuvre, et même s'il l'a vendue, le créateur jouit de différents droits :

- droits moraux de divulgation, d'opposition à une modification de l'œuvre, d'y attacher son nom ;
- droits patrimoniaux d'exploitation (représentation et reproduction de l'œuvre).

Qui est concerné ?

L'article L112-2 du CPI prévoit que « sont considérés notamment comme œuvres de l'esprit :

- 1° les livres, brochures et autres écrits littéraires, artistiques et scientifiques ;
- 2° les conférences, allocutions, sermons, plaidoiries et autres œuvres de même nature ;
- 3° les œuvres dramatiques ou dramatico-musicales ;
- 4° les œuvres chorégraphiques, les numéros et tours de cirque, les pantomimes, dont la mise en œuvre est fixée par écrit ou autrement ;
- 5° les compositions musicales avec ou sans paroles ;
- 6° les œuvres cinématographiques et autres œuvres consistant dans des séquences animées d'images, sonorisées ou non, dénommées ensemble œuvres audiovisuelles ;
- 7° les œuvres de dessin, de peinture, d'architecture, de sculpture, de gravure, de lithographie ;

8° les œuvres graphiques et typographiques ;
 9° les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie ;
 10° les œuvres des arts appliqués ;
 11° les illustrations, les cartes géographiques ;
 12° les plans, croquis et ouvrages plastiques relatifs à la géographie, à la topographie, à l'architecture et aux sciences ;
 13° les logiciels, y compris le matériel de conception préparatoire ;
 14° les créations des industries saisonnières de l'habillement et de la parure. »
 Cette liste n'est pas limitative : en effet, le CPI protège « toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination » (article L112-1).
 Les traductions sont également protégées, ainsi que les anthologies (article L112-3).

Droit d'auteur sur une photo

Le 20 décembre 2012, le tribunal de grande instance de Paris a précisé les conditions nécessaires pour qu'une photo soit protégée par le droit d'auteur. Le tribunal a rappelé qu'« une photographie n'est protégeable par le droit de la propriété intellectuelle que dans la mesure où elle procède d'un effort créatif et qu'elle ne vise pas seulement à reproduire de la manière la plus fidèle possible un objet préexistant. » Une photographie banale n'est pas protégeable ; pour revendiquer la qualité d'auteur, le photographe doit avoir opéré des « choix [techniques] personnels en vue de produire un effet particulier ». Par ailleurs, une fois qu'il est établi qu'une photo est protégée par le droit d'auteur, la personne revendiquant ce droit doit apporter la preuve qu'elle en est bien l'auteur. Dans ce cas précis, le tribunal a jugé que le fait de publier une photo sur un site web ne permet pas de présumer qu'on en est l'auteur, si on ne l'avait pas explicitement précisé au moment de la mise en ligne.

Droit d'auteur sur un tableau

Le propriétaire d'un tableau n'a pas le droit de le reproduire sur son site Internet ou sur des objets publicitaires sans l'autorisation de l'auteur. En effet, ce dernier a cédé l'œuvre, mais pas les droits incorporels de reproduction ou de modification. Le tribunal de grande instance de Paris a ainsi condamné le 21 juin 2013 une société à payer 3 500 euros de dommages (plus 2 000 euros de remboursement des frais de justice) au peintre à qui elle avait acheté un tableau qu'elle avait par la suite utilisé pour décorer sa boutique, son véhicule utilitaire, ses objets publicitaires et son site web.

Droit d'auteur sur un tweet

Un tweet est-il une « œuvre de l'esprit », et à ce titre protégeable par le droit d'auteur ? La question n'est pas que théorique : la pratique du reweet, qui consiste à rediffuser les tweets d'autrui, fait partie intégrante du fonctionnement de Twitter, et peut laisser place à une tentation de s'appropriier l'œuvre d'autrui. En 2010, un photographe de presse a ainsi attaqué l'AFP, qui avait utilisé sans son autorisation et sans citer son nom une de ses photos publiée sur Twitter.

Pour être protégée, il faut que la rédaction du tweet soit suffisamment originale. Une simple information factuelle n'est pas une œuvre de l'esprit. En revanche, les mots d'humour, les prises de position, les rédactions surprenantes, peuvent le devenir. En janvier 2014, l'éditeur Larousse a publié un ouvrage intitulé *Les perles des tweets et du Net*, reprenant des tweets marquants, sans l'accord de leurs auteurs, sans citer leur nom et sans les avoir informés. Devant la menace de procès en contrefaçon et en violation du droit d'auteur, l'éditeur a rapidement retiré l'ouvrage de la vente.

Les droits de divulgation et d'exploitation

Les droits moraux de l'auteur

Les droits moraux visent à assurer le contrôle de l'auteur sur l'œuvre qu'il a créée.

L'auteur jouit du *droit de divulgation* : lui seul a le droit de divulguer son œuvre, de déterminer les procédés de divulgation et les conditions de celle-ci.

Il est également maître du *respect de l'œuvre* : il peut s'opposer à toute dénaturation de son œuvre (par exemple, un architecte peut refuser une modification d'un bâtiment dont il est l'auteur). Il peut exiger que son nom soit attaché à l'œuvre.

Ces droits moraux sont *incessibles* ; l'auteur en jouit jusqu'à sa mort. Après sa mort, son nom reste attaché à l'œuvre.

Les droits patrimoniaux

Les droits patrimoniaux visent à rétribuer l'effort de création. Ils sont *cessibles* : l'auteur peut les transférer gratuitement ou contre rétribution, avec ou sans exclusivité. Ces droits sont transmis aux héritiers de l'auteur pendant 70 ans après sa mort.

L'auteur jouit d'un droit d'exploitation qui comprend le droit de représentation et le droit de reproduction (article L122-1).

- La *représentation* consiste dans la communication de l'œuvre au public par un procédé quelconque (y compris donc en insérant cette œuvre sur une page web ou en la proposant en téléchargement).
- La *reproduction* consiste à créer des copies matérielles de l'œuvre, quel que soit le procédé. Elle peut s'effectuer notamment par imprimerie, dessin, gravure, photographie, moulage et par tout procédé d'enregistrement (sur disque dur, DVD, clé USB, iPod...).

Droit d'auteur et lien hypertexte

A-t-on le droit de faire pointer un lien hypertexte vers un contenu en ligne sans l'autorisation de l'auteur de ce contenu ? Le 13 février 2014, la Cour de justice de l'Union européenne a rappelé qu'un lien hypertexte constitue une communication au public, ce qui est censé être une prérogative de l'auteur. Mais si ce lien vise le même public que celui qui pouvait déjà accéder au contenu initial, l'autorisation de l'auteur n'est pas nécessaire pour insérer le lien. La solution serait différente si le lien mettait le contenu à la disposition d'un public nouveau, par exemple s'il permettait au grand public d'accéder à un contenu initialement réservé à des abonnés : dans ce cas l'autorisation de l'auteur serait indispensable.

Les droits voisins

Dans le cas des chansons ou des films, les acteurs, artistes, interprètes et producteurs, qui sont des auxiliaires de la création, bénéficient de droits similaires à ceux des auteurs, notamment en ce qui concerne les droits de reproduction et de représentation. Les interprètes jouissent également du droit moral sur leur prestation (droit au respect de son nom, par exemple).

Les exceptions

Le public dispose toutefois d'un certain nombre de possibilités d'utiliser une œuvre sans l'accord de l'auteur ou sans rétribution. Ainsi, l'auteur ne peut pas interdire un certain nombre d'utilisations de son œuvre une fois qu'elle a été divulguée (article L122-5).

Notamment, il ne peut pas interdire les représentations privées et gratuites effectuées exclusivement dans un *cercle de famille*.

Est autorisée la célèbre *copie privée*, c'est-à-dire les copies ou reproductions réalisées à partir d'une source licite, strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective. Notons bien que la source doit être licite : il ne s'agit pas d'une autorisation de télécharger puis de copier une œuvre sans régler les droits afférents, même pour son usage privé.

Sont également autorisées, sous réserve que soient indiqués clairement le nom de l'auteur et la source :

- les analyses et *courtes citations*, si elles sont justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information du support où elles sont publiées ;
- les *revues de presse* ;
- la diffusion, même intégrale, à titre d'information d'actualité, des *discours destinés au public* prononcés dans les assemblées politiques, administratives, judiciaires ou académiques, ainsi que dans les réunions publiques d'ordre politique et les cérémonies officielles ;
- dans le cadre de *l'exception d'enseignement*, la représentation ou la reproduction d'extraits d'œuvres, à des fins exclusives d'illustration dans le cadre de l'enseignement et de la recherche, à l'exclusion de toute activité ludique ou récréative, dès lors que le public auquel cette représentation ou cette reproduction est destinée est composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs directement concernés, que l'utilisation de cette représentation ou cette reproduction ne donne lieu à aucune exploitation commerciale et qu'elle est compensée par une rémunération forfaitaire (versée par le ministère de l'Éducation nationale aux sociétés d'auteurs). Un enseignant peut donc citer des extraits d'œuvres dans ses cours numériques tant que ceux-ci ne sont accessibles qu'à ses élèves, et non au grand public.

Par ailleurs, la *parodie*, le *pastiche* et la *caricature* sont autorisés dans les limites des lois du genre. La cour d'appel de Paris a rappelé le 18 février 2011 que cette exception « suppose à la fois une référence non équivoque à l'œuvre parodiée et une distanciation recherchée qui vise à travestir ou à subvertir l'œuvre dans une forme humoristique, avec le dessein de moquer, de tourner en dérision pour faire rire ou sourire ; que ne peuvent alors relever de l'exception de parodie les œuvres qui empruntent les ressorts d'œuvres premières pour s'attribuer le bénéfice de leur notoriété et vivre ainsi de leur rayonnement ». L'exception de parodie suppose donc à la fois une intention de faire rire et une distanciation suffisante par rapport à l'œuvre originale pour éviter toute confusion auprès du public.

Les copies transitoires

La reproduction d'une œuvre sur Internet nécessite évidemment des copies transitoires sur le réseau ou dans les mémoires vives des ordinateurs. Ces copies techniques provisoires sont autorisées si elles sont indispensables à l'utilisation licite de l'œuvre ou à sa transmission sur le réseau, tant qu'elles n'ont pas de valeur économique propre. Cette exception n'est toutefois pas valable pour les logiciels et les bases de données.

Licences, logiciels et données libres

Une licence libre est une modalité selon laquelle l'auteur d'une œuvre de l'esprit concède aux utilisateurs tout ou partie de ses droits d'auteur, notamment les droits de modification, de diffusion et de réutilisation. Cette cession peut être soumise à des conditions, comme la mention obligatoire du nom de l'auteur, l'interdiction d'un usage commercial, ou l'application du même type de licence aux œuvres dérivées.

Par confusion sur le terme anglais *free*, on assimile souvent licence libre et licence gratuite. Ce n'est pourtant pas systé-

matique, une œuvre sous licence libre permettant la modification peut très bien ne pas être gratuite.

Il existe plusieurs types de licences libres. Citons notamment les *Creative Commons*, plutôt pour les œuvres littéraires et multimédias, et les licences GNU (GPL) pour les logiciels.

Pour les données publiques, détenues par les administrations, se développe depuis plusieurs années un mouvement d'*open data* qui consiste à proposer ces données en libre accès, pour une libre réutilisation sans restriction technique, juridique ni financière. L'objectif est de favoriser l'innovation et la création à partir de ces données pour créer de nouveaux services ou améliorer les services existants.

Zoom Les données généalogiques

Parmi les données publiques, les données généalogiques font l'objet de nombreuses convoitises. En effet, des sociétés spécialisées collectent les données de l'état civil pour les revendre aux passionnés de généalogie. Se pose alors la question de la légitimité de l'accès aux données publiques : est-il normal qu'une collectivité investisse dans la numérisation de ses données, pour qu'ensuite des sociétés privées les récupèrent gratuitement puis les revendent ? Les collectivités locales sont donc réticentes à les communiquer. Le 26 février 2015, la cour d'appel de Bordeaux a validé le refus du département de la Vienne de céder ses archives numérisées à la société *Notrefamille.com* (gestionnaire du site *genealogie.com*), en se fondant sur la protection des bases de données prévue à l'article L112-3 du Code de la propriété intellectuelle. Le 4 juillet 2012, la cour administrative d'appel de Lyon avait approuvé le refus du département du Cantal de fournir ses données à *Notrefamille.com*, car il s'agit de données personnelles et les exigences de la loi Informatique et Libertés (notamment la sécurité des données et l'interdiction de leur transfert à l'étranger) n'étaient pas respectées par cette société. En revanche, la cour administrative d'appel de Nancy a, le 18 avril 2013, fait injonction au département de la Moselle de proposer à *Notrefamille.com* un accès à ses archives non numérisées, éventuellement aux frais du demandeur.

Pour les logiciels, l'*open source* autorise à redistribuer le logiciel ou à en créer des produits dérivés, et surtout donne accès

au code source pour l'analyser et le modifier (à la différence des logiciels propriétaires). Cet accès au code source est un garant de sécurité (on peut vérifier qu'il n'y a pas d'erreur, de faille ou de trappe dans le logiciel) et de qualité.

Jurisprudences pour violation des droits d'auteur

Condamnation pour concurrence déloyale *via* une revue de presse

Concernant les revues de presse, la cour d'appel de Paris a condamné le 9 novembre 2012 à 50 000 euros de dommages-intérêts et 6 000 euros de frais la société The Web Family de Jean-Marc Morandini, pour concurrence déloyale au détriment du site web de l'hebdomadaire *Le Point*, dont elle reprenait textuellement les brèves sur son propre site. The Web Family s'appropriait ainsi sans investissement de sa part les revenus publicitaires liés aux lecteurs de ces brèves, revenus qui auraient dû revenir au *Point*. Le fait que The Web Family citait sa source ne l'autorisait pas pour autant à reproduire systématiquement le travail d'autrui.

Notons enfin que la cour n'a pas reconnu au *Point* dans ce dossier la propriété des droits d'auteur sur les brèves, celles-ci, longues de quelques lignes seulement, ne témoignant pas « d'un véritable effort créatif », ce qui entraînait que ces textes ne pouvaient être protégés par le droit d'auteur. Cet arrêt rappelle que si la loi autorise les revues de presse, celles-ci ne doivent pas pour autant devenir le support d'une véritable concurrence aux auteurs des articles originaux.

Condamnation pour contrefaçon de dessins de Tintin

Le 11 juin 2004, le tribunal de grande instance de Paris, jugeant en référé, a estimé qu'un site publiant à la fois des parodies des aventures de Tintin et des reprises des personnages de la bande dessinée, sans travestissement quelconque, sur des produits tels que cartes de vœux ou billets de banque imaginaires, était en raison de ces dernières susceptible de

constituer une contrefaçon et donc un trouble manifestement illicite. Les parodies publiées sur le site, en revanche, étaient bien autorisées par l'exception de parodie. Le site ayant déjà été fermé par son éditeur, le juge a condamné ce dernier à verser aux ayants-droits d'Hergé une provision de 1 500 euros sur les dommages-intérêts à déterminer lors du jugement sur le fond et 2 000 euros de remboursement des frais de justice.

Lourde condamnation pour reproduction non autorisée de photos et de catalogues

Le 26 juin 2013, la cour d'appel de Paris a condamné la société d'information sur le marché de l'art Artprice à verser près d'un million d'euros de dommages et intérêts à une société de vente aux enchères dont elle avait reproduit sans autorisation sur son site les catalogues (contrefaçon), ainsi qu'à un photographe dont elle avait mis en ligne les clichés (contrefaçon) sans indiquer le nom de l'auteur (atteinte à son droit à la paternité sur ses œuvres et à son droit à leur intégrité). Le montant élevé des dommages s'explique par le bénéfice économique retiré par Artprice, qui vend ses bases de données à ses abonnés.

Autorisation des sites de fans

Un fan d'une série peut-il créer une page Facebook dédiée à l'objet de sa passion, dans laquelle il utilise la marque, le logo, le nom et des images de la série ? Oui, a jugé le tribunal de grande instance de Paris le 28 novembre 2013, tant que le fan n'induit pas les internautes en erreur (indication du titulaire des droits) et qu'il ne retire de cette page Facebook aucun avantage économique, notamment en n'exerçant aucune activité commerciale susceptible de concurrencer les ayants-droit.

Les DRM, les téléchargements illégaux et Hadopi

Le numérique permet à chacun de reproduire à l'infini des œuvres (livres, musiques, images, audiovisuel, jeux vidéo...), sans perte de qualité, et sans contrôle ni rétribution de l'auteur. Pour assurer le respect des droits patrimoniaux de l'auteur, plusieurs mesures ont été adoptées sous la pression des sociétés de gestion de droits et des gestionnaires de portefeuilles d'œuvres. Bien entendu, le Code de la propriété intellectuelle s'applique aux œuvres audiovisuelles.

Jurisprudences concernant le téléchargement illicite

Lourde condamnation pour mise à disposition de musiques sans autorisation

La Cour de cassation a validé le 25 septembre 2012 la condamnation des responsables de Radioblogclub. Ce site mettait à disposition des internautes de la musique gratuite en *streaming*, sans payer les droits d'auteur correspondants. Les responsables ont été condamnés à neuf mois de prison avec sursis et à 10 000 euros d'amende. Ils devront verser 1 089 755 euros de dommages-intérêts aux sociétés d'auteurs, somme correspondant aux gains qu'ils avaient engrangés grâce à la publicité sur leur site. Le tribunal a également ordonné la fermeture définitive de leur société.

Lourdes condamnations pour mise à disposition de vidéos sans autorisation

Le tribunal correctionnel de Paris a condamné le 26 septembre 2012 cinq personnes qui proposaient en téléchargement illégal des films sans autorisation, à des peines de trois à six mois de prison avec sursis, et à des dommages-intérêts d'un montant cumulé de plus de 1,1 million d'euros.

De même, le tribunal correctionnel de Thionville a condamné le 12 novembre 2013 à dix mois de prison avec sursis et plus de 1,1 million d'euros de dommages-intérêts l'administrateur d'un site de téléchargement illégal.

Plus modestement, la cour d'appel de Bordeaux a condamné le 8 mars 2013 à 9 300 euros de dommages-intérêts une personne qui avait créé un annuaire de référencement des sites de téléchargement illégal.

L'interdiction de sites de streaming illicite

Le 28 novembre 2013, le tribunal de grande instance de Paris a ordonné aux fournisseurs d'accès Internet d'empêcher les internautes d'accéder au site Allostreaming qui proposait des films ou des séries illicites. Le tribunal a également ordonné aux moteurs de recherche de déréférencer Allostreaming.

De même, le 4 décembre 2014, le même tribunal a ordonné aux fournisseurs d'accès d'empêcher l'accès au site The Pirate Bay, qui propose de la musique sans payer les droits d'auteur.

L'encadrement de la copie privée

On a vu qu'était autorisée la copie privée d'une œuvre, à partir d'une source licite, pour l'usage privé du copiste. Avant la généralisation du numérique, cette copie privée pouvait prendre la forme d'une photocopie d'un livre, d'une cassette magnétique de sauvegarde d'un disque vinyle, ou d'une compilation personnelle sur cassette de morceaux de musique figurant sur plusieurs cassettes du commerce.

En numérique, il est par exemple licite de copier sur son iPod les morceaux qu'on a achetés ou téléchargés légalement.

Pour compenser le manque à gagner subi par les auteurs du fait de cette copie privée, une redevance forfaitaire de copie privée a été instituée sur tous les supports mémoire : CD, DVD, disques durs, baladeurs, clés USB, smartphones, box

Internet... Le barème de cette redevance est fixé pour chaque type de support par une commission.

La redevance de copie privée vise tous les supports, qu'ils servent effectivement à de la copie privée ou pas. Les entreprises y sont ainsi assujetties pour leurs disques durs, alors qu'*a priori* aucune copie privée d'œuvre n'est censée se trouver dans des disques durs d'entreprise ! Toutefois, dans un arrêt du 21 octobre 2010, la Cour de justice de l'Union européenne a précisé que la redevance de copie privée ne devait pas s'appliquer aux équipements et supports d'enregistrement « non mis à la disposition d'utilisateurs privés et manifestement réservés à des usages autres que la réalisation de copies à usage privé ». En particulier, les entreprises doivent donc pouvoir se faire rembourser la redevance sur les équipements qu'elles achètent. Le formulaire de remboursement n'est disponible que depuis avril 2014, et les démarches à accomplir sont fastidieuses.

Refus de payer la redevance

Estimant qu'en faisant payer la redevance indistinctement par les particuliers et par les professionnels, la France ne respecte pas le droit européen, la société néerlandaise Imation refuse depuis 2011 de verser la redevance de copie privée sur les supports de stockage qu'elle vend. La société de collecte Copie France l'ayant fait assigner en référé, le tribunal de grande instance de Paris, confirmé par la cour d'appel de Paris le 19 novembre 2013, a estimé que les contestations adressées au dispositif français étaient sérieuses et ne pouvaient être tranchées en référé (c'est-à-dire en urgence) ; le dossier est donc renvoyé aux juges du fond.

Apple refuse également de verser à Copie France la redevance de copie privée qu'elle collecte sur ses iPad. En juin 2014, le tribunal de grande instance de Paris l'a condamnée à verser 18 millions d'euros sur un compte sous séquestre, dans l'attente d'une validation par le Conseil d'État des barèmes de la redevance, validation finalement prononcée le 19 novembre 2014.

DÉBAT Les barèmes

Les tarifs de la redevance pour copie privée sont plus élevés en France que dans les autres pays européens. Du coup, un même support mémoire, un disque dur par exemple, peut être vendu moins cher à l'étranger qu'en France. Les clients ont alors tendance à commander leurs supports mémoire chez des distributeurs situés hors du territoire national. Les distributeurs français se plaignent d'être ainsi défavorisés par des tarifs excessifs et de subir une distorsion de concurrence. En effet, la perception de la redevance par la douane lors du passage de la frontière, qui devrait rétablir l'égalité, n'est en pratique pas mise en œuvre.

Dans son arrêt du 10 avril 2014, la Cour de justice de l'Union européenne a précisé que, dans le calcul de la compensation à verser aux ayants-droit, seuls les usages licites doivent être pris en compte ; la redevance pour copie privée n'a pas pour but de compenser la copie illicite.

Les DRM

On appelle DRM (*Digital Rights Management* – Gestion des droits numériques) des mesures techniques destinées à empêcher ou à limiter les utilisations non autorisées d'une œuvre, comme les copies abusives. On trouve ces dispositifs sur les CD, DVD, jeux vidéo... (article L331-5 du CPI).

Les DRM ne doivent pas empêcher l'utilisation normale de l'œuvre ni l'interopérabilité, c'est-à-dire sa lecture sur tous les types d'appareils.

DÉBAT Les clés du Blu-Ray

En 2012, les développeurs du lecteur multimédia français en logiciel libre VLC ont saisi l'Hadopi afin d'obtenir de Sony, au nom du droit à l'interopérabilité, les clés de chiffrement permettant de lire les disques Blu-Ray dont l'industriel est l'inventeur. Faute de ces clés, le lecteur VLC ne peut pas lire les Blu-Ray.

Si dans le principe, les DRM ne sont pas censées s'opposer au droit à la copie privée, le CPI précise que les limitations sus-

ceptibles d'être apportées à ce droit par les DRM doivent être portées à la connaissance de l'utilisateur. C'est ainsi que les CD, DVD et jeux vidéo portent souvent sur leur jaquette la mention d'un dispositif anticopie.

Toutefois, la Cour de cassation a précisé le 19 juin 2008 dans son arrêt « Mulholland Drive » que « la copie privée ne constitue pas un droit mais une exception » et qu'on ne pouvait exiger son application.

Débat Les contradictions du dispositif

On aboutit ainsi à une interdiction *de facto* de la copie privée du fait des DRM, tandis que dans le même temps, non seulement la redevance pour copie privée sur les supports mémoire est maintenue, mais son champ est étendu à de nouveaux supports et son barème augmente ! L'utilisateur paye ainsi de plus en plus cher une copie privée qu'on l'empêche d'exercer.

Les mesures pénales

Le Code de la propriété intellectuelle punit sévèrement les atteintes aux œuvres protégées. Ainsi, l'article L335-2-1 punit de trois ans d'emprisonnement et de 300 000 euros d'amende le fait d'éditer, de mettre à la disposition du public ou de communiquer au public, un logiciel manifestement destiné à la mise à disposition non autorisée d'œuvres ou d'objets protégés, ou de faire la publicité d'un tel logiciel. La même peine sanctionne la reproduction d'une œuvre ou sa mise à disposition du public sans autorisation. Le défaut de versement de la rémunération de l'auteur ou de la redevance de copie privée est puni de 300 000 euros d'amende (article L335-4).

Par ailleurs, l'article L335-3-1 punit de 3 750 euros d'amende le fait de contourner ou de supprimer un DRM sans usage d'un dispositif technologique spécialement adapté à cette fin. L'utilisation d'un dispositif spécifique, sa simple détention, sa mise à

disposition d'autrui ou la publicité en sa faveur, sont punis de six mois d'emprisonnement et de 30 000 euros d'amende.

Ces dispositions ne sont pas applicables si les faits ont eu lieu dans le cadre de la recherche ou de la sécurité informatique.

Jurisprudences

Comme nous l'avons vu, la Cour de cassation a validé le 25 septembre 2012 la condamnation des responsables du site Radioblogclub. Ce site mettait à disposition des internautes de la musique gratuite en streaming, *via* un logiciel permettant de créer une liste de lecture. Les responsables ont été condamnés à neuf mois de prison avec sursis et à 10 000 euros d'amende.

Un étudiant qui avait pénétré frauduleusement dans le système informatisé de Deezer pour s'emparer des données de codage, puis qui les avait utilisées pour concevoir et mettre en ligne un logiciel permettant le contournement des DRM, a été condamné le 28 juin 2014 par le tribunal de grande instance de Nîmes à 15 000 euros d'amende avec sursis et plus de 30 000 euros de dommages-intérêts et de frais de justice.

Le 19 février 2015, le tribunal de grande instance de La Rochelle a condamné à six mois de prison avec sursis et environ 2 millions d'euros de dommages-intérêts le créateur d'un site de téléchargements, notamment illégaux, qui avait permis près de trois millions de téléchargements de vidéos et de musiques.

Le téléchargement illégal et Hadopi

Pour lutter contre le téléchargement d'œuvres sans s'acquitter des droits d'auteur correspondants (ce qui constitue une contrefaçon au sens du CPI), le gouvernement français a instauré en 2009 une obligation pour l'abonné à Internet de veiller à ce qu'aucune contrefaçon d'œuvre ne soit effectuée à partir de son accès Internet. Une autorité administrative indépendante, la Hadopi (Haute autorité pour la diffusion des

œuvres et la protection des droits sur Internet), a été créée pour sanctionner les infractions à cette obligation.

Droit Les autorités administratives indépendantes

L'évolution de la législation à la fin des années 1970 a vu l'apparition d'une innovation juridique avec la création des autorités administratives indépendantes (AAI). Ces autorités ont chacune la mission de réguler un secteur bien défini. Leur indépendance doit leur apporter à la fois une autorité face aux différents acteurs, puisqu'il n'est pas possible de tenter de faire pression sur elles au travers d'une administration, et également la capacité de s'opposer éventuellement à l'État. Cette prérogative constitue donc un enjeu essentiel de leur statut. La Commission nationale de l'Informatique et des Libertés (Cnil), créée par la loi Informatique et Libertés de 1978 comme l'organe régulateur pour la protection des données personnelles, est historiquement la première des autorités administratives indépendantes. Dans ce cas particulier, le choix de l'indépendance du régulateur provenait également d'une méfiance à l'égard de l'État.

La Hadopi a pour missions de promouvoir l'offre légale d'œuvres sur Internet, de lutter contre le téléchargement illégal ou la mise à disposition illégale et de réguler les DRM.

Droit Le peer-to-peer (P2P) et le streaming

La loi de 2009 ne vise que la contrefaçon par *peer-to-peer* (P2P), c'est-à-dire *via* des logiciels spéciaux permettant la mise à disposition, le téléchargement et le partage de fichiers. Notons que le *peer-to-peer* peut être parfaitement légal s'il vise à partager des fichiers dont l'internaute détient les droits. En revanche, son utilisation pour partager des fichiers sans payer les droits correspondants est réprimée. Ce n'est donc pas la technologie du P2P en tant que telle qui est visée, mais l'usage qui en est fait.

La loi ne vise pas les autres technologies, comme le streaming, utilisé par YouTube ou Dailymotion pour visionner des films sans les télécharger. La Hadopi ne peut donc pas sanctionner le visionnage illégitime d'œuvres par streaming.

Toutefois, dans son arrêt du 7 mars 2013, la Cour de justice de l'Union européenne a précisé que, s'agissant d'un programme de télévision, la retransmission en streaming nécessite « l'autorisation des auteurs des œuvres retransmises lorsque celles-ci sont communiquées au public ».

Lorsque la Hadopi est informée par les ayants-droit (sociétés de collecte des droits d'auteurs ou détenteurs de catalogues d'œuvres) de possibles infractions correspondant à certaines adresses IP, elle entame un mécanisme de réponse graduée.

TECHNIQUE L'adresse IP

L'adresse IP (*Internet Protocol*) est le numéro, unique au monde, sous lequel un ordinateur est relié à Internet. Ce numéro permet de le reconnaître sur la Toile et de s'y connecter. L'adresse IP contient une indication de la zone géographique de l'ordinateur : la première partie de cette adresse désigne le réseau, la seconde repère le client sur ce réseau.

Ce mécanisme de réponse graduée est le suivant.

- Lors du premier acte de téléchargement ou de mise à disposition signalé, la Hadopi envoie un courriel au titulaire de l'abonnement pour lui rappeler son obligation de veiller à ce que son accès ne serve pas à la contrefaçon.
- Si, dans les six mois qui suivent, un nouveau téléchargement est signalé, la Hadopi peut envoyer un second courriel, accompagné d'une lettre recommandée.
- Si, dans l'année qui suit, un nouveau téléchargement est signalé, la Hadopi avertit l'abonné par lettre recommandée que ces faits sont susceptibles de poursuites pénales.
- La Hadopi peut alors transmettre le dossier au procureur pour jugement au tribunal. L'abonné encourt une amende de 1 500 euros.
- Une peine complémentaire de suspension de l'accès à Internet, d'une durée maximale d'un mois, avait été instaurée en 2010. Très critiquée, puisqu'elle privait l'abonné de son droit d'accès aux informations et aux services, et qu'elle pénalisait également les autres membres de son foyer, elle a été supprimée en 2013.

Cette peine de suspension d'accès n'avait été prononcée qu'une seule fois, en mai 2013, envers un internaute condamné par un tribunal de Seine-Saint-Denis à 600 euros d'amende et à 15 jours de suspension. Toutefois, cette suspension de 15 jours n'a finalement pas été mise en œuvre, le décret supprimant cette peine ayant été publié entre-temps. Finalement, aucun internaute n'a donc subi de coupure d'Internet.

Lors de chacune des étapes de la réponse graduée, l'abonné peut envoyer à la Hadopi ses observations par courriel ou par courrier (un formulaire est disponible sur le site web de la Hadopi).

BIAN Hadopi 2010-2014

De 2010 à juin 2014, la Hadopi a envoyé plus de 3 millions de courriels de première recommandation et 300 000 de seconde recommandation. Plus de 100 dossiers ont été transmis au parquet et 17 ont donné lieu à des décisions de justice, dont des amendes allant jusqu'à 600 euros et 15 jours de suspension d'Internet, cette dernière mesure n'ayant pas été mise en œuvre.

D'après les exemples donnés par la Hadopi, si l'abonné, après avoir reçu un courriel d'avertissement, s'engage à ne plus opérer de téléchargement illégitime et s'il tient son engagement, la Hadopi ne transfère pas le dossier au tribunal. En revanche, si l'abonné persiste à utiliser du P2P, en téléchargement ou en mise à disposition, pour des œuvres dont il ne détient pas les droits, la Hadopi transfère le dossier au tribunal. La Hadopi note cependant que de nombreux internautes, après avoir téléchargé une fois une œuvre par P2P, ne sont pas conscients du fait que le logiciel continue à mettre cette œuvre en partage depuis leur ordinateur, même si eux-mêmes ne téléchargent plus activement. La méconnaissance du fonctionnement du logiciel conduit ainsi à une persistance involontaire de l'infraction.

Condamnation pour téléchargement illégal

L'intervention de la Hadopi n'est pas indispensable pour réprimer le téléchargement illégal. Comme nous l'avons vu plus haut, le Code de la propriété intellectuelle interdit la contrefaçon. Un internaute a ainsi été directement condamné en janvier 2013 par le tribunal correctionnel d'Amiens à 450 euros d'amende et 2 200 euros de dommages-intérêts pour contrefaçon après avoir

téléchargé 18 films en peer-to-peer. Il n'avait reçu aucun avertissement de la Hadopi, mais avait été directement repéré par les fédérations d'ayants-droit qui avaient déposé plainte.

Les logiciels, sites web et bases de données

Le Code de la propriété intellectuelle a prévu le cas des logiciels, sites web et bases de données, qui sont des œuvres numériques. On a vu plus haut que les logiciels étaient compris dans la liste des œuvres de l'esprit figurant à l'article L112-2. L'article L112-3 ajoute qu'il « en est de même des [...] bases de données, qui, par le choix ou la disposition des matières, constituent des créations intellectuelles. On entend par base de données un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen ».

DÉTAIL Le cas des auteurs salariés

Lorsqu'un salarié d'une société (ou d'un organisme public) crée un logiciel ou un site web dans le cadre de sa mission, les droits d'auteur reviennent-ils au salarié ou à sa société ? Les droits moraux reviennent au salarié, mais pour les droits patrimoniaux, l'article L113-9 du CPI prévoit que « sauf dispositions statutaires ou stipulations contraires, les droits patrimoniaux sur les logiciels et leur documentation créés par un ou plusieurs employés dans l'exercice de leurs fonctions ou d'après les instructions de leur employeur sont dévolus à l'employeur qui est seul habilité à les exercer ».

Le CPI ne précise pas explicitement que pour bénéficier de la protection du droit d'auteur, le logiciel doit présenter un caractère d'originalité, mais cette condition a été ajoutée par la jurisprudence. La Cour de cassation a ainsi indiqué dans son arrêt

Pachot du 7 mars 1986 que pour revendiquer le droit d'auteur, le créateur du logiciel doit avoir « fait preuve d'un effort personnalisé allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante et que la matérialisation de cet effort résidait dans une structure individualisée » qui porte « la marque de son apport intellectuel ».

La Cour a confirmé sa position le 17 octobre 2012 en expliquant que pour démontrer cette originalité, il fallait montrer « en quoi les choix opérés témoignaient d'un apport intellectuel propre et d'un effort personnalisé de celui qui avait élaboré le logiciel litigieux, seuls de nature à lui conférer le caractère d'une œuvre originale protégée, comme telle, par le droit d'auteur ». Et le 14 novembre 2013, la Cour précisait les « éléments de nature à justifier de l'originalité des composantes du logiciel » : ce sont les « lignes de programmation, les codes ou l'organigramme, ou du matériel de conception préparatoire ».

La condition d'originalité entre ainsi dans le droit prétorien.

DÉFINITION Le droit prétorien

Comme on l'a déjà vu, le droit prétorien rassemble des dispositions qui ne figurent pas dans la loi, mais qui résultent des jurisprudences retenues par les tribunaux, lesquelles finissent par « prendre force de loi », en l'absence justement d'une loi sur le sujet. Parmi les créations prétoriennes les plus connues, citons le devoir d'information et de conseil de la banque, ou de l'agent immobilier.

Un droit prétorien développé et confirmé par la Cour de cassation, comme c'est le cas ici, a plus de valeur que celui créé par les simples tribunaux de première instance, car il s'impose à tous.

Concernant les bases de données, le CPI (article L341-1) exige également que leur constitution ait demandé un « investissement substantiel ». Le 19 juin 2013, la Cour de cassation a ainsi refusé la protection du CPI à une base de données réalisée en assemblant des annuaires préexistants. En

revanche, le 6 décembre 2013, le tribunal de grande instance de Paris a accordé 5 000 euros de dommages-intérêts à un site de vente de jantes automobiles dont un concurrent avait reproduit la base de données de modèles. Le plaignant avait démontré avoir consacré 500 heures à constituer cette base et avoir dépensé 30 000 euros de frais de prestataire informatique, ce qui constituait bien un investissement substantiel pour une société dont le capital s'élevait à 7 500 euros.

Outre la protection offerte par le CPI, un logiciel peut également être protégé par le droit commun. La cour d'appel d'Aix a ainsi condamné le 10 octobre 2013 un développeur qui avait réutilisé les codes sources de son ancien employeur pour lancer des applications concurrentes. Qualifiant ses agissements de « parasitisme, s'agissant d'une appropriation sans autorisation du travail ou du savoir-faire d'autrui et de ses investissements », la cour a condamné le développeur à rendre à son ancien employeur les revenus indûment perçus.

Lorsque plusieurs personnes ont concouru à la création de l'œuvre, il sera nécessaire de préciser l'apport de chacun en cas de litige sur la répartition des droits.

La paternité d'un logiciel

La cour d'appel de Paris a débouté le 27 février 2013 une personne qui revendiquait la qualité de co-auteur sur un logiciel développé par une société qu'elle avait créée avec des associés, mais qu'elle avait quittée. La cour a noté que c'est un de ses collègues qui, depuis l'origine, était désigné publiquement comme l'auteur du logiciel et qui était cité comme tel dans tous les documents. Ce collègue bénéficiait dès lors d'une présomption de qualité d'auteur que seules des preuves indiscutables auraient permis de renverser. Or, le plaignant ne disposait pas de telles preuves permettant d'évaluer l'importance de sa participation à l'élaboration du logiciel.

Il est donc indispensable, si l'on souhaite pouvoir revendiquer des droits sur l'élaboration d'un logiciel ou d'un site web, de constituer des preuves de sa participation, au besoin par voie d'huissier.

Le droit d'exploitation d'un logiciel, qui fait partie des droits patrimoniaux, comprend le droit d'effectuer et d'autoriser (article L122-6) :

- la reproduction permanente ou provisoire d'un logiciel en tout ou partie, par tout moyen et sous toute forme ;
- la traduction ou toute adaptation du logiciel ;
- la vente, la distribution gratuite ou la location de ce logiciel.

Toutefois, l'autorisation de l'auteur n'est pas nécessaire pour permettre l'utilisation du logiciel ou la correction de ses erreurs par une personne ayant le droit de l'utiliser, sauf si le contrat d'utilisation le stipule différemment.

L'utilisateur a également le droit de faire une copie de sauvegarde (article L122-6-1).

La personne ayant le droit d'utiliser le logiciel peut également, sans autorisation de l'auteur, observer et tester le logiciel pour en déterminer les principes.

Précision La limite du droit d'observation

Le droit d'observation du logiciel (ou de « rétro-ingénierie ») ne signifie évidemment pas que l'utilisateur a le droit de rédiger un programme similaire : cela deviendrait de la contrefaçon !

L'utilisateur a également le droit d'accéder au code du logiciel sans autorisation de l'auteur si cela est indispensable pour assurer l'interopérabilité avec d'autres logiciels, aux conditions que les informations nécessaires à l'interopérabilité ne soient pas déjà disponibles, et que cet acte se limite aux parties du logiciel concernées par cette interopérabilité.

Enfin, le Code de la propriété intellectuelle rappelle (article L122-6-2) que l'utilisation illicite des moyens de supprimer ou de contourner les dispositifs techniques protégeant

un logiciel constitue une contrefaçon. La publicité ou la notice d'utilisation de ces moyens (en vue de leurs usages licites !) doit porter mention de ce rappel.

Revente de logiciels d'occasion

Le 3 juillet 2012, la Cour de justice de l'Union européenne a indiqué que l'auteur d'un logiciel ne pouvait empêcher, au nom de son droit de contrôle sur les reproductions, la revente d'occasion d'une licence d'utilisation de ce logiciel. Si l'auteur a déjà été rémunéré lors de la vente initiale pour une utilisation sans limitation de durée, il ne peut s'opposer à la revente de ce droit d'utilisation et ne peut prétendre à une nouvelle rémunération. La Cour a donc précisé qu'il était tout à fait légal de revendre une licence, que le logiciel soit sur un support physique ou téléchargé sur Internet. Dans ce dernier cas, l'auteur du logiciel ne peut s'opposer au nouveau téléchargement. Évidemment, l'utilisateur initial qui revend sa licence doit désinstaller le programme chez lui.

Vente liée de l'ordinateur et du système d'exploitation

De manière générale, il est interdit dans le commerce de procéder à une « vente liée », c'est-à-dire de conditionner la vente d'un produit à l'achat d'un autre produit (article L122-1 du Code de la consommation). Toutefois, ce principe connaît des exceptions pour motif légitime : par exemple, l'achat d'une voiture implique l'achat des freins qui sont montés dessus et personne n'aurait l'idée de revendiquer la possibilité d'acheter séparément la voiture et les freins.

Pour l'informatique, la question s'est longtemps posée de savoir s'il était légitime de vendre obligatoirement un ordinateur avec un système d'exploitation, par exemple Windows, obligeant ainsi le client à acheter ce système même s'il en aurait préféré un autre (Linux, par exemple). Plusieurs clients ont attaqué les constructeurs informatiques ou les distribu-

teurs pour se faire rembourser le système dont ils ne voulaient pas et pour les faire condamner pour vente liée ou pour pratique déloyale.

Faute de texte précis sur ce sujet, de nombreuses jurisprudences ont conduit à reconnaître que la vente d'un ordinateur « nu », sans système d'exploitation, nécessite des manipulations d'installation délicates qui conduisent à la réserver à des utilisateurs avertis, professionnels ou experts en informatique. Pour le grand public, la vente liée de l'ordinateur et du système est plus sécurisante et est donc admise. Toutefois, l'acheteur grand public doit avoir la possibilité d'acheter un PC « nu » ou de se faire rembourser le système vendu avec l'ordinateur.

En pratique, les procédures de remboursement et de désinstallation, quand elles sont proposées, sont souvent rédhitoires (nécessitant par exemple le renvoi de l'ordinateur au constructeur pour désinstallation). Plusieurs constructeurs ont été condamnés ces dernières années à rembourser les licences et à payer quelques centaines d'euros de dommages-intérêts aux acheteurs. D'autres procès sont en cours, intentés par des particuliers ou par des associations de consommateurs, pour faire préciser les droits du client.

Le 5 juin 2014, la cour d'appel de Paris, suite à un premier renvoi en cassation, a estimé que la vente d'ordinateurs prééquipés d'un système d'exploitation ne constitue pas une pratique commerciale déloyale, si l'acheteur a, sur la même boutique, la possibilité d'acquérir un ordinateur « nu ».

Les droits sur le développement d'un site web

Un site web est une œuvre de l'esprit et bénéficie donc des protections prévues par le CPI s'il présente les qualités d'originalité requises. *A contrario*, s'il se limite au remplissage de rubriques (par exemple un profil Facebook), le manque d'originalité interdit de lui accorder le statut d'œuvre.

Si le site contient des bases de données, celles-ci sont également protégées.

Si le site web est conçu et développé par la même personne, il n'y a pas de difficulté à en désigner l'auteur. Les choses sont plus compliquées lorsque plusieurs personnes ont collaboré à sa création.

Dans le cas où le site incorpore des images, textes ou éléments multimédias développés par d'autres personnes, l'autorisation de chacun des titulaires des droits sur ces éléments doit avoir été obtenue.

À REtenir Le cas des sous-traitants

Lorsque la création d'un site web est sous-traitée à un prestataire, si le commanditaire se borne à passer une commande d'ordre général, sans donner « des indications précises sur la présentation des différentes pages et l'agencement des éléments qui les composent, sur le graphisme, l'animation ou l'arborescence favorisant la consultation d'un site » et si c'est le prestataire qui prend l'initiative de cette création, alors le prestataire est considéré comme l'auteur du site web. Son client bénéficie évidemment d'un droit d'exploitation, mais le prestataire auteur conserve les droits moraux, et notamment le droit de voir son nom demeurer sur le site même dans le cas où le client change ultérieurement d'hébergeur.

Ainsi, le tribunal de grande instance de Paris a reconnu le 10 novembre 2011 les droits d'auteur d'un prestataire qui avait développé et hébergé un site pour un client. Ce dernier avait ensuite transféré le site chez un prestataire concurrent, qui l'avait conservé tout en substituant son nom à celui du créateur, ce qui constituait une contrefaçon. Le client a été condamné à verser 3 000 € au prestataire auteur du site, en réparation du préjudice subi et le nouveau prestataire a été condamné à lui verser 8 000 € pour concurrence déloyale.

Le nom de domaine

Pour accéder à un site web, celui-ci doit avoir un nom de domaine de la forme www.ledomaine.fr (ou www.ledomaine.com, ou toute autre extension).

TECHNIQUE L'adresse URL

En fait, l'adresse d'une page web consiste en une suite de chiffres de la forme 127.0.0.1, qui détermine exactement le serveur sur lequel se trouve cette page. Pour des raisons d'ergonomie, il est plus facile de se souvenir d'une adresse de la forme *monsite.com* que de la forme 318.25.69.33. Internet propose donc des noms de domaines, qui se superposent aux adresses de base. Les serveurs du réseau Internet savent traduire les noms de domaines en adresses exactes.

Chacun peut créer et acheter un nom de domaine pour son site web. Cette opération s'effectue auprès de prestataires appelés *registrars*, qui vendent les noms de domaine ainsi que différents services annexes (hébergement de sites, serveur de messagerie, adresses mail liées au nom de domaine...). L'achat d'un nom de domaine se fait généralement pour la durée d'une année, renouvelable. Le prix varie selon les extensions (.fr, .com, .org...) et selon les prestations annexes proposées par le *registrar*; cela est accessible à partir d'une quinzaine d'euros par an, donc à la portée de chacun.

Comme les noms de domaine ne peuvent exister qu'une seule fois au niveau mondial, leur attribution se fait selon la règle du premier arrivé, premier servi. Il y a toutefois quelques limitations : certains mots sont par exemple interdits car réservés techniquement par le système. D'autres noms ne peuvent être réservés que par certaines catégories de clients (noms de sociétés, par exemple).

Le Code des postes et des communications électroniques prévoit (article L45-2) que l'enregistrement d'un nom de domaine peut être refusé si celui-ci est contraire à l'ordre public ou aux bonnes mœurs, s'il porte atteinte à la propriété intellectuelle d'un tiers (s'il correspond par exemple à une marque enregistrée par ce tiers), ou s'il est similaire au nom de l'État, d'une collectivité territoriale, ou d'un organisme public. Le nom de domaine ne doit pas non plus porter

atteinte aux droits de la personnalité d'un tiers, par exemple reprendre le nom patronymique de ce tiers.

Ces dernières dispositions visent à mettre un terme à la pratique du *cybersquatting*, c'est-à-dire au fait de réserver un site correspondant au nom d'un tiers, soit pour gêner ce dernier (s'il s'agit d'un adversaire politique ou d'un concurrent commercial), soit dans l'objectif lucratif de lui revendre le domaine à un prix élevé.

Jurisprudences sur les noms de domaine

Condamnation pour enregistrement d'un domaine au nom d'un concurrent

En mars 2008, le candidat à la mairie de Cancale a été condamné par le tribunal de grande instance de Saint-Malo pour avoir déposé un nom de domaine correspondant au nom de son adversaire aux élections. Ce candidat a été condamné à verser 5 000 euros de dommages-intérêts à son adversaire et à lui rembourser 2 000 euros de frais de justice.

Contrairement au nom, le prénom n'ouvre aucun droit

En 2001, le fils de Milka Budimir offrait à sa mère, qui exploitait un établissement de couturière en province, à l'enseigne Milka Couture, le nom de domaine *milka.fr*.

En 2002, la société Kraft Foods, propriétaire de la marque de chocolat Milka, a demandé à M^{me} Budimir d'arrêter l'exploitation de ce nom de domaine et de le lui transférer. Faute d'accord amiable, Kraft Foods a porté l'affaire en justice.

Le 27 avril 2006, la cour d'appel de Versailles a précisé « qu'à la différence du nom patronymique, le prénom ne confère aucun droit privatif à son titulaire sauf [...] à démontrer qu'elle a acquis une certaine célébrité sous ce prénom ». Même s'il n'existait aucune confusion possible dans l'esprit du public entre les chocolats de Kraft Foods et les services purement locaux de la « petite couturière de la Drôme », le simple

fait d'utiliser le nom de domaine *milka.fr* constituait une exploitation injustifiée de la marque déposée Milka. La cour a donc confirmé le jugement de première instance, qui décidait « que le transfert sans frais à la société Kraft Foods du nom de domaine *milka.fr* constituait une exacte réparation du préjudice par elle subi en raison de cette exploitation ». Le nom de domaine est donc revenu au groupe agro-alimentaire.

Condamnation pour cybersquatting

Deux jours après la publication d'un communiqué de presse du groupe NRJ, propriétaire de la radio Chérie FM, annonçant le lancement de la chaîne Chérie HD (haute définition), un particulier a acheté les noms de domaine *cheriehd.net*, *cherie-hd.com*, *cherie-hd.net*, *cheriehd.fr* et *cherie-hd.fr*. Il a aiguillé ces noms de domaine vers un site web comportant des liens publicitaires vers des produits et services similaires à ceux de Chérie FM et a mis en vente ces noms de domaine sur un site d'enchères.

Le 28 juin 2012, le tribunal de grande instance de Nanterre a estimé que ces faits caractérisaient la contrefaçon de la marque Chérie FM et a condamné le contrefacteur à verser 6 000 euros de dommages-intérêts à Chérie FM, ainsi que 3 000 euros de frais de justice.

Un nom de domaine trop peu original n'est pas protégé

Deux jurisprudences ont rappelé en 2013 que pour être protégé par le droit de la propriété intellectuelle et de la concurrence, un nom de domaine doit revêtir un caractère distinctif et original. Il ne doit pas se borner à décrire l'activité de son titulaire. Ainsi, la cour d'appel de Bastia a débouté le 20 mars 2013 les propriétaires du domaine *mariagesencorse.com*, organisateurs de mariages, qui se plaignaient de la concurrence déloyale du site concurrent *mariageencorse.com*. La cour a jugé que le nom *mariagesencorse* était trop générique et trop descriptif pour pouvoir revendiquer une protection.

De même, le tribunal de commerce de Paris a débouté le 24 mai 2013 la société de pompes funèbres titulaire du nom de domaine ~~e~~obseques.fr, qui se plaignait de la concurrence des services funéraires de la Ville de Paris avec le domaine iobseques.fr. Le tribunal a noté qu'en choisissant un nom de domaine descriptif, la société avait cherché à faire des économies et avait « évité les investissements indispensables pour donner une notoriété propre à une adresse Internet » ; protéger un nom aussi peu original reviendrait à créer un monopole sur un terme descriptif.



Les transactions en ligne

Qu'il s'agisse d'acheter, de vendre ou de consulter son compte bancaire en ligne, chacun utilise Internet pour ses transactions financières. Quelles sont les protections prévues pour le consommateur ?

Le commerce en ligne connaît depuis plusieurs années une progression annuelle de 10 à 20 % et a atteint le chiffre d'affaires de 57 milliards d'euros en 2014. Si l'on dénombre en France plus de 150 000 sites marchands, les plus grandes enseignes (notamment américaines) dominent largement le secteur. 32 millions de Français ont acheté en ligne en 2012 et le taux de satisfaction après achat a atteint fin 2014 le chiffre de 99 %, ce qui confirme que les e-acheteurs sont des clients satisfaits.

Rappel Des débuts peu attirants

Le début du commerce en ligne en France a été marqué par l'arnaque du site *pere-noel.fr*, lequel ne livrait pas les objets qui lui avaient été commandés (et payés) ni ne réglait ses fournisseurs. 1 270 plaintes avaient été déposées en 2001 et en 2002, et en 2003 l'ex-PDG du site était condamné pour tromperie à 30 mois de prison ferme. En 2010, il était en outre condamné à rembourser 4,5 millions d'euros de passif. Cependant, ces condamnations n'ont pu être exécutées, l'ex-PDG étant en fuite depuis 2003.

L'acheteur en ligne bénéficie des protections générales du consommateur, ainsi que d'un certain nombre de dispositions propres à Internet.

L'achat en ligne

La loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) définit le commerce électronique comme « l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services ». Cette activité comprend également « les services tels que ceux consistant à fournir des informations en ligne, des communications commerciales et des outils de recherche, d'accès et de récupération de données, d'accès à un réseau de communication ou d'hébergement d'informations, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent. »

L'article 14 de la LCEN prévoit qu'un cybercommerçant est regardé comme établi en France, pour l'application de ladite loi, lorsqu'il y est installé « d'une manière stable et durable pour exercer effectivement son activité », même si son siège social est implanté dans un autre pays.

Tout prestataire de commerce électronique est responsable à l'égard de l'acheteur de la bonne exécution des obligations résultant du contrat de prestation. Cela est valable, que ces obligations soient à exécuter par lui-même ou par d'autres prestataires de services auxquels il a fait appel. Toutefois, dans ce dernier cas de figure, il peut à son tour exercer un recours contre ces sous-traitants.

Le prestataire ne peut s'exonérer de sa responsabilité que s'il apporte « la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable, soit à l'acheteur, soit au fait, imprévisible et insurmontable, d'un tiers étranger à la fourniture des prestations prévues au contrat, soit à un cas de force majeure » (article 15 de la LCEN).

Pas plus que le commerce traditionnel, le commerce en ligne ne peut porter sur des objets contrefaits. La Cour de justice de l'Union européenne a précisé le 6 février 2014 que cette interdiction était valable dès que l'objet contrefait entrait dans l'Union, même si l'achat avait été effectué sur un site étranger ne s'adressant pas aux consommateurs européens.

NOUVEAU Les pharmacies en ligne

Depuis 2013, la vente de médicaments en ligne est autorisée en France, mais uniquement si le site web est géré par une officine de pharmacie traditionnelle et a reçu un agrément de l'agence régionale de santé, et uniquement pour des médicaments vendus sans ordonnance. Mais les sites pirates pullulent. Plusieurs sites illégaux ont été fermés par les autorités françaises en août 2013. En mai 2014, Interpol a procédé à la fermeture de 10 000 sites illégaux dans 110 pays et a saisi pour 20 millions d'euros de médicaments contrefaits qui étaient écoulés en ligne. Or un médicament contrefait est rarement efficace : au mieux il est inoffensif, mais ne soigne pas ; au pire il est nocif. Pour éviter les arnaques ou l'achat d'un médicament contrefait ou interdit, donc dangereux, il convient de bien vérifier que le site de pharmacie en ligne est agréé et, bien sûr, d'éviter d'acheter des médicaments vendus à des prix excessivement bas, ou nécessitant une ordonnance : leur mise en ligne est obligatoirement une arnaque.

Identification du prestataire

Le prestataire de commerce électronique doit afficher sur son site les informations suivantes (article 19 de la LCEN) :

- s'il s'agit d'une personne physique, ses nom et prénoms ;
- s'il s'agit d'une personne morale (entreprise, association...), sa dénomination ;
- son adresse, son adresse mail, le numéro de téléphone permettant d'entrer effectivement en contact ;
- si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, son titre professionnel, l'État membre de l'Union européenne dans lequel il a été octroyé, ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite ;
- dans le cas d'une personne morale :
 - son numéro d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, son capital social et l'adresse de son siège social ;
 - si elle est assujettie à la taxe sur la valeur ajoutée, son numéro individuel d'identification ;
 - si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci.

Précision Le numéro de téléphone est-il vraiment obligatoire ?

La Cour de justice européenne a estimé dans son arrêt du 16 octobre 2008 qu'il n'est pas obligatoire que le prestataire fournisse un numéro de téléphone. Selon la Cour, « le prestataire de services est tenu de fournir aux destinataires du service, dès avant toute conclusion de contrat avec ces derniers, en sus de son adresse de courrier électronique, d'autres informations permettant une prise de contact rapide ainsi qu'une communication directe et efficace. Ces informations ne doivent pas obligatoirement correspondre à un numéro de téléphone. Elles peuvent résider dans un formulaire de contact électronique, au moyen duquel les destinataires du service peuvent s'adresser sur Internet au prestataire de services et auquel celui-ci répond par courrier électronique, sauf dans des

situations où un destinataire du service, se trouvant, après la prise de contact par voie électronique avec le prestataire de services, privé d'accès au réseau électronique, demande à ce dernier l'accès à une voie de communication non électronique. »
L'interprétation de la Cour de justice de l'Union européenne s'impose aux États membres.

Détail de l'offre

L'article 19 de la LCEN prévoit que le prix correspondant à l'offre doit être mentionné « de manière claire et non ambiguë », et qu'il convient de préciser si les taxes et les frais de livraison sont inclus.

Paléowave Les prix sont-ils vraiment plus intéressants sur Internet ?

Le e-commerce accroît la concurrence entre les sites marchands et diminue leurs coûts (pas de magasin, pas de vendeur...), ce qui diminue logiquement les prix. Toutefois, deux pratiques ont été accusées de pousser les prix à la hausse. En effet, en analysant l'adresse IP de l'internaute, le commerçant peut localiser ce dernier géographiquement ou voir si l'internaute revient plusieurs fois sur un objet sans l'acheter.

Des chercheurs américains ont publié fin 2012 une étude montrant que certains sites de e-commerce affichaient des tarifs plus élevés pour les internautes dont l'adresse IP montrait qu'ils habitaient loin de tout magasin physique concurrent.

Par ailleurs, la gestion fine des tarifs en fonction de l'offre et de la demande (*yield management*), bien connue dans le transport aérien, a été accusée d'être dévoyée pour pousser les internautes indécis à l'achat, en augmentant les prix à chaque fois qu'ils revenaient sur la même page. Cette pratique, si elle était prouvée, serait illégale, mais aucune preuve n'a pu être apportée de son existence : les internautes qui ont constaté des hausses de tarif ont peut-être simplement été victimes du succès de l'offre convoitée. La Cnil a lancé fin 2013 une enquête sur ce sujet, qui n'a pas permis de démontrer l'existence de cette pratique.

S'il n'est pas exclu que certains e-commerçants peu scrupuleux mettent en œuvre de telles méthodes, la concurrence qui règne sur Internet devrait toutefois en limiter les effets.

Le prestataire de commerce électronique doit par ailleurs respecter les dispositions communes du Code de la consommation et notamment informer le consommateur sur les caractéristiques essentielles du bien ou du service proposé, et sur le délai d'exécution ou de livraison de la commande. La période pendant laquelle les pièces détachées éventuellement indispensables seront disponibles doit également être précisée (articles L111-1 à L111-3). Le vendeur doit enfin informer clairement le consommateur sur les prix, les limitations éventuelles de la responsabilité contractuelle et les conditions particulières de la vente. Lorsque le prix ne peut pas être calculé à l'avance, le mode de calcul du prix doit être communiqué (articles L113-3 et L113-3-1).

DÉTAIL Les réclamations

L'article L113-5 du Code de la consommation prévoit que le numéro de téléphone destiné à recueillir l'appel d'un consommateur en vue d'obtenir la bonne exécution d'un contrat conclu avec un professionnel ou le traitement d'une réclamation ne peut pas être surtaxé. Il est indiqué dans le contrat et dans la correspondance.

S'il ne respecte pas ces obligations du Code de la consommation, le professionnel est passible d'une amende de 3 000 euros pour une personne physique et de 15 000 euros pour une personne morale (articles L111-6, L113-3-2 et L113-6).

Responsabilité du prestataire

Le Code de la consommation (article L121-19-4) prévoit que le prestataire de commerce électronique est responsable à l'égard du consommateur de la bonne exécution des obligations résultant du contrat, que ces obligations soient à exécuter par le professionnel qui a conclu ce contrat ou par d'autres prestataires de services. S'il a recours à des sous-traitants et si ceux-ci sont les responsables de la défaillance éventuelle, il pourra dans un deuxième temps exercer lui-même un recours contre eux.

Toutefois, le prestataire peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable, soit au consommateur, soit à l'action, imprévisible et insurmontable, d'un tiers au contrat (par exemple grève du personnel de l'entreprise de livraison), soit à un cas de force majeure.

Précision Les places de marché et les sites de vente entre particuliers

Le commerce en ligne ne concerne pas que les vendeurs classiques. On y trouve également des acteurs comme eBay, PriceMinister ou leboncoin.fr, qui sont des sites de mise en contact entre vendeurs et acheteurs, mais qui ne vendent rien par eux-mêmes. On y trouve enfin, sur les sites de grands cybercommerçants (linac.com, Amazon...), des places de marché (*marketplace*) où se trouvent proposées les offres de vendeurs tiers. Dans ces cas de figure, le site web est considéré comme un hébergeur au sens de la loi pour la confiance dans l'économie numérique (LCEN). Il n'est pas responsable du contenu des annonces. N'étant pas le vendeur, il n'est pas non plus responsable en cas de problème à l'occasion de la vente.

Cela a par exemple été rappelé par le tribunal d'instance de Vienne le 12 novembre 2010 : saisi par des plaignants qui n'avaient jamais reçu un véhicule acheté sur eBay (et payé hors des procédures sécurisées proposée par le site), le tribunal a indiqué que « la société eBay a un statut d'hébergeur, en ce qu'elle n'intervient pas dans les transactions réalisées sur le site, mais seulement pour des prestations de courtage, c'est-à-dire en qualité de simple intermédiaire. [...] N'étant pas le vendeur, elle ne peut être tenue responsable du défaut de délivrance du véhicule, de sorte qu'il n'y a pas lieu de faire application de l'article L121-20-3 [ancienne numérotation du L121-19-4] du Code de la consommation ». Dans le même sens, le tribunal d'instance de Grenoble avait indiqué le 1^{er} février 2007 que les vendeurs d'objets sur eBay sont seuls responsables de la bonne exécution des contrats de vente conclus sur ce site.

Notons toutefois que le 31 mai 2013, le tribunal de commerce de Paris a estimé que le site 2xmoinscher.com n'est pas un hébergeur et ne peut bénéficier du régime de la LCEN. En effet, selon le tribunal, 2xmoinscher.com ne se limite pas à la mise en ligne des annonces, mais autorise les recherches par mots-clés, organise l'anonymat des vendeurs et des acheteurs, et joue un rôle de tiers de confiance dans les paiements, ce qui en fait un courtier en ligne.

Délai de livraison

Selon l'article L111-1 du Code de la consommation, le fournisseur doit indiquer, avant la conclusion du contrat, la date limite à laquelle il s'engage à livrer le bien ou à exécuter la prestation de services. À défaut, selon l'article L138-1, le fournisseur est réputé devoir délivrer le bien ou exécuter la prestation de services sans retard injustifié et au plus tard trente jours après la conclusion du contrat.

En cas de non-exécution du contrat dans ces délais, l'acheteur peut enjoindre, par lettre recommandée avec accusé de réception, le prestataire d'honorer la commande dans un délai supplémentaire raisonnable, et si le professionnel ne le fait pas, l'acheteur peut annuler le contrat. Le consommateur peut toutefois annuler immédiatement le contrat si la date de livraison en constituait une condition essentielle (article L138-2).

Le fournisseur doit alors rembourser le consommateur de la totalité des sommes versées, au plus tard dans les quatorze jours. Au-delà, la somme due est, de plein droit, majorée par la loi (article L138-3).

Garanties

L'acheteur bénéficie de plusieurs types de garanties.

- La *garantie légale de conformité*, prévue à l'article L211-4 du Code de la consommation, oblige le vendeur à « livrer un bien conforme au contrat et [à répondre] des défauts de conformité existant lors de la délivrance. Il répond également des défauts de conformité résultant de l'emballage, des instructions de montage ou de l'installation lorsque celle-ci a été mise à sa charge par le contrat ou a été réalisée sous sa responsabilité ». Cette garantie s'applique principalement à la vente d'objets. En cas de défaut de conformité, l'acheteur a le droit de choisir entre la réparation et le remplacement du bien, sauf si ce choix entraîne un coût manifestement

disproportionné au regard de l'autre modalité, compte tenu de la valeur du bien ou de l'importance du défaut (article L211-9 du Code de la consommation). Si la réparation et le remplacement du bien sont impossibles, l'acheteur peut rendre le bien et s'en faire restituer le prix (sauf si le défaut est mineur) ou garder le bien et se faire rembourser une partie du prix (article L211-10).

- La *garantie légale contre les vices cachés*, prévue à l'article 1641 du Code civil, prévoit que « le vendeur est tenu de la garantie à raison des défauts cachés de la chose vendue qui la rendent impropre à l'usage auquel on la destine, ou qui diminuent tellement cet usage que l'acheteur ne l'aurait pas acquise, ou n'en aurait donné qu'un moindre prix, s'il les avait connus ». Le défaut caché devait exister préalablement à la vente. L'acheteur peut actionner la garantie dans les deux ans qui suivent la découverte de ce vice. Si le vendeur était au courant du défaut et l'avait dissimulé à l'acquéreur, ce dernier peut réclamer des dommages et intérêts en plus du remboursement (article 1645 du Code civil).
- Le contrat de vente peut en outre prévoir des *garanties supplémentaires*, gratuites ou payantes : allongement de la durée de la garantie de fonctionnement, dépannage à domicile, rapidité de dépannage ou prêt d'un appareil de remplacement... Les conditions précises de cette garantie doivent être précisées dans le contrat de vente ou de souscription de garantie. Il en est de même du service après-vente pour l'électroménager.

La conclusion de l'achat

Sauf en cas de mention explicite de conditions de validité particulière, le cybercommerçant reste engagé par une offre tant qu'il la publie sur son site (article 1369-4 du Code civil).

Le Code civil (article 1369-5) prévoit également que pour que le contrat soit valablement conclu, le destinataire de

L'offre doit avoir eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de passer à l'étape finale de confirmation de la commande pour exprimer son acceptation.

L'auteur de l'offre doit accuser réception de la commande sans délai injustifié et par voie électronique (courriel ou page de confirmation).

Information du consommateur

Le Code de la consommation prévoit (article L121-17) que le consommateur doit recevoir avant la conclusion du contrat :

- les caractéristiques essentielles du bien ou du service commandé, et le délai d'exécution ou de livraison de la commande ;
- une information sur les conditions et les modalités d'exercice du droit de rétractation ;
- les coordonnées du professionnel et le mode de règlement des litiges ;
- les informations relatives aux garanties commerciales et autres conditions contractuelles, telles que le service après-vente ;
- les conditions de résiliation du contrat.

Il est conseillé de conserver une copie de ces informations, pour en avoir une trace en cas de litige.

Par ailleurs, les moyens de communication permettant au consommateur de suivre l'exécution de sa commande, d'exercer son droit de rétractation ou de faire jouer la garantie ne doivent engendrer que des coûts de communication et ne faire l'objet d'aucun coût complémentaire spécifique.

Cas du m-commerce

L'article L121-19-1 prévoit que lorsque la technique utilisée (par exemple un achat sur smartphone) impose des limites d'espace ou de temps à l'information du client, le vendeur doit au moins communiquer avant la conclusion du contrat les informations relatives aux caractéristiques essentielles des biens ou des services, à leur prix, à son identité, à la durée du contrat et au droit de rétractation.

Droit de rétractation

Selon l'article L121-21 du Code de la consommation, le consommateur dispose d'un délai de quatorze jours pour exercer son droit de rétractation sans avoir à justifier de motifs ni à payer de pénalités, à l'exception, le cas échéant, des frais de retour. Ce délai court à partir de la conclusion du contrat s'il s'agit d'une prestation de services, ou de la livraison s'il s'agit d'un achat de biens. S'il y a plusieurs livraisons, c'est la première qui est prise en compte.

Lorsque les informations sur le droit de rétractation prévues à l'article L121-17 n'ont pas été fournies, le délai d'exercice de ce droit de rétractation est prolongé de douze mois. Toutefois, lorsque la fourniture de ces informations intervient pendant cette prolongation, elle déclenche le délai normal de quatorze jours.

Le consommateur doit donc adresser au vendeur, dans le délai de quatorze jours, un formulaire de rétractation (éventuellement en ligne) ou une déclaration dénuée d'ambiguïté, exprimant sa volonté de se rétracter. Il doit ensuite, dans les quatorze jours suivant la communication de sa décision, renvoyer les biens au professionnel. Le consommateur supporte les frais de renvoi, sauf si le professionnel accepte de les prendre à sa charge ou s'il a omis d'informer le consommateur que ces coûts sont à sa charge.

Exception au droit de rétractation

Article L121-21-8 : le droit de rétractation ne peut être exercé pour les contrats :

- 1° de fourniture de services pleinement exécutés et dont l'exécution a commencé, avec l'accord du consommateur, avant la fin du délai de rétractation ;
- 2° de fourniture de biens ou de services dont le prix est fonction de fluctuations des taux du marché financier ;
- 3° de fourniture de biens confectionnés selon les spécifications du consommateur ou nettement personnalisés ou qui, du fait de leur nature, ne peuvent être réexpédiés ou sont susceptibles de se détériorer ou de se périmer rapidement ;
- 4° de fourniture d'enregistrements audio ou vidéo ou de logiciels informatiques lorsqu'ils ont été descellés par le consommateur ;
- 5° de biens descellés qui ne peuvent être renvoyés pour raison d'hygiène ou de santé ;
- 6° de fourniture de journaux, de périodiques ou de magazines ;
- 7° de téléchargement d'un contenu numérique dont l'exécution a commencé après accord de l'acheteur et renonciation à son droit de rétractation.

Dans le cas où le consommateur exerce son droit de rétractation sur une prestation de services qui a commencé, avec son accord, avant la fin du délai de rétractation, il doit verser au prestataire un montant correspondant au service fourni jusqu'à la communication de sa décision (article L121-21-5).

Selon l'article L121-21-4 du Code de la consommation, lorsque le droit de rétractation est exercé, le professionnel est tenu de rembourser le consommateur de la totalité des sommes versées, dans les meilleurs délais et au plus tard dans les quatorze jours à compter de la communication de la décision. Pour la vente de biens, ce remboursement peut être différé jusqu'à la récupération des biens, ou jusqu'à la communication par le consommateur d'une preuve du renvoi. Au-delà, la somme due est, de plein droit, productive d'intérêts à des taux majorés fixés par la loi. Ce remboursement s'effectue par le moyen de paiement utilisé pour l'achat. Sur proposition du professionnel, le consommateur ayant exercé son droit de rétractation peut toutefois opter pour une autre modalité de remboursement.

ANALYSE JURISPRUDENCIELLE Contrat d'assurance conclu à distance

La Cour de cassation a précisé le 17 janvier 2013 que dans le cas des contrats d'assurance conclus à distance, le paiement de la prime par le client avant la fin du délai de rétractation ne signifie pas que le client a expressément demandé le commencement immédiat de l'exécution de la prestation. En conséquence, le client qui n'a pas demandé expressément l'application immédiate de la garantie peut, même après avoir payé la prime d'assurance, exercer son droit de rétractation dans le délai légal.

Courriels publicitaires et offres promotionnelles

Selon l'article L121-15-1 du Code de la consommation, les publicités, et notamment les offres promotionnelles, telles que les rabais, les primes ou les cadeaux, ainsi que les concours ou les jeux promotionnels, adressés par courrier électronique, doivent pouvoir être identifiés de manière claire et non équivoque dès leur réception par leur destinataire, ou en cas d'impossibilité technique, dans le corps du message.

Ces messages doivent indiquer une adresse ou un moyen électronique servant effectivement au destinataire qui veut faire valoir son droit d'opposition, en transmettant une demande visant à obtenir que ces publicités cessent.

Par ailleurs, la publicité par courriel vers des personnes qui n'ont pas préalablement consenti à recevoir des messages (*spam*) est interdite (article L34-5 du Code des postes et communications électroniques).

SANCTION Le spam

Un commerçant qui envoie des spams publicitaires est passible de plusieurs sortes de sanctions :

- en cas de plainte devant un tribunal, il peut se voir condamner à une amende de 750 euros pour chaque courriel envoyé (article R10-1 du Code des postes et communications électroniques) ;
- s'il a en outre collecté les adresses mails des destinataires d'une manière illicite ou frauduleuse, il risque cinq ans de prison et 300 000 euros d'amende (article 226-18 du Code pénal) ;
- en cas de plainte devant la Cnil, celle-ci peut lui infliger une sanction d'un montant maximal de 150 000 euros (loi Informatique et Libertés).

Toutefois, la publicité par courriel est autorisée si l'adresse du destinataire a été recueillie auprès de lui à l'occasion d'une précédente vente de biens ou de services, et si la publicité en question concerne le même type de biens ou de services proposés par le même prestataire. En outre, le destinataire doit avoir la possibilité, lors de la vente initiale puis lors de chaque réception de courriel, de s'opposer sans frais à la poursuite de l'utilisation de ses coordonnées.

Dans tous les cas, il est interdit d'émettre des courriels publicitaires sans indiquer de coordonnées valables auxquelles le destinataire peut transmettre une demande d'opposition. Il est également interdit de dissimuler l'identité de l'émetteur et de mentionner en objet du message publicitaire un intitulé sans rapport avec la prestation ou le service proposé.

Auprès de qui se tourner en cas de litige ?

En cas de litige avec un prestataire de commerce électronique, le client peut s'adresser pour conseil à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF). Celle-ci propose sur son site web des fiches pratiques. Elle indique également les coordonnées des

associations de consommateurs. Un règlement du litige à l'amiable est recommandé. En cas d'impossibilité de trouver un accord amiable, elle expose les démarches à effectuer. Ses services sont joignables par téléphone au 3939.

Si le cybercommerçant est membre d'une association professionnelle (par exemple la Fédération du e-commerce et de la vente à distance, www.fevad.com), il est également possible d'alerter celle-ci.

LE POINT DE VUE DU SPÉCIALISTE **Marc Lolivier, délégué général de la Fevad (Fédération du e-commerce et de la vente à distance)**

Comment se positionne le e-commerce ?

Le e-commerce a connu une croissance extrêmement rapide, surtout depuis 2004 et le déploiement de l'ADSL. Il représente actuellement en France 57 milliards d'euros de chiffre d'affaires, 500 millions de transactions par an, 32 millions d'acheteurs et plus de 150 000 sites marchands. Le e-commerce représente aujourd'hui 9 % du commerce de détail hors alimentaire. Il pourrait d'ici 2020 dépasser les 20 %. Sa croissance demeure à des niveaux élevés, de l'ordre de 10 % par an, ce qui en fait le premier secteur de l'économie numérique, devant les télécoms. On constate un véritable engouement des clients pour ce mode de consommation, qui ne remplace pas le commerce traditionnel mais qui lui est complémentaire : de plus en plus de magasins ont une présence sur le Web et les clients utilisent Internet pour se renseigner et pour comparer avant d'aller acheter en boutique. Il s'agit d'une manière nouvelle de consommer et de vendre.

Quelles sont les nouvelles tendances ?

On voit apparaître la combinaison de la commande en ligne et du retrait en magasin, pour l'alimentaire notamment avec le *drive*. Le client combine ainsi le meilleur de chaque canal : par Internet il dispose d'une offre 24h/24 et de la possibilité de comparer, puis en magasin il bénéficie de la disponibilité du produit.

Avec la généralisation des smartphones, le m-commerce fait également irruption au cœur même des magasins. Dans certains cas, en boutique, le client finalise son acte d'achat en présence d'un vendeur mais sur le site Internet. Cela pose la question du régime juridique applicable : s'agit-il de vente à distance (avec ses conséquences notamment en termes de droit de rétractation) ou de vente en boutique ? Le régime juridique applicable dépend en fait de celui avec lequel le client signe le contrat : s'il s'agit du site web, on est en vente à distance, s'il s'agit du magasin, on est en boutique.

Y a-t-il des chartes de qualité et de confiance ?

Tous les adhérents de la Fevad, soit plus de 570 entreprises et plus de 800 sites Internet, s'engagent à respecter ses codes déontologiques, par exemple sur les bonnes pratiques et sur les courriels publicitaires, avec des exigences supérieures à celles de la loi.

En cas de problème rencontré avec une entreprise membre de la Fevad, le client peut contacter celle-ci aux coordonnées disponibles sur son site www.fevad.com. La fédération s'efforcera de trouver un accord amiable, ou saisira si besoin le médiateur du e-commerce.

Constate-t-on une crise de confiance ?

Au contraire, le niveau de satisfaction est très élevé. C'est indispensable, car la confiance est au cœur du développement du e-commerce. Nous sommes donc collectivement vigilants pour mériter et conserver la confiance des clients. Rappelons que le commerce dans son ensemble (traditionnel et électronique confondus) a engendré en 2012 environ 20 000 réclamations à la DGCCRF et 1 200 plaintes à la Gnl, chiffres à comparer aux 500 millions de transactions du seul e-commerce. La Fevad quant à elle reçoit 1 500 réclamations par an, qui sont réglées dans les 10 jours pour 99 % des cas. Le nombre de litiges est donc extrêmement réduit par rapport au nombre de clients satisfaits.

Le e-commerce transfrontalier se développe-t-il ?

Le public étranger représente un relais de croissance pour les commerçants français ; inversement, 25 % des internautes français ont commandé en ligne à l'étranger. Les facteurs déterminants sont l'offre (produit qui n'est pas proposé sur un site national) et le prix (pour les produits standardisés). Toutefois, acheter à l'étranger comporte plus de risques. Dans l'Union européenne, les droits des consommateurs sont harmonisés ; en revanche un achat hors Union est moins protecteur : il faut prévoir des droits de douane et, en cas de litige, il faut déterminer la localisation du vendeur pour savoir quel est le droit applicable.

En conclusion, Internet révolutionne la consommation, comme il a révolutionné la communication, la politique, l'éducation... Et cette révolution est portée par les clients, il y a une énorme attente de leur part, on ne peut pas ne pas y être.

Le paiement en ligne

L'internaute dispose de plusieurs moyens de payer un achat en ligne : l'envoi d'un chèque, le paiement par carte bancaire, la création d'un compte PayPal, un virement bancaire, un virement par Western Union ou par un organisme similaire, l'utilisation d'une monnaie virtuelle comme le *bitcoin*...

Précision Faut-il déclarer son compte PayPal au fisc ?

Le 25 avril 2013, le tribunal administratif de Pau a validé une amende de 750 euros infligée par le fisc à une personne qui n'avait pas déclaré son compte PayPal : en effet, selon le fisc, la société PayPal étant localisée au Luxembourg, un compte PayPal est considéré comme un compte à l'étranger.

Suite à l'émotion suscitée parmi les internautes par cette nouvelle, le ministère des Finances a précisé que la personne à qui l'amende a été infligée était un commerçant qui se servait de son compte PayPal pour encaisser des recettes. L'administration fiscale n'exige pas de déclaration pour les comptes à l'étranger servant à payer des achats en ligne ou à encaisser le règlement de la vente de biens, à condition que ces comptes soient adossés à un compte en France et que les encaissements concernant des ventes ne dépassent pas 10 000 euros par an.

Les virements par organismes du type Western Union ou par monnaie virtuelle sont à déconseiller, car l'argent peut aboutir sur des comptes anonymes, ce qui est souvent utilisé par des cyberescrocs pour détrousser des clients crédules avant de disparaître sans livrer les biens commandés. Ces systèmes peuvent également servir, toujours en raison de leur anonymat, à blanchir de l'argent sale.

En mai 2013, les responsables de l'émetteur de monnaie numérique Liberty Reserve ont été arrêtés aux États-Unis et accusés d'avoir blanchi six milliards de dollars au profit du crime organisé. En permettant des transferts anonymes d'argent dans le monde entier, sans aucune vérification de légalité et sans traçabilité, Liberty Reserve était devenu l'outil idéal pour les cybercriminels ainsi que pour les trafiquants traditionnels.

Le paiement par carte bancaire

Le paiement par le numéro de carte bancaire est le moyen de paiement le plus répandu pour les achats en ligne : l'internaute est invité à donner les éléments suivants :

- le numéro de carte ;
- la date d'expiration ;
- éventuellement le nom du titulaire ;
- le « cryptogramme visuel » (ou « code de sécurité », ou « code de vérification »), c'est-à-dire en général les trois ou quatre chiffres inscrits, soit au dos de la carte près de la zone de signature, soit au recto près du numéro de carte (selon les modèles de cartes).

Zoom Le cryptogramme visuel et le code PIN

Il ne faut pas confondre le cryptogramme visuel avec le code secret (ou « code PIN »). Le code PIN (*Personal Identification Number*) sert uniquement à activer la puce électronique de la carte. Le contrat d'abonnement stipule que le titulaire doit conserver ce code secret et ne le divulguer à personne. En effet, par sécurité, la puce est conçue pour ne fonctionner que si le code PIN a été tapé. Le terminal sur lequel ce code est saisi est lui aussi spécialement conçu pour ne pas divulguer le code. Cela assure que seul le titulaire de la carte peut activer la puce, puisqu'il est le seul à connaître le code.

Le cryptogramme visuel, quant à lui, n'a rien de secret puisqu'il est écrit sur la carte et qu'on l'envoie sur Internet. Il sert juste à éviter que lors d'un paiement en boutique, un vendeur indelicat relève le numéro de carte pour l'utiliser ensuite sur Internet. En effet, le vendeur en boutique n'a normalement pas la possibilité de voir le cryptogramme visuel.

Le cryptogramme visuel ne constitue pas une protection très efficace, puisqu'il n'empêche ni l'usage de la carte sur Internet par un éventuel voleur, ni la réutilisation frauduleuse des éléments par un cybercommerçant indelicat.

C'est pourquoi la loi protège le titulaire de la carte en prévoyant que « la responsabilité du payeur n'est pas engagée en cas d'opération de paiement non autorisée effectuée sans utilisation du dispositif de sécurité personnalisé », et que « la responsabilité du payeur n'est pas engagée si l'opération de paiement non autorisée a été effectuée en détournant, à l'insu du payeur, l'instrument de paiement ou les données qui lui sont liées » (Code monétaire et financier, article L133-19, alinéas I et II). Cela signifie que si, dans un acte de paiement, le code PIN n'a pas été tapé et la puce pas activée (ce qui est le cas pour un paiement en ligne), alors le titulaire de la carte peut contester l'achat auprès du prestataire de services de paiement (banque ou organisme de crédit) qui lui a fourni la carte. Dans ce cas, le client a automatiquement gain de cause et le prestataire financier doit lui rembourser l'achat sans discussion.

Précision Le risque d'abus

Le droit de contester tout achat effectué en ligne et de se faire rembourser automatiquement les montants prélevés ne doit pas inciter le titulaire de la carte à se faire rembourser abusivement des achats qu'il aurait réellement effectués. Certes, le prestataire de services de paiement doit rembourser, mais s'il suspecte une fraude, une enquête peut être diligentée : si l'on s'aperçoit que les biens achetés en ligne ont été livrés au domicile du titulaire de la carte, celui-ci aura quelques explications à donner sur cette escroquerie.

Même lorsque le code PIN a été tapé et la puce activée, le client peut constater une erreur et contester le paiement. Dans ce cas, il revient à son prestataire de prouver la réalité de l'achat. En effet, la loi dispose que « lorsqu'un utilisateur de services de paiement nie avoir autorisé une opération de paiement qui a été exécutée, ou affirme que l'opération de paiement n'a pas été exécutée correctement, il incombe à son prestataire de services de paiement de prouver que l'opération en question a été authentifiée, dûment enregistrée et comptabilisée ».

lisée et qu'elle n'a pas été affectée par une déficience technique ou autre » (Code monétaire et financier, article L133-23).

Sécurité 3D Secure

Pour éviter la fraude à l'utilisation en ligne du numéro de carte bancaire, les banques françaises proposent aux cybercommerçants le système 3D Secure : lorsque l'internaute veut payer avec son numéro de carte, il est redirigé vers le site web de sa banque. Il lui est alors demandé de taper, soit une information convenue à l'avance (date de naissance, etc.), soit un code secret à usage unique qui lui est envoyé en temps réel par SMS sur le numéro de portable connu de la banque. La banque vérifie ainsi que la personne en train d'effectuer l'achat est bien le titulaire légitime de la carte.

Notons bien que l'objectif de 3D Secure est de protéger le cybercommerçant contre la fraude, et non le client. Comme nous l'avons vu, ce dernier est déjà protégé par la loi. L'accueil réservé à 3D Secure par les cybercommerçants est mitigé. En effet, en allongeant le mécanisme d'achat et en désorientant le client (qui ne comprend pas pourquoi il se retrouve sur le site d'une banque sans l'avoir demandé), 3D Secure conduit un certain nombre de clients à abandonner l'achat en cours. Il entraîne donc une perte de chiffre d'affaires pour les commerçants.

Le délai pour contester un paiement est de treize mois après le débit (Code monétaire et financier, article L133-24).

En cas d'opération de paiement non autorisée signalée par l'utilisateur, le prestataire doit rembourser immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablir le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu (Code monétaire et financier, article L133-18).

Pour éviter l'utilisation en ligne d'un numéro de carte à l'insu de son propriétaire, certaines banques proposent à leurs clients des e-cartes bancaires, qui sont des numéros « jetables » utilisables une seule fois.

ANALYSE Protection du client en cas d'usage du code PIN

Jusqu'à récemment, lorsqu'une carte de crédit volée était utilisée avec son code PIN pour acheter des biens en boutique ou pour retirer de l'argent à un distributeur, les tribunaux condamnaient le titulaire de la carte à payer les sommes dépensées jusqu'au moment de la mise en opposition de la carte, en estimant que celui-ci avait été négligent puisqu'on lui avait volé son code avec sa carte. Cependant, les progrès des voleurs, qui savent désormais espionner un code grâce à des microcaméras sans négligence de la part du titulaire, ont été pris en compte par la Cour de cassation. Celle-ci a reconnu le 2 octobre 2007 qu'une utilisation frauduleuse de carte avec code PIN était possible sans impliquer une négligence de la part de son titulaire et qu'il revient donc à la banque de prouver que le client a commis une faute lourde pour ne pas avoir à le rembourser. La charge de la preuve repose donc désormais sur le prestataire de services de paiement : s'il ne veut pas rembourser un achat ou un retrait effectué avec code PIN, il doit démontrer la négligence de son client. La Cour de cassation a confirmé cette position le 21 septembre 2010. La rédaction du Code monétaire et financier a été remaniée suite à ces arrêts de la Cour de cassation. La version actuelle de la loi prévoit donc que le porteur de la carte a pour obligations :

- de prendre « toute mesure raisonnable pour préserver la sécurité » de son code PIN (article L133-16) ;
- d'avertir « sans tarder » le prestataire en cas de perte ou de vol de la carte, pour la mettre en opposition (article L133-17). Si la carte a été utilisée avant cette mise en opposition, le titulaire en supporte les pertes jusqu'à un plafond de 150 euros (article L133-19). Après la mise en opposition, il est déchargé de toute responsabilité (article L133-20).

Ce n'est que s'il n'a pas satisfait à ces exigences, « intentionnellement ou par négligence grave », ou alors évidemment s'il s'agit d'un comportement frauduleux de sa part, que le titulaire supporte toutes les pertes occasionnées par des opérations de paiement non autorisées (article L133-19 IV).

Ainsi, la Cour de cassation a confirmé le 16 octobre 2012 qu'une personne qui a reconnu avoir laissé dans sa voiture sa carte bancaire avec son code PIN, avait commis une faute lourde justifiant qu'elle doive supporter les pertes qui ont résulté du vol de la carte et du code.

Fin 2013, plusieurs banques françaises ont lancé Paylib, une application de paiement en ligne (fixe ou mobile) destinée à

concurrencer PayPal. En choisissant Paylib pour régler ses achats, l'internaute n'aura plus à donner au commerçant son numéro de carte bancaire : *via* l'application Paylib, il donnera instruction à sa banque de régler le commerçant. En évitant de diffuser les numéros de carte bancaire, cette application devrait faire reculer les usurpations de carte.

Les ventes entre particuliers

Les sites de vente entre particuliers, à prix fixes ou aux enchères (eBay, PriceMinister, leboncoin.fr...) se multiplient et sont l'occasion de faire de bonnes affaires, à condition de respecter quelques règles de prudence :

- privilégier les sites connus ;
- consulter, si cette information est disponible, l'historique ou l'évaluation du vendeur ;
- ne pas conclure la vente en dehors des procédures du site, si celui-ci assure et garantit la transaction ;
- ne pas envoyer d'argent par des organismes assurant l'anonymat (type Western Union) ;
- ne pas envoyer de somme importante avant d'avoir reçu le bien.

Pour les acheteurs, ces précautions élémentaires permettent d'éviter des déconvenues.

En mai 2014, le tribunal correctionnel d'Alès a condamné à deux ans de prison ferme un escroc qui postait des annonces sur leboncoin.fr, mais n'envoyait jamais les objets payés par les acheteurs. Le préjudice était estimé à 15 000 euros.

Pour des faits similaires, le tribunal correctionnel de Grasse avait condamné en septembre 2012 un autre escroc à un an de prison ferme.

Les obligations du vendeur particulier

Le vendeur particulier est soumis à moins d'obligations que le vendeur professionnel (ce qui signifie que l'acheteur bénéficie de moins de protection...).

Le vendeur doit communiquer à l'acheteur les caractéristiques essentielles du bien ou du service, ainsi que le prix de vente et les frais éventuels de livraison.

Il n'y a pas, dans le cas d'un vendeur particulier, de droit automatique de rétractation. Le vendeur peut accepter de reprendre un bien, mais ce n'est pas une obligation, contrairement au vendeur professionnel.

En revanche, le vendeur particulier est tenu à la garantie légale contre les vices cachés (voir plus haut), même en l'absence de contrat écrit.

Jurisprudence Une moindre protection de l'acheteur

Dans son jugement du 25 juin 2013, la juridiction de proximité de Paris 3^e arrondissement a débouté une personne qui avait acheté à un particulier sur *PriceMinister* une imprimante qui s'était avérée défectueuse. L'acheteur invoquait les articles du Code de la consommation concernant son droit de rétractation et la garantie légale de conformité pour demander l'annulation de la vente. Cependant, constatant que le vendeur était un particulier alors que le Code de la consommation ne s'applique qu'aux vendeurs professionnels, la juridiction a confirmé que l'acheteur ne pouvait bénéficier de ces droits.

Si l'acheteur avait invoqué l'article 1641 du Code civil (garantie contre les vices cachés), peut-être aurait-il pu faire annuler la transaction litigieuse... D'où l'importance de bien choisir les textes de loi sur lesquels baser un recours.

Le vendeur particulier doit-il déclarer ses ventes au fisc ?

La revente par un particulier de ses objets d'occasion ou de collection ne constitue pas une activité devant faire l'objet d'une déclaration au fisc. Évidemment, cela implique que ces ventes demeurent marginales et ne constituent pas une source

de revenu régulier voire un commerce, c'est-à-dire la vente d'objets achetés spécifiquement dans le but d'être revendus. La loi ne fixe pas de seuil (en nombre de ventes par an, ou en montant des ventes) au-delà duquel le vendeur serait automatiquement considéré comme professionnel.

Au regard du Code du commerce (article L121-1), seuls « sont commerçants ceux qui exercent des actes de commerce et en font leur profession habituelle ». Si l'internaute achète des objets pour les revendre, organise son activité dans cette optique (voire crée une boutique en ligne...) et en tire des revenus réguliers, alors il devient commerçant et doit s'acquitter d'obligations fiscales (déclaration des revenus de cette activité) et sociales (cotisations), en adoptant un statut approprié (par exemple auto-entrepreneur ou SARL).

Jurisprudences sur les ventes *via* eBay

Le 26 mars 2007, le tribunal d'instance de Rennes avait créé la surprise en retenant la responsabilité résiduelle d'eBay dans une affaire d'escroquerie à la vente en ligne. Un acheteur se plaignait de ne jamais avoir reçu le bien qu'il avait acheté suite à une annonce sur eBay. Cet acheteur avait été bien imprudent, puisqu'au lieu d'utiliser les services sécurisés d'eBay, il avait correspondu directement par courriel avec le vendeur et lui avait envoyé le paiement par mandat Western Union à l'étranger, tout cela malgré un courriel d'eBay lui déconseillant de conclure cette transaction. Il s'agissait évidemment d'une escroquerie. Néanmoins, le tribunal a estimé que la société eBay portait une responsabilité partielle dans cette escroquerie en ne démontrant pas qu'elle avait satisfait à ses obligations d'information de ses clients sur les risques de fraude. eBay avait été condamné à rembourser 20 % de la somme escroquée.

Ce jugement était surprenant, d'une part parce qu'eBay n'avait évidemment aucune complicité dans le montage de l'escroquerie et d'autre part surtout parce que la loi ne prévoit aucune obligation d'information. Il s'agissait là aussi d'une création du droit pré-torien.

L'affaire fut portée devant la cour d'appel de Rennes, mais un accord transactionnel étant survenu entre les parties, le dossier fut clos.

Dans un dossier similaire (escroc proposant un bien sur eBay, acheteur crédule virant de l'argent à l'étranger en dehors des procédures sécurisées du site), le tribunal d'instance de Grenoble avait retenu le 1^{er} février 2007 une solution plus classique en notant que l'acheteur « n'a pas utilisé les moyens de paiement sécurisés mis à sa disposition par eBay et n'a pas respecté les règles élémentaires de sécurité » et qu'il « a fait preuve d'une particulière imprudence, laquelle a largement concouru à la réalisation de son préjudice alors qu'aucune faute n'est démontrée de la part d'eBay ». Il concluait que les vendeurs d'objets sur eBay sont seuls responsables de la bonne exécution des contrats de vente.

Citons encore un dossier semblable et une décision classique, au tribunal d'instance de Vienne le 12 novembre 2010 : saisi par des plaignants qui n'avaient jamais reçu un véhicule acheté sur eBay (et payé hors des procédures sécurisées proposées par le site), le tribunal a indiqué que « la société eBay a un statut d'hébergeur, en ce qu'elle n'intervient pas dans les transactions réalisées sur le site, mais seulement pour des prestations de courtage, c'est-à-dire en qualité de simple intermédiaire. [...] N'étant pas le vendeur, elle ne peut être tenue responsable du défaut de délivrance du véhicule ». Le tribunal prenait par ailleurs acte de ce que le site d'eBay arborait de manière très visible des avertissements sur les risques de fraude (souvenir du jugement de Rennes en 2007 ?) : « il convient d'observer que selon le procès-verbal de constat sur

Internet [...], une information complète et précise sur les risques de fraude et sur la sécurité des transactions étaient en ligne sur le site et ces recommandations étaient facilement accessibles pour les utilisateurs », ce qui rendait d'autant plus impardonnable l'imprudence des acheteurs.

Notons que dans les trois cas, les escrocs avaient envoyé aux acheteurs crédules des courriels usurpant ou imitant le logo, l'adresse électronique et le nom d'eBay. Attention donc aux messages incitant à envoyer de l'argent par des procédures exotiques ; encore une fois, il est vivement recommandé de suivre les procédures sécurisées proposées par les prestataires web.

Les sites de mise en relation

Les sites permettant aux particuliers d'échanger des services se multiplient et leur succès empiète parfois sur des formes traditionnelles de commerce. Par exemple, le site AirBnB permet les locations touristiques temporaires entre particuliers. Les hôteliers et les municipalités (qui perçoivent des taxes de séjour) y perdent des recettes.

Le 13 février 2014, le tribunal de grande instance de Paris a rappelé que si la loi autorise un locataire à loger chez lui qui bon lui semble, il ne peut en tirer un profit financier. La sous-location à titre onéreux est interdite. Il a donc condamné une personne qui sous-louait des pièces de son appartement *via* AirBnB à cesser cette pratique et à rembourser à son propriétaire les frais de justice.

Les autres transactions financières en ligne

En dehors des achats sur Internet, l'internaute peut également se connecter au site de sa banque ou accéder à des jeux d'argent et à des paris en ligne.

La banque en ligne

Votre banque traditionnelle vous propose de réaliser en ligne certaines opérations (consultation de compte, virement, ordre de bourse...). Certaines banques totalement dématérialisées n'existent que sur Internet et n'ont pas d'agence : vous ouvrez un compte en ligne, vous envoyez (par poste ou par courriel) vos documents justificatifs, puis vous utilisez tous les services qui vous sont proposés.

L'accès à la banque en ligne se fait après vérification de votre identité par, le plus souvent, une procédure de login/mot de passe. Le niveau de sécurité de cette procédure est sommaire, mais suffisant pour une simple consultation de compte ou pour un virement entre comptes d'une même personne. Pour des opérations potentiellement plus risquées, comme un virement vers un nouveau compte externe ou un ordre de bourse, la banque peut mettre en place une vérification plus poussée de l'identité du titulaire, par exemple en demandant une validation par SMS. Pour des actes nécessitant une signature (ouverture d'un livret d'épargne ou d'un plan d'épargne en actions, souscription d'une assurance-vie ou d'un emprunt...), la banque peut proposer une solution de signature électronique. De plus en plus fréquemment, cette signature électronique est proposée sous une forme ergonomique ne nécessitant pas d'installation d'application sur l'ordinateur.

Précision La signature électronique

L'article 1316-4 du Code civil prévoit l'équivalence juridique de la signature électronique et de la signature manuscrite. Concrètement, pour signer électroniquement, le client prend connaissance du document à signer, puis marque son approbation en tapant un code qui lui a été communiqué par sa banque. Le système enregistre alors de manière infalsifiable à la fois le contenu du texte signé et la marque du consentement du signataire calculée à partir de son code secret.

Techniquement, lorsque l'on paie en boutique avec sa carte bancaire en tapant son code secret, on réalise en fait une signature électronique de la facture éditée par le commerçant. Une carte bancaire serait d'ailleurs capable de signer n'importe quel type de document, pourvu qu'elle soit couplée à l'ordinateur par un lecteur adéquat.

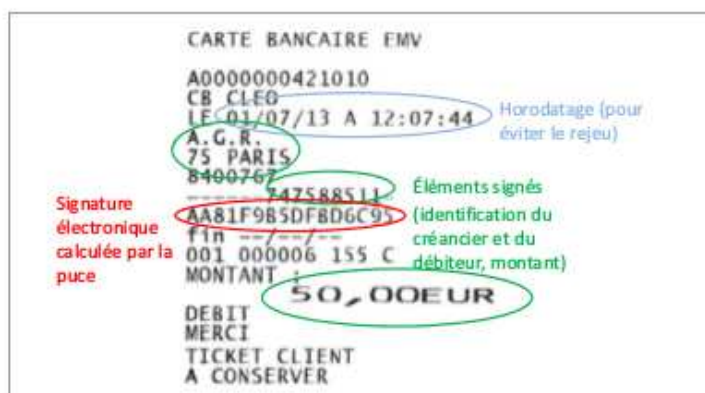


Fig. 6-1 > Exemple de facturette CB.

Dans cet exemple de facturette, la mention de la date et de l'heure empêche de présenter deux fois la facture à la banque (rejeu). Les éléments signés (infalsifiables) sont l'identification du créancier et du débiteur (*via* son numéro de CB), ainsi que le montant de la transaction. La saisie du code secret déclenche dans la puce le calcul de la ligne hexadécimale (signature), dont on peut prouver mathématiquement qu'elle

n'a pu être calculée que par la puce de la carte en question, et à partir des éléments signés.

La monnaie électronique

Le Code monétaire et financier (articles L315-1 et suivants) définit la monnaie électronique comme le stockage, sous forme électronique ou magnétique, de fonds qui sont remis à l'émetteur, en vue d'une utilisation auprès d'autres entités. Il y a donc équivalence à l'euro entre l'argent déposé et l'argent inscrit sous forme électronique (moins celui qui est ensuite dépensé). Le Code interdit toute rémunération du porteur, tout versement d'intérêts sur les sommes déposées, ou tout autre avantage lié à la durée de détention.

Avant la délivrance de la monnaie électronique, le futur client doit se voir délivrer une information en français « dans des termes clairs et aisément compréhensibles ». Les conditions et les frais éventuels de remboursements doivent être précisés.

Les points de fidélité qui sont distribués par certaines compagnies à leurs clients et qui servent à acheter des prestations, ne constituent pas une monnaie électronique car ils ne sont pas la contrepartie d'une somme réelle qui aurait été déposée.

Des systèmes de monnaie alternative comme bitcoin ont également été lancés. Il s'agit d'une monnaie privée émise par des ordinateurs répartis dans le monde, et convertible en devises. La relative opacité du système peut favoriser la spéculation et son utilisation pour le blanchiment d'argent.

Les jeux en ligne

Les jeux d'argent et de hasard sont traditionnellement un monopole d'État, à la fois pour protéger les joueurs des escroqueries et de l'addiction, et pour éviter le blanchiment que ces activités facilitent. Sous la pression des sites web de poker ou

de paris ouverts dans les autres pays de l'Union européenne, la France a libéralisé en 2010 les jeux et paris en ligne.

Comme leurs homologues traditionnels, ces services sont interdits aux mineurs.

La loi du 12 mai 2010 oblige les sociétés désirant opérer en France des jeux d'argent ou des paris en ligne à solliciter un agrément de l'Autorité de régulation des jeux en ligne (ARJEL).

Pour jouer ou parier, l'internaute doit obligatoirement s'inscrire auprès de l'opérateur en lui fournissant des justificatifs de son identité, de son âge et de son adresse ; il doit également fournir des coordonnées bancaires pour pouvoir toucher ses gains. Le compte du joueur auprès de l'opérateur ne peut être approvisionné que *via* un organisme financier (les versements en liquide sont impossibles).

Le fait de proposer au public des paris ou des jeux d'argent sans être titulaire d'un agrément de l'ARJEL est puni de trois ans d'emprisonnement et de 90 000 € d'amende. Ces peines sont portées à sept ans d'emprisonnement et à 200 000 € d'amende lorsque l'infraction est commise en bande organisée.



Internet dans la vie professionnelle

Le salarié doit certes utiliser son temps de travail à remplir les missions professionnelles confiées par son employeur, mais un certain droit à la vie privée sur le lieu de travail lui est néanmoins reconnu. Ce droit inclut traditionnellement la possibilité d'utiliser les moyens fournis par l'employeur (téléphone, ordinateur, connexion Internet...) à titre personnel, dans des limites strictes.

Avec le développement du télétravail, de l'utilisation à domicile de l'ordinateur portable professionnel et enfin de son inverse le BYOD (*Bring your own device*, utilisation au bureau de son ordinateur personnel, plus performant ou plus pratique que celui fourni par l'employeur), la frontière entre utilisation professionnelle et utilisation personnelle devient de plus en plus difficile à tracer.

L'usage d'Internet au bureau à titre personnel

Les connexions Internet au bureau sont présumées professionnelles. Les connexions pour un usage personnel pendant le temps de travail sont tolérées, à condition de rester dans des limites raisonnables et de ne pas mettre en danger la sécurité du réseau informatique de l'entreprise. Lorsque l'utilisation personnelle d'Internet devient excessive, le licenciement pour faute grave est justifié.

La Cour de cassation a considéré le 26 février 2013 que « présentait un caractère particulièrement abusif et constitutif d'une faute grave », même en l'absence d'une définition précise du poste du salarié, le fait de se connecter « pendant son temps de travail à de très nombreuses reprises à de nombreux sites extraprofessionnels tels que des sites de voyage ou de tourisme, de comparaison de prix, de marques de prêt-à-porter, de sorties et événements régionaux ainsi qu'à des réseaux sociaux et à un site de magazine ».

Le licenciement est également justifié lorsque le règlement intérieur de l'entreprise proscrit certains usages personnels de la connexion Internet mise à la disposition de l'employé.

La cour d'appel d'Aix-en-Provence a ainsi validé le 13 janvier 2015 le licenciement pour faute grave d'une employée qui se connectait pendant ses heures de travail sur des sites de commerce en ligne, en violation du règlement intérieur de l'entreprise.

Pour vérifier qu'il n'y a pas d'abus dans l'utilisation d'Internet, l'employeur a le droit d'analyser les connexions de son salarié, même sans en avertir ce dernier. En effet, comme la Cour de cassation l'a rappelé le 9 juillet 2008, « les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence. »

Précision La liste des « favoris » dans le navigateur

La Cour de cassation a indiqué le 9 février 2010 que la liste des « favoris » du navigateur sur l'ordinateur d'un employé n'a pas de caractère personnel et peut être consultée par l'employeur, même en l'absence de l'employé et sans l'en avertir.

Le filtrage des accès Internet

L'employeur a le droit de filtrer les connexions Internet du salarié, en interdisant l'accès à certains types de sites et en analysant le trafic entrant.

L'interdiction d'accès à des sites peut avoir pour objectif de limiter certaines utilisations chronophages et difficilement justifiables sur le temps de travail (jeux en ligne, etc.), présentant des risques pour l'image de l'entreprise (réseaux sociaux) ou pour ses données confidentielles (sites de partage de fichiers), voire contraires aux bonnes mœurs (sites pornographiques), ou bien de protéger le système informatique contre des sites porteurs de virus et de chevaux de Troie. Cette interdiction peut figurer dans une charte d'utilisation de l'informatique, négociée avec les représentants du personnel, ou être directement implémentée dans le système : la connexion est alors physiquement impossible.

ARRÊTÉS La consultation de sites pornographiques au bureau

De nombreuses jurisprudences valident le licenciement pour faute grave de salariés utilisant les moyens informatiques de l'entreprise pour consulter de manière abusive des sites pornographiques pendant leur temps de travail. Mentionnons à titre d'exemples trois arrêts rendus par la Cour de cassation.

La Cour a ainsi validé le 10 mai 2012 le licenciement pour faute grave d'un directeur d'établissement qui « avait, au cours de l'été 2007 et jusqu'en décembre 2007, utilisé de manière répétée pendant les heures de service les ordinateurs que son employeur avait mis à sa disposition pour l'exécution de sa prestation de travail en se connectant pendant les heures de service, au vu et au su du personnel, à des sites pornographiques sur Internet ». Inversement, toujours le 10 mai 2012, la Cour a toutefois indiqué qu'un licenciement pour faute grave n'était pas justifié dans le cas d'un salarié qui, certes, consultait des sites pornographiques avec son ordinateur professionnel, mais qui n'était pas le seul à le faire : « la pratique existait dans l'entreprise même en l'absence du salarié ». Une telle tolérance de l'employeur rendait le licenciement abusif, même si la pratique était en théorie interdite par le règlement intérieur de l'entreprise.

Par ailleurs, le 8 décembre 2009, la Cour de cassation a indiqué que le fait de conserver sur son poste informatique un nombre réduit de fichiers pornographiques, dont la consultation n'affectait pas le travail de manière abusive, ne constituait pas une faute du salarié.

En conclusion, ce n'est pas simplement la consultation de sites pornographiques sur le lieu de travail qui constitue une faute justifiant le licenciement. Il y a faute si cette consultation est abusive, ou si elle concerne des sites délictueux (pédopornographie), ou si elle avait préalablement été interdite par le règlement intérieur.

L'accès de l'employeur aux fichiers et aux courriels

Dans son célèbre arrêt Nikon du 2 octobre 2001, la Cour de cassation avait énoncé que « le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des

messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. » L'employeur qui accéderait malgré tout aux courriels personnels d'un employé enfreindrait alors l'article 9 du Code civil posant le droit à la vie privée, et encourrait les peines prévues à l'article 226-15 du Code pénal réprimant les atteintes au secret des correspondances, soit un an de prison et 45 000 euros d'amende.

Néanmoins, cette position a été affinée depuis lors et, de nos jours, la justice estime de manière constante que les courriels, mais aussi les dossiers et les fichiers créés par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail, sont présumés avoir par défaut un caractère professionnel, sauf si le salarié les identifie comme étant personnels en ajoutant « personnel » ou « privé » dans leur intitulé.

La Cour de cassation a ainsi rappelé le 16 mai 2013 que « les courriels adressés et reçus par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel en sorte que l'employeur est en droit de les ouvrir hors la présence de l'intéressé, sauf si le salarié les identifie comme personnels. »

Pour les fichiers, c'est le 15 décembre 2009 que la Cour écrivait de même : « les fichiers créés par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur pour les besoins de son travail étant présumés avoir un caractère professionnel, sauf si le salarié les identifie comme étant personnels ».

Enfin, le 10 février 2015, la Cour a écrit que les SMS « envoyés ou reçus par le salarié au moyen du téléphone mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, en sorte que l'employeur est en droit de les consulter en dehors de la présence de l'intéressé, sauf s'ils sont identifiés comme étant personnels ».

L'employeur peut donc de plein droit accéder à ces documents hors de la présence du salarié et sans son accord.

ATTENTION L'accès de l'employeur aux documents professionnels du salarié est un droit

La Cour de cassation a validé le 18 octobre 2006 le licenciement pour faute grave d'un salarié qui avait crypté son poste de travail sans l'autorisation de son employeur, empêchant ainsi ce dernier d'accéder à son disque dur.

Toutefois, ce droit peut être restreint si le règlement intérieur ou la charte informatique de l'entreprise le décide. L'employeur voit alors ses droits réduits à proportion de ce qui est prévu dans ce document interne. La Cour de cassation a ainsi validé le 26 juin 2012 la condamnation d'un employeur qui avait ouvert la messagerie électronique d'un salarié en l'absence de ce dernier, alors que le règlement intérieur de l'entreprise prévoyait que les messageries électroniques des salariés ne pouvaient être consultées par la direction qu'en présence du salarié.

Attention donc à la rédaction des documents internes, ils engagent définitivement l'employeur aussi bien que les salariés.

Certes, l'employeur a ainsi un droit d'accès aux documents présumés professionnels, mais si après lecture il s'avère que le contenu de ces documents était en fait personnel, alors l'employeur ne peut pas les utiliser contre le salarié.

Le 15 décembre 2009, la Cour écrivait ainsi que, puisqu'il était confirmé que les correspondances découvertes sur l'ordinateur de l'employé en son absence « ne revêtaient pas un caractère privé, [alors seulement elles] pouvaient être retenues au soutien d'une procédure disciplinaire ».

Les salariés protégés (dont les représentants du personnel et délégués syndicaux) doivent être à l'abri d'une telle surveillance de leur employeur dans le cadre de leur mission. La

Cour de cassation a ainsi précisé le 4 avril 2012 que « pour l'accomplissement de leur mission légale et la préservation de la confidentialité qui s'y attache, les salariés protégés [...] doivent pouvoir disposer sur leur lieu de travail d'un matériel ou procédé excluant l'interception de leurs communications téléphoniques et l'identification de leurs correspondants ».

Comment intituler les éléments personnels ?

Pour bien identifier les courriels, dossiers et fichiers personnels, il est recommandé d'inscrire « personnel » ou « privé » dans leur intitulé.

JURISPRUDENCE Les dossiers « manifestement personnels »

Le 18 décembre 2012, la cour d'appel administrative de Versailles a estimé que, certes, dans le cas d'un fichier dénommé "Marc+Paul", « l'intitulé n'indique pas explicitement le caractère personnel de ce fichier », mais en l'occurrence « l'affichage en mosaïque de ce fichier révélait toutefois des photographies [pornographiques] miniatures suffisamment explicites pour que ce caractère personnel soit manifeste ». L'ouverture de ce dossier ne pouvait donc se faire sans la présence du salarié.

Bien entendu, le salarié ne doit pas abuser et ne peut pas inscrire comme personnelle la totalité de son disque dur pour empêcher l'employeur de le consulter ! La Cour de cassation a indiqué le 4 juillet 2012 que « la dénomination donnée au disque dur lui-même ne peut conférer un caractère personnel à l'intégralité des données qu'il contient » et que « la dénomination D:/données personnelles du disque dur de l'ordinateur du salarié ne pouvait lui permettre d'utiliser celui-ci à des fins purement privées et en interdire ainsi l'accès à l'employeur ».

La Cour de cassation a également précisé le 10 mai 2012 que le dossier *Mes documents*, bien connu des utilisateurs Windows, ne présentait pas par ce simple nom un caractère personnel !

La Cour a enfin estimé, le 21 octobre 2009, qu'un répertoire ayant comme intitulé les initiales du salarié n'était pas pour autant considéré comme personnel.

Le 19 juin 2013, la Cour a indiqué qu'un courriel transféré de la messagerie personnelle de l'employé vers sa messagerie professionnelle, sans être intitulé « personnel », devait être considéré comme professionnel.

L'accès de l'employeur aux documents personnels

L'employeur a toutefois un droit d'accès aux documents indiqués comme « personnels » présents sur l'ordinateur qu'il a mis à disposition de son employé, mais seulement sous certaines conditions énumérées par la Cour de cassation le 17 mai 2005 :

- soit en présence du salarié ;
- soit en son absence, mais après l'avoir fait « dûment appeler » ;
- soit en cas de « risque ou d'événement particulier ».

Les modalités permettant de « dûment appeler » le salarié et les situations de « risque ou d'événement particulier » justifiant de ne pas l'informer ou de ne pas l'appeler, devront être précisées par de futurs jugements. L'arrêt du 17 mai 2005 montre que la simple suspicion que le disque dur contenait des images pornographiques ne constituait pas un « risque ou événement particulier » permettant de se passer de la présence du salarié.

Le droit d'accès de l'employeur s'étend à tous les objets connectés au système d'information de l'entreprise, même s'ils appartiennent au salarié. Ainsi, dans le cas d'une clé USB appartenant au salarié, la Cour de cassation a énoncé le 12 février 2013 « qu'une clé USB, dès lors qu'elle est connectée à un outil informatique mis à la disposition du

salarié par l'employeur pour l'exécution du contrat de travail, étant présumée utilisée à des fins professionnelles, l'employeur peut avoir accès aux fichiers non identifiés comme personnels qu'elle contient, hors la présence du salarié ».

Cette dernière décision ouvre de dangereuses perspectives si on l'étend à tous les appareils personnels que le salarié va utiliser dans le cadre du BYOD !

Travailler chez soi ou avec son matériel ?

Les cadres n'ont pas attendu l'invention de l'informatique pour emmener du travail à la maison. Les ouvriers non plus d'ailleurs, puisque certaines régions françaises avaient d'anciennes traditions de travail à façon à domicile, dans le textile ou dans l'horlogerie, parfois comme complément hivernal à l'exploitation agricole.

L'informatique amène deux mutations à cette tradition : la possibilité de venir au bureau avec son propre portable ou son propre smartphone, et celle de travailler chez soi en se connectant à distance au réseau de l'entreprise.

Le BYOD

BYOD est le sigle de *Bring your own device* (Apportez votre propre appareil). La traduction française officielle est « Avec » (Apportez votre équipement personnel de communication). Il s'agit de la pratique consistant à utiliser dans l'entreprise ses appareils personnels (smartphone, ordinateur portable, tablette) jugés plus performants que ceux fournis par l'employeur.

Cette pratique pose notamment à l'employeur des problèmes en termes de sécurité : il ne contrôle plus les informations sus-

ceptibles de sortir de l'entreprise, il n'a plus la maîtrise du niveau de sécurité de l'équipement (chiffrement éventuel des données sur le disque dur, antivirus...) et la connexion d'un appareil inconnu au système d'information constitue une porte d'entrée pour les virus et les attaques malveillantes.

Certains points annexes doivent être précisés : par exemple, si l'employeur finance une assurance ou des licences logicielles que le salarié peut utiliser aussi à titre personnel, s'agit-il d'avantages en nature qui doivent être déclarés fiscalement ?

Le BYOD brouille également un peu plus la frontière entre la vie privée et la vie professionnelle.

La question du droit d'accès de l'employeur au matériel personnel du salarié n'a encore jamais été abordée en justice, sauf dans le cas cité plus haut de la clé USB à laquelle l'employeur a accès *tant qu'elle est connectée à un équipement de l'entreprise*. On ne sait pas dans quelles limites l'employeur peut vouloir accéder au disque dur d'un équipement appartenant au salarié, et à sa messagerie privée : sera-ce seulement pendant la connexion de cet équipement au système d'information de l'entreprise et l'accès sera-t-il limité aux dossiers identifiés comme professionnels (et comment les identifier dans ce cas ?), ou s'étendra-t-il à tout le disque dur et à toute la messagerie, y compris les activités privées et familiales ?

PRATIQUE Comment encadrer le BYOD ?

Avec le BYOD, l'employeur devient un fournisseur d'accès Internet pour ses salariés, avec les contraintes légales que cela suppose. Il convient d'encadrer de manière contractuelle les droits et obligations des salariés et ceux de l'employeur (par exemple son droit à couper le service à tout moment). Si seuls quelques salariés sont concernés, il suffit souvent de leur faire signer des conditions générales d'utilisation leur donnant le droit de se connecter au système d'information de l'entreprise. Si le BYOD concerne de nombreux salariés, un accord d'entreprise avec les partenaires sociaux devient nécessaire pour régler les différentes problématiques concernant l'aspect fiscal, la prise en charge des assurances, etc.

Notons toutefois qu'aux États-Unis, patrie d'origine du BYOD, cette pratique tend à reculer, notamment en raison des problèmes de sécurité et d'homogénéité du parc qu'elle pose aux employeurs. Ceux-ci ont alors tendance à exiger un droit de regard sur la sécurisation de l'équipement, ou sinon à interdire la connexion à leur système d'information.

LE POINT DE VUE DU SPÉCIALISTE **François Coupez, avocat à la Cour,
chargé d'enseignement à l'université Paris II**

Qu'est-ce qui explique le succès du BYOD ?

S'il est difficile d'avoir une réponse unique, on peut citer un ensemble de circonstances favorables : le fait que, dans la sphère privée, l'utilisateur ait accès à des solutions plus puissantes, plus ergonomiques et plus simples d'usage que dans la vie professionnelle, la pression des VIP et des managers qui veulent se simplifier la vie, la génération Y... Mais ne nous leurrions pas sur ce dernier point, la principale demande provient bien du *top management*. Rappelons quand même qu'il n'existe pas de droit au BYOD : l'employeur peut toujours refuser cette pratique.

Quels en sont les principaux inconvénients ?

Certaines entreprises croient encore qu'autoriser le BYOD leur permettra de faire des économies, notamment en matériel, en abonnement, en licences... Le coût doit en réalité être appréhendé de façon bien plus globale car si le BYOD nécessite peut-être moins de formation, il ne faut pas écarter le coût des assurances, des infrastructures d'accueil à mettre en place ou encore de la sécurité. Surtout, la mise en place de telles pratiques n'évite pas de devoir acheter aussi les outils professionnels du salarié (ordinateur, tablette, etc.) si celui-ci décidait d'arrêter d'utiliser les siens dans l'entreprise. Sous-estimer le coût de la mise en place du BYOD constitue le principal risque pour les entreprises. Sans oublier la perte de contrôle éventuelle des connexions à son système, qui peut avoir pour conséquences des fuites d'informations, des intrusions malveillantes, la contamination du réseau interne par des malwares, etc.

Sur qui le risque pèse-t-il ?

Les risques pèsent sur l'employeur. Rappelons en effet que l'employeur est responsable envers tous de la sécurité de son système d'information et des données qu'il contient, sous peine de sanctions pénales le plus souvent (dans le cas de données à caractère personnel par exemple). Il est responsable également des actions commises par ses salariés dans le cadre professionnel. Quant au salarié, il sous-estime souvent les implications du BYOD en termes de surveillance par l'employeur de son appareil personnel et des données privées qu'il contient. Car un appareil connecté au système d'information de l'entreprise est présumé professionnel, ainsi que l'ensemble de son contenu.

Le droit est-il adapté ?

Il n'existe pas de loi spécifique au BYOD et c'est sans doute mieux ainsi, car les principes généraux de la loi Informatique et Libertés et du Code du travail, ou ceux dégagés par la jurisprudence sur la surveillance par l'employeur, son droit d'accès aux fichiers des salariés... s'appliquent pleinement. La jurisprudence a évolué depuis l'arrêt Nikon de 2001 et va continuer à se construire : les juges ont prouvé qu'ils savent s'adapter.

Quelles solutions techniques conseiller ?

Dans l'idéal, il convient de privilégier des outils intégrant la *privacy by design*, qui compartimentent les données dans le BYOD : il y a d'un côté les courriels et fichiers personnels, de l'autre les documents professionnels. Toutefois, les utilisateurs recherchent souvent au contraire la fusion des deux, l'effacement des barrières.

L'employeur peut, comme alternative, proposer un catalogue d'outils mobiles qu'il a testés et dont il maîtrise la sécurité. On revient alors aux traditionnels portables et smartphones fournis par l'employeur et dont un usage personnel limité est toléré.

Que conseillez-vous pour la mise en œuvre du BYOD dans une organisation ?

L'employeur doit bien mesurer toutes les conséquences du BYOD : le dimensionnement de ses infrastructures (nombre de bornes Wi-Fi par exemple), les assurances à souscrire, l'aspect fiscal, le droit du travail, la sécurité, le respect des données personnelles... Il doit être d'air vis-à-vis des salariés sur les solutions techniques mises en œuvre : peut-il effacer à distance les données (y compris privées) en cas de vol de l'outil ? Y a-t-il archivage automatique sur serveur des données du disque dur ? Si oui, comment les données privées sont-elles distinguées des données professionnelles ? Si le salarié part de l'entreprise, que deviennent les données privées archivées chez l'employeur et les données professionnelles enregistrées sur le disque dur du BYOD ?

Quelles sont les perspectives ?

Au-delà du BYOD, on constate maintenant l'apparition d'une tendance à vouloir intégrer dans l'entreprise l'usage des comptes et identifiants du salarié sur les réseaux sociaux : connexion par Facebook Connect, usage du compte Twitter ou Google+ du salarié pour le compte de l'entreprise...

Néanmoins, que se passera-t-il si le salarié quitte l'entreprise ? Est-il propriétaire des *followers* de son compte Twitter ? À partir de quand ce compte devient-il « professionnel » ? De nouveaux débats pour les années à venir...

Le télétravail

Le pendant du BYOD est le télétravail : le salarié ne travaille plus au bureau à horaires fixes, mais n'importe où et n'importe quand, avec du matériel fourni par l'entreprise ou avec son propre équipement. Dans ce cas, on peut se demander si les critères permettant de juger comme abusif un accès personnel à Internet « pendant les horaires de bureau » a encore un sens : un salarié peut très bien effectuer ses accès privés à Internet pendant la journée, aux heures ouvrables, et préférer travailler pour son employeur pendant la nuit !

Le télétravail a fait l'objet d'un accord cadre européen du 16 juillet 2002 signé par tous les partenaires sociaux européens, transposé en France par l'accord national interprofessionnel du 17 juillet 2005. Il contribue à préserver l'environnement par la diminution des déplacements quotidiens, à trouver un meilleur équilibre entre vie familiale et vie professionnelle, mais aussi une nouvelle conception des rapports hiérarchiques qui, par la distance, sont rééquilibrés vers plus de délégation et moins de présentéisme.

Le télétravail est défini par l'article L1222-9 du Code du travail comme « toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon régulière et volontaire en utilisant les

technologies de l'information et de la communication dans le cadre d'un contrat de travail ou d'un avenant à celui-ci ». Contrairement au nomadisme informatique occasionnel, le télétravail doit donc être *régulier* et *contractualisé*.

Le Code précise que le télétravail doit résulter d'un accord du salarié : ce dernier doit être volontaire et « le refus d'accepter un poste de télétravailleur n'est pas un motif de rupture du contrat de travail ». Par ailleurs, le contrat de travail doit préciser les conditions de passage en télétravail et prévoir les conditions de retour à une exécution classique du contrat.

JURISPRUDENCE L'employeur ne peut pas imposer la cessation du télétravail

Le 13 février 2013, la Cour de cassation a indiqué que « lorsque les parties sont convenues d'une exécution de tout ou partie de la prestation de travail par le salarié à son domicile, l'employeur ne peut modifier cette organisation contractuelle du travail sans l'accord du salarié. » Il est donc primordial de prévoir dans le contrat de travail les conditions de cessation de cette modalité d'exécution du travail.

L'article L1222-10 du Code du travail prévoit en outre que l'employeur est tenu :

1. « de prendre en charge tous les coûts découlant directement de l'exercice du télétravail, notamment le coût des matériels, logiciels, abonnements, communications et outils, ainsi que de la maintenance de ceux-ci ;
2. d'informer le salarié de toute restriction à l'usage d'équipements ou outils informatiques ou de services de communication électronique et des sanctions en cas de non-respect de telles restrictions ;
3. de lui donner priorité pour occuper ou reprendre un poste sans télétravail qui correspond à ses qualifications et compétences professionnelles et de porter à sa connaissance la disponibilité de tout poste de cette nature ;

4. d'organiser chaque année un entretien qui porte notamment sur les conditions d'activité du salarié et sa charge de travail ;
5. de fixer, en concertation avec lui, les plages horaires durant lesquelles il peut habituellement le contacter. »

Des accords encadrant le télétravail ont été négociés entre la direction et les représentants du personnel dans de nombreuses grandes entreprises françaises, dont près de la moitié des entreprises du CAC 40 : Atos, Air France, Alcatel, Axa, Accenture, Areva, Alstom, Bouygues Telecom, Caisse des dépôts, Canal Plus, CapGemini, L'Oréal, La Poste, Michelin, Orange, Renault, Schneider, SFR... Il est difficile d'évaluer le nombre réel de télétravailleurs en France : s'il y a au total peu de contrats formellement signés, de nombreux cadres pratiquent le télétravail de manière informelle ou sporadique. On peut estimer que 10 à 15 % de la population active est concernée.

Le fait de télétravailler ne doit pas conduire à ne pas respecter les limites horaires prévues par le Code du travail, même pour les cadres soumis au forfait jour, qui ne pointent pas. Le repos quotidien d'une durée minimale de onze heures, ainsi que le repos hebdomadaire d'une durée minimale de 35 heures, doivent être assurés. La Cour de cassation a donc exigé le 24 avril 2013 des employeurs de s'assurer du respect de ces dispositions, et de mettre en place une obligation de déconnexion pour les salariés se connectant à distance. La convention Syntec a été modifiée en ce sens en 2014.

Comment parler de son employeur sur les réseaux sociaux ?

Un salarié qui s'épanche sur Internet au sujet de ses conditions de travail risque aussi bien de diffamer son employeur s'il en dit du mal, que de révéler par inadvertance (ou par malveil-

lance d'ailleurs) des informations confidentielles. Il risque alors le licenciement.

Diffamation publique de l'employeur

De nombreux litiges ont opposé des entreprises à certains de leurs salariés qui avaient publié sur Facebook des propos ressentis par leur employeur comme diffamatoires. À chaque fois, les salariés, licenciés, ont contesté leur licenciement.

Le 19 novembre 2010, le conseil des prud'hommes de Boulogne-Billancourt a validé le licenciement de trois salariés qui avaient dénigré leur hiérarchie sur Facebook. Le mur sur lequel les propos en cause étaient affichés était accessible aux amis d'amis, ce qui a été considéré comme un espace public par les prud'hommes. La critique publique de son employeur constitue une faute grave.

Une des salariées a fait appel : la cour d'appel de Versailles, dans son arrêt du 22 février 2012, a estimé le licenciement sans cause réelle et sérieuse. Toutefois, pour se prononcer ainsi, la cour n'a pas procédé à une analyse approfondie du dossier, mais s'est simplement basée sur un point de principe : en effet, avant de licencier la salariée, son employeur lui avait infligé une première sanction sous forme de mise à pied, or on ne peut sanctionner quelqu'un deux fois pour les mêmes faits.

Le 15 novembre 2011, la cour d'appel de Besançon, saisie d'un litige similaire, a estimé que Facebook, « par application du principe "*les contacts de mes contacts deviennent mes contacts*"[...] doit être nécessairement considéré, au regard de sa finalité [de réseau social] et de son organisation, comme un espace public », sauf à prendre des précautions particulières dans le paramétrage de son compte et à s'assurer que ses amis en ont fait autant. Or, « si le salarié jouit, dans l'entreprise ou en dehors d'elle, de sa liberté d'expression [...], il ne peut

abuser de cette liberté par des propos injurieux, diffamatoires ou excessifs ».

Toutefois, la cour d'appel de Rouen a adopté le même jour une position inverse : selon elle, « il ne peut être affirmé de manière absolue que la jurisprudence actuelle nie à Facebook le caractère d'espace privé, alors que ce réseau peut constituer soit un espace privé, soit un espace public, en fonction des paramétrages effectués par son utilisateur. » Saisie, elle aussi, d'un litige similaire, elle a estimé qu'il revenait à l'employeur de prouver que les paramétrages des comptes Facebook en cause en faisaient des espaces publics. En l'absence de cette preuve, elle a déclaré le licenciement sans cause réelle et sérieuse.

Il faut noter une dernière décision dans ce sens : la cour d'appel de Douai a estimé le 16 décembre 2011 qu'un licenciement pour diffamation sur Facebook était abusif. Elle a jugé que les propos en cause ne constituaient pas une faute grave.

CONCLUSION Facebook, espace public ou privé ?

On constate que, dans des dossiers similaires, la jurisprudence varie d'une cour d'appel à l'autre. On ne peut donc pas trancher de manière définitive sur le caractère public ou privé des propos publiés sur Facebook, ni sur un éventuel « droit à se plaindre de son employeur sur Facebook ». Dans une telle incertitude, il vaut mieux être prudent et éviter tout propos négatif sur un support susceptible d'être consulté par d'autres personnes que son interlocuteur.

Rappelons que la confidentialité d'une communication électronique (courriel) non chiffrée est équivalente à celle d'une carte postale et que toute publication sur une page personnelle, un réseau social, un forum ou un blog est aussi confidentielle qu'un panneau publicitaire au coin de la rue.

La sanction d'une diffamation publique de son employeur ne résulte pas toujours d'une décision de justice. Ainsi, en mai 2014, aux États-Unis, le directeur de la stratégie de

PayPal a été licencié, pour avoir émis des tweets injurieux pour la vice-présidente du groupe. En France, ce sont des journalistes et animateurs de télé qui ont ainsi été licenciés pour des tweets sexistes ou mettant en cause leur employeur : Pierre Salviac par RTL en 2012, Julien Courbet par France 2 en 2013.

QUESTION Quel droit de regard pour l'employeur sur les tweets personnels ?

S'il est compréhensible que l'employeur puisse se plaindre d'un dénigrement publié par son salarié aussi bien sur Twitter que sur Facebook, la question se pose de savoir si l'employeur peut sanctionner le salarié même sans être la cible des tweets litigieux ? Par exemple en cas de tweets racistes, publiés par le salarié dans un cadre strictement personnel ? La tendance est de considérer que les propos du salarié ne doivent pas porter atteinte à l'image de l'employeur, au sens large. Ainsi, en 2011, le créateur de mode John Galliano, condamné à 6 000 euros d'amende avec sursis pour injures racistes et antisémites, a été licencié par son employeur Dior qui ne voulait pas avoir l'air de cautionner ses propos.

Divulgaration d'informations confidentielles

Les salariés sont en général tenus au respect de règles de confidentialité en ce qui concerne les informations relatives à leur employeur. Le contrat de travail peut également prévoir une clause spécifique de confidentialité. De manière générale, la violation du secret professionnel est également sanctionnée par l'article 226-13 du Code pénal, qui punit au maximum d'un an de prison et de 15 000 euros d'amende « la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire ».

Il est régulièrement question de pénaliser plus lourdement la violation du secret des affaires. En 2012, le député Carayon avait ainsi proposé de créer une infraction de « violation du

secret des affaires », passible d'une sanction de trois ans de prison et de 375 000 euros d'amende. Ces dispositions ont été reprises début 2015 dans le projet de loi Macron. Toutefois, les contestations contre ce texte, accusé d'entraver par exemple les enquêtes journalistiques ou l'action syndicale, ont conduit au retrait de ces articles.

ANISPRUDENCE **Condamnation pour violation du contrat de travail**

Le tribunal de grande instance de Béthune a condamné le 14 décembre 2010 un salarié qui avait dévoilé sur son blog des informations confidentielles sur son employeur, « concernant les aspects commerciaux de son activité, le côté technique de ses prestations et la gestion des ressources humaines de l'entreprise », en violation de son contrat de travail qui prévoyait une obligation de secret professionnel renforcée, à un euro de dommages et intérêts, mais aussi à la suppression des textes litigieux sur Internet et à la publication, aux frais du condamné et dans la limite de 10 000 € hors taxes, de la condamnation dans quatre revues ou magazines, ainsi que sur le blog personnel du condamné pendant six mois. Le condamné a également dû rembourser à la société les frais de justice.

La cybercriminalité

La notion de cybercriminalité englobe à la fois les atteintes perpétrées à l'encontre des systèmes informatiques et les formes traditionnelles de délinquance, qui utilisent Internet comme vecteur ou comme moyen d'expansion. Quelles sont les limites du droit de l'internaute à rechercher ou à profiter des failles de sécurité, même pour s'amuser ? Quelles sont ses protections s'il est victime d'une attaque ?

Les attaques contre les systèmes informatiques

La protection des systèmes informatiques contre les attaques pirates, tant externes qu'internes, a fait l'objet de la loi Godfrain du 5 janvier 1988, qui avait inséré dans l'ancien Code pénal des articles consacrés à la répression « de certaines infractions en matière informatique ».

Historique La loi Godfrain (1988)

Dans les années 1980, l'augmentation du nombre des fraudes informatiques a attiré l'attention du législateur. Le droit pénal de l'époque n'était pas du tout adapté à ces nouvelles formes de délinquance. En conséquence, pour une répression pénale plus efficace des atteintes aux systèmes informatiques, le député Jacques Godfrain proposa en 1988 une loi qui instituait les délits d'accès et de maintien frauduleux dans un système, d'entrave au fonctionnement d'un système, d'action frauduleuse sur les données, de falsification de document informatisé, d'usage de documents falsifiés et enfin d'association de malfaiteurs informatiques.

Ces articles ont été modifiés lors des refontes successives du Code pénal et en constituent désormais les articles 323-1 et suivants. Ils répriment d'une part l'accès et le maintien frauduleux dans un système de traitement automatisé de données (STAD), avec une aggravation de peine s'il en est résulté une suppression ou modification de données ou une altération du fonctionnement, d'autre part l'entrave au fonctionnement du STAD et enfin l'introduction, la modification, l'extraction ou la suppression frauduleuse de données. Ils répriment également la simple détention ou la diffusion de moyens de piratage : logiciels spécialisés, virus, etc.

Ces articles sont évidemment applicables pour toute attaque contre un site web, qu'il s'agisse d'une intrusion dans ses bases de données (« accès frauduleux à un système »), d'une attaque en déni de service (« entrave au fonctionnement »), d'une modification pirate (« modification frauduleuse »). En effet, la loi ne définit pas précisément ce qu'est un « système de traitement automatisé de données », mais cette ouverture autorise une application très large de ces articles.

Accès ou maintien frauduleux dans un STAD

L'accès ou le maintien frauduleux dans un STAD constitue souvent la première action d'un pirate pour s'emparer de bases

de données personnelles : bases de mots de passe, de numéros de cartes bancaires, d'informations sur l'identité des personnes... Si l'on est victime de ce type d'agression, on peut porter plainte sur la base de l'article 323-1 du Code pénal.

La loi L'article 323-1 du Code pénal

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende. »

Pour un système informatique ou un site web, l'accès doit s'entendre comme l'exécution de manœuvres afin de pénétrer dans le fonctionnement du système ou d'accéder aux données. La simple utilisation de l'ordinateur et de l'abonnement Internet d'autrui a été qualifiée d'accès frauduleux : ainsi, le 24 mai 2006, le chef de l'équipe de nettoyage de la cour d'appel de Montpellier a été reconnu par cette même cour coupable d'accès frauduleux dans un STAD pour avoir utilisé les ordinateurs de la cour d'appel (!) pendant ses horaires de travail pour se connecter à des sites web à caractère pornographique. Le STAD pouvant également être constitué d'un réseau d'informatique ou de télécommunications, une écoute passive peut elle aussi être considérée comme un accès, qu'elle soit réalisée par espionnage des artères de transmission ou par captation des signaux parasites émis par le circuit électrique.

Quant au « maintien », il a été jugé qu'il peut succéder à un accès licite : la cour d'appel de Paris a ainsi indiqué le

5 avril 1994 que même si « l'accès a été régulier, le maintien sur un STAD peut devenir frauduleux [...], que l'accès ou le maintien irrégulier suppose que leur auteur n'a pas respecté la "règle du jeu", que celle-ci procède de la loi, du contrat ou de la volonté du "maître du système" ». Cela interdit donc, après un accès autorisé, de se maintenir abusivement connecté.

Pour le juge pénal, l'élément intentionnel est primordial : la fraude est constituée dès que le délinquant a conscience que l'accès n'est pas autorisé et qu'il agit contre le gré du maître du système, même s'il n'y a pas de sécurisation, et à plus forte raison s'il y en a une. Le mobile (qui peut être désintéressé) n'est pas pris en compte, comme le montreront les jurisprudences.

L'éventuelle modification des données, suite à l'accès frauduleux, constitue une circonstance aggravante de l'infraction.

Le dernier alinéa de l'article 323-1 concernant les traitements de données personnelles mis en œuvre par l'État a été ajouté en 2012 dans le cadre de la loi sur la protection de l'identité : cette loi prévoyait de créer une base des empreintes digitales des porteurs de cartes d'identité et de passeports. Afin de dissuader toute tentative d'attaque externe, mais aussi interne, contre cette base d'empreintes, le législateur avait décidé d'alourdir les sanctions en cas d'accès frauduleux aux traitements de données personnelles de l'État. En mars 2012, le Conseil constitutionnel a finalement déclaré cette base d'empreintes non conforme à la Constitution. Cette base n'a donc pas vu le jour, mais les dispositions réprimant plus sévèrement les atteintes aux systèmes de l'État sont restées.

Condamnation des accès frauduleux, même à des fins ludiques ou de test

L'accès non autorisé est pénalement condamnable, même s'il n'y a pas intention de nuire et même s'il n'y a eu aucune conséquence dommageable pour le système.

La cour d'appel de Paris a ainsi condamné le 15 mai 2001 un prévenu qui avait pénétré dans le système informatique d'une

université grâce à un logiciel de piratage, sans provoquer aucune modification des données ni aucune altération du système. De même, le tribunal de grande instance de Vannes a condamné le 13 juillet 2005 quatre étudiants qui avaient utilisé des logiciels de piratage des mots de passe pour accéder aux comptes d'autres utilisateurs du réseau de leur université. Les prévenus ont été condamnés à 1 000 euros d'amende avec sursis chacun.

Un expert en sécurité qui « teste » la sécurité d'un site web est lui aussi passible de cet article 323-1. C'est pourquoi, lorsqu'une société lance un audit sur ses systèmes, elle doit donner aux auditeurs une autorisation écrite de chercher à contourner ses dispositifs de sécurité.

Condamnation des accès frauduleux à des fins répréhensibles

Contrairement aux exemples précédents, de nombreux accès frauduleux à des sites web sont commis à des fins répréhensibles. Un motif fréquent est d'accéder à des données personnelles ou à des informations confidentielles, exploitables dans un but économique ou de nuisance. Les condamnations se multiplient et confirment le spectre très large de cette incrimination, ce qui la rend très utile dans la répression de nombreuses fraudes informatiques. Le recours à l'article 323-1 permet par exemple une répression efficace du vol d'information, voire de l'espionnage économique.

L'utilisation d'un identifiant et d'un mot de passe obtenus régulièrement, pour continuer à accéder à un système d'information alors que l'on n'est plus censé en avoir le droit, constitue aussi un accès frauduleux à un système. Un ancien employé d'une agence de presse a ainsi été condamné par la cour d'appel de Paris le 27 mars 2002, pour avoir à plusieurs reprises accédé par Internet aux bases de données de son ancien employeur après son départ, en continuant à utiliser

son identifiant et son mot de passe qui étaient toujours valables. La condamnation à une amende de 762 euros a été confirmée, plus 1 franc symbolique de dommages-intérêts.

L'utilisation de logiciels espions pour récupérer des codes secrets et l'utilisation des codes secrets d'autrui constituent également des accès et des maintiens frauduleux à un système. Le 29 juin 2005, la cour d'appel de Versailles a confirmé la condamnation à quatre mois de prison avec sursis et 120 h de travaux d'intérêt général, d'un employé qui avait utilisé des logiciels espions pour récupérer les codes bancaires de ses collègues.

Dans le même sens, le 1^{er} juin 2007, un ancien consultant d'une société financière a été condamné par le tribunal de grande instance de Paris pour accès frauduleux à un STAD et atteinte au secret des correspondances, pour avoir utilisé de manière répétée les codes secrets des membres de la direction de l'entreprise afin d'accéder à leur messagerie pour espionner leurs courriels. Le tribunal a souligné que « l'utilisation d'un code d'accès à une messagerie par un ancien salarié constitue bien une manœuvre, l'intéressé ayant parfaitement conscience qu'il n'a plus le droit d'utiliser ce code et qu'il ne fait plus partie de la liste des personnes autorisées. » Le prévenu a été condamné à six mois d'emprisonnement avec sursis, plus 5 000 euros de dommages-intérêts à payer à l'entreprise et 1 000 euros à chacun des directeurs concernés.

Enfin, le 21 février 2008, l'administrateur réseau d'une société, qui avait installé dans le serveur dont il avait la charge des logiciels espions afin de capturer les mots de passe des membres de la direction, et qui avait utilisé ces mots de passe pour accéder à des informations confidentielles, a été déclaré par le tribunal de grande instance de Rennes coupable de modification frauduleuse et d'accès frauduleux à un STAD, et condamné à six mois d'emprisonnement avec sursis et à 1 500 euros d'amende.

Condamnation pour copie d'un site web

Le fait de recopier en totalité le site web d'une société tierce, dans le but notamment de disposer des bases de données de cette société, a également été qualifié d'accès et de maintien frauduleux à un système. En l'espèce, le gérant d'une société, qui avait « aspiré » le site des éditions d'annonces immobilières Neressis (« De particulier à particulier »), y compris la partie confidentielle du site contenant les bases de données de la société et les coordonnées personnelles des annonceurs, a été reconnu coupable par le tribunal de grande instance de Paris d'accès et de maintien frauduleux à un STAD, et de collecte déloyale de données nominatives. Il a été condamné le 18 septembre 2008 à une amende de 5 000 euros avec sursis.

La société dirigée par cette personne a été reconnue coupable des mêmes faits et condamnée à une amende de 15 000 euros, plus 50 000 euros de dommages-intérêts et 3 000 euros de frais de justice. Une société dont les gérants commettent une infraction dans le cadre de leur activité peut ainsi être condamnée à une amende beaucoup plus élevée que celle qui sanctionne ses dirigeants.

L'article 323-6 du Code pénal

En effet, l'article 323-6 du Code pénal prévoit de condamner les sociétés pour les infractions commises par leurs dirigeants :

« Les personnes morales peuvent être déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre.

Les peines encourues par les personnes morales sont :

- 1^o L'amende, suivant les modalités prévues par l'article 131-38 ^a ;
- 2^o Les peines mentionnées à l'article 131-39 ^b.

L'interdiction mentionnée au 2^o de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. »

a. « Le taux maximum de l'amende applicable aux personnes morales est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction. »

b. Ces peines consistent en des interdictions diverses, surveillance judiciaire, confiscation de la chose qui a servi à commettre l'infraction, diffusion publique de la décision...

L'accès à un système non sécurisé

Un accès à un site web peut-il être qualifié de frauduleux si ce site n'est pas sécurisé et se retrouve librement accessible ? La fraude se matérialise-t-elle obligatoirement par le piratage d'une protection ?

Ces questions ont été débattues dans le cadre de l'affaire *Kitetoo*, qui opposa en 2002 la société Tati à Antoine C. (voir la section sur les jurisprudences, à la fin du chapitre 2). Ce journaliste informatique avait trouvé sur le site Internet de Tati des fichiers de données personnelles de clients librement accessibles. La particularité de cette affaire résidait justement dans le manque de sécurisation du site web : les fichiers étaient accessibles avec un simple navigateur grand public.

Comme l'explique le tribunal de grande instance de Paris, « l'ensemble du contenu du serveur s'affichait sous forme d'arborescence ; en consultant les liens HTML, il [le journaliste] avait trouvé notamment le listing de clients [...], fichier de type .mdb dans lequel la société Tati enregistrait le résultat de questionnaires posés aux internautes, dans lequel apparaissaient les noms, adresses et autres données personnelles des visiteurs du site ayant bien voulu répondre à des questions personnelles, fichier qui comportait selon lui environ 4 000 entrées. »

Peut-être suite à la parution d'un article dans la revue *Newbiz* de novembre 2000 révélant au grand public la perméabilité de son site, Tati porta plainte contre Antoine C. sur la base de l'article 323-1 du Code pénal.

Condamné dans un premier temps le 13 février 2002 pour accès frauduleux à un système de traitement automatisé de données, Antoine C. fut finalement déclaré non coupable en appel.

À RETENIR Que conclure ?

Il convient de relever que l'article 323-1 du Code pénal, sur lequel la plainte était basée, n'exige pourtant pas que le système soit protégé par une sécurisation. Lors de l'élaboration de ce texte, les parlementaires avaient débattu de ce point et c'est en toute connaissance de cause que l'exigence de sécurisation du système avait été écartée.

Peut-être ce résultat est-il dû au fait que l'affaire Kitetoa concerne un site web. En effet, lorsqu'un litige concerne un accès potentiellement frauduleux à un STAD qui n'est pas un site web, par exemple le réseau interne, le système d'information ou l'intranet d'une organisation, le prévenu peut difficilement plaider la bonne foi, car il ne dispose pas d'une raison valable pour justifier sa connexion. Dans l'affaire Kitetoa, les pages qui auraient dû rester confidentielles étaient librement accessibles sur le site web externe de la société Tati, le grand public pouvait s'y connecter par hasard et en toute bonne foi, sans que l'internaute ait conscience du caractère confidentiel des informations. Or, le Code pénal (article 121-3) pose comme principe qu'« il n'y a point de crime ou de délit sans intention de le commettre ». L'important n'est donc pas la présence ou l'absence d'un dispositif de sécurité : pour que l'accès soit considéré comme frauduleux, la personne qui accède au système doit avoir conscience de le faire sans autorisation, et le responsable du système doit avoir, sinon sécurisé, du moins fait savoir que l'accès à certaines données était interdit. Ce qui n'était pas le cas dans ce dossier.

Dans le même sens, le tribunal de grande instance de Créteil a estimé le 23 avril 2013 qu'un internaute, qui avait téléchargé des documents internes sur le site d'une agence officielle, avait pu légitimement penser que ces données étaient en libre accès puisque, du fait d'une défaillance technique, la protection par mot de passe était inopérante et aucun message n'indiquait le caractère confidentiel des documents. L'accès à ces données ne pouvait donc être considéré comme frauduleux. Mais le 5 février 2014, la cour d'appel de Paris infirma ce jugement et, le prévenu ayant reconnu avoir constaté la présence d'un contrôle d'accès, même inopérant, elle considéra qu'il avait conscience du caractère illicite de son maintien dans le système. Il fut condamné à 3 000 euros d'amende. L'affaire est désormais devant la Cour de cassation.

La fraude scolaire

Les infractions décrites ci-dessus peuvent servir à des étudiants pour frauder dans le cadre scolaire et universitaire. Aux sanctions pénales s'ajouteront donc éventuellement les sanctions disciplinaires (renvoi, interdiction de passer un examen, etc.).

En avril 2012, un étudiant de l'université Paris II Melun a été condamné à six mois de prison avec sursis, 3 000 euros d'amende et cinq ans d'interdiction d'exercer dans la fonction publique, pour avoir, en profitant de l'absence d'une secrétaire, accédé au système informatique de l'université afin de modifier ses notes et celles de sa petite amie (condamnation confirmée en appel en 2014).

En 2010, une étudiante en master à l'université Rennes II avait été exclue de toute université pour cinq ans, pour avoir, en profitant de son statut de vacataire, dérobé des codes lui permettant de modifier ses notes pour devenir major de sa promotion.

En 2009, un étudiant de l'École supérieure de commerce d'Amiens a piraté le code du responsable des examens pour accéder aux sujets.

Entrave au fonctionnement d'un STAD

Les atteintes au fonctionnement d'un système sont réprimées par l'article 323-2 du Code pénal.

L'article 323-2 du Code pénal

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »

Le terme d'entrave n'a pas de signification spécifique en informatique. On peut évoquer parmi les entraves le fait de bloquer totalement le fonctionnement du système, ou celui de causer un ralentissement : par exemple, suite à un envoi de spam massif. Les attaques de sites web par déni de service (DDOS, *Distributed Denial Of Service*, consistant à lancer simultanément, depuis des milliers d'ordinateurs, des tentatives de connexion à un même site web pour saturer ce dernier) sont particulièrement visées par cet article.

Le terme « fausser » n'a pas non plus de définition précise ; il peut évoquer toute modification du fonctionnement du système, non souhaitée par son responsable. Le « fonctionnement » ici visé est plus large que le seul « traitement » des données. Les jurisprudences qui suivent montrent, par exemple, que le code d'accès à un traitement fait partie de son fonctionnement.

Cet article sert à réprimer les atteintes intentionnelles au fonctionnement d'un STAD, que l'accès soit frauduleux ou légitime : il réprime l'intention de nuire. Toutefois, on peut noter que certains cas d'entrave involontaire ont aussi été condamnés sur cette base.

Comme pour l'article 323-1, le dernier alinéa a été ajouté en 2012.

Condamnations pour entrave volontaire

La cour d'appel de Paris a condamné le 5 octobre 1994 le directeur technique d'une société informatique, co-auteur d'un logiciel, qui pour nuire à son associé avait bloqué le système en effaçant le programme de clé d'accès au logiciel.

Le 23 janvier 2006, un informaticien qui avait supprimé frauduleusement des données du système dont il avait la gestion, et qui avait également détruit les copies de sauvegarde, a également été condamné par la cour d'appel d'Aix-en-Provence

pour entrave au fonctionnement d'un STAD. Il a dû payer 3 000 euros de dommages et intérêts à la société victime.

Dans ces deux dossiers, l'entrave était bien intentionnelle. Dans ces deux cas également, il ne s'agissait pas d'un piratage d'origine externe et l'auteur des faits appartenait à l'entreprise. De manière générale, en sécurité informatique, il apparaît d'ailleurs que la majorité des attaques est d'origine interne. Cela n'exclut pas la possibilité qu'une attaque externe puisse également être sanctionnée grâce au même article 323-2.

Condamnations pour entrave involontaire

L'article 323-2 a également été invoqué pour réprimer des entraves non intentionnelles au fonctionnement d'un système, mais ne résultant pas d'un accès frauduleux, ce qui interdisait d'invoquer l'article 323-1. Le 5 avril 1994, à l'époque du Minitel, la cour d'appel de Paris a ainsi jugé le cas de prévenus qui avaient saturé automatiquement des minitels roses avec des messages de publicité pour des services concurrents. Ce « racolage » avait évidemment entraîné une perturbation des messageries en question. Les prestataires des services attaqués avaient dû mettre en place des filtres qui, avançaient-ils, consommaient 30 % des ressources de leurs systèmes. Ils avaient donc porté plainte sur la base du maintien frauduleux dans un STAD et de l'entrave au fonctionnement d'un système. La cour avait écarté l'accès frauduleux (connexion normale par le 3615 ouvert au public), mais avait retenu le maintien frauduleux et l'entrave au fonctionnement.

Autre jurisprudence, le 30 mars 2005, une personne ayant procédé à des envois massifs de messages vers les forums de discussion d'un grand magasin et invitant les autres internautes à envoyer à leur tour des messages en forme de pétition, a été condamnée par la cour d'appel de Paris pour entrave au fonctionnement d'un STAD.

Enfin, la cour d'appel d'Aix-en-Provence a jugé le 22 septembre 2004 un prévenu qui avait utilisé un logiciel d'interrogation automatique de fichier pour recopier un annuaire en multipliant les consultations. La cour a estimé qu'il s'agissait d'une collecte frauduleuse, déloyale ou illicite de données personnelles (article 226-18 du Code pénal). En outre, cette multiplication des consultations avait saturé l'annuaire, entravant donc son bon fonctionnement, ce qui constituait le délit d'entrave au fonctionnement d'un système (article 323-2 du Code pénal). Le prévenu a été condamné.

Modification frauduleuse des données d'un STAD

Après avoir accédé à un STAD, un pirate peut soit récupérer les données qu'il contient, soit en entraver le fonctionnement, soit procéder à une modification frauduleuse des données. Cette dernière infraction est prévue par l'article 323-3 du Code pénal.

L'article 323-3 du Code pénal

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 100 000 € d'amende. »

La Cour de cassation a précisé le 8 décembre 1999 que « le seul fait de modifier ou supprimer, en violation de la réglementation en vigueur, des données contenues dans un système de traitement automatisé caractérise le délit prévu à l'article 323-3 du Code pénal, sans qu'il soit nécessaire que ces modifications ou suppressions émanent d'une personne

n'ayant pas un droit d'accès au système ni que leur auteur soit animé de la volonté de nuire. »

Comme pour les articles 323-1 et 323-2, le dernier alinéa a été ajouté en 2012.

Condamnations pour attaques informatiques

Un prévenu a été condamné par le tribunal de grande instance de Nanterre le 10 février 2006 à une amende de 1 500 euros avec sursis et à 1 euro de dommages et intérêts, pour accès frauduleux à un STAD entraînant une modification des données (article 323-1), accès frauduleux à un STAD entraînant une suppression des données (article 323-1) et modification frauduleuse de données (article 323-3).

Cas plus frappant, un informaticien avait en 2002 compromis un serveur d'un opérateur de télécommunications et s'en était servi pour scanner les vulnérabilités de 394 serveurs gouvernementaux et de 63 autres serveurs publics ou privés. Sur les serveurs comportant des failles de sécurité, il avait affiché un message d'alerte. Le « but » affiché de l'attaque était donc, non pas la nuisance, mais la pédagogie ou la recherche de notoriété. Le prévenu avait été reconnu par le tribunal de grande instance de Paris coupable d'accès frauduleux dans un STAD, entrave au fonctionnement d'un STAD, introduction frauduleuse de données (articles 323-1, 323-2, 323-3 du Code pénal) et avait été condamné le 2 juin 2006 à quatre mois d'emprisonnement avec sursis et à 1 000 euros de dommages-intérêts pour chaque partie civile.

La répression de la fraude informatique organisée

Le piratage informatique n'est plus le fait de petits génies cassant des mots de passe derrière leur écran ; il est devenu une véritable industrie, avec des spécialistes pour chaque tâche et

un marché sur lequel s'achètent et se vendent les compétences, les outils et les données volées. Ainsi, certains réalisent et vendent les logiciels de piratage (malwares) clés en main à ceux qui vont lancer des attaques, dont les produits (numéros de cartes bancaires, par exemple) seront revendus à des spécialistes de l'escroquerie, qui eux-mêmes auront recours à des officines de blanchiment pour transférer le produit de leur activité.

Prenant acte de l'implication grandissante du milieu du crime organisé dans le secteur de la fraude informatique et de la transformation du piratage en une véritable industrie d'ampleur internationale, le législateur a créé, à l'occasion de la loi de 2004 pour la confiance dans l'économie numérique, deux nouveaux articles du Code pénal consacrés à la répression du *hacking* en tant que crime organisé.

Le trafic de logiciels conçus pour le piratage est désormais réprimé par l'article 323-3-1 du Code pénal, qui dispose que « le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

L'appartenance à une « bande organisée » est également prévue et réprimée par l'article 323-4 du Code pénal, qui dispose que « la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

On trouve sur Internet de véritables éditeurs de malwares, qui proposent de télécharger leurs logiciels, avec différents niveaux de services associés, y compris une assistance technique 24h/24 et 7j/7. Dans l'exemple qui suit (figure 8-1), selon le niveau choisi par le client (99 \$, 179 \$ ou 249 \$), ce dernier bénéficie même d'une garantie si le malware est détecté par les antivirus, la durée de la garantie allant d'un mois à six mois. Le produit proposé peut enregistrer les frappes sur le clavier des victimes (numéros de cartes et mots de passe), envoyer de faux messages, lancer des attaques en saturation sur des sites web, intercepter des mots de passe, déclencher un espionnage par la webcam, etc.

	Bronze Edition • This product is the improved version of Turbojan 3.0 and it has some limitations(Webcam - audio streaming and man sniffer doesn't work for this version) • 1 month replacement warranty if it gets detected by any antivirus • 7/24 online support via e-mail • Supports only Windows 95/98/ME/NT/2000/XP • Realtime Screen viewing(controlling is disabled) Price : 99\$ (United State Dollar)
	Silver Edition • 4 months (maximum 3 times) replacement warranty if it gets detected by any antivirus • 7/24 online support via e-mail and instant messengers • Supports 95/98/ME/NT/2000/XP/Vista • Webcam streaming is available with this version • Realtime Screen viewing(controlling is disabled) • Notifies changements on clipboard and save them Price : 179\$ (United State Dollar)
	Gold Edition • 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months) • 7/24 online support via e-mail and instant messengers • Supports Windows 95/98/ME/NT/2000/2003/XP/Vista • Remote Shell (Managing with Ms-Dos Commands) • Webcam - audio streaming and man sniffer • Controlling remote computer via keyboard and mouse • Notifies changements on clipboard and save them • Technical support after installing software • Viewing pictures without any download(Thumbnail Viewer) Price : 249\$ (United State Dollar)

Fig. 8-1 > Plaquette publicitaire d'un éditeur de malwares

Enfin, l'article 323-7 du Code pénal réprime la tentative des délits de piratage : « la tentative des délits prévus par les articles 323-1 à 323-3-1 est punie des mêmes peines. »

La jurisprudence de ces articles récents est nécessairement réduite. Le 12 juin 2008, le tribunal de grande instance de Saverne a condamné une personne sur la base de l'article 323-3-1 à six mois d'emprisonnement avec sursis et 300 euros d'amende, ainsi qu'à des dommages-intérêts de 5 000 euros.

Peut-on chercher et publier des failles de sécurité ?

Les articles 323-1 à 323-3-1 ont été critiqués car ils interdisent par exemple aux journalistes ou aux « hackers blancs » (ceux qui préviennent lorsqu'ils trouvent une faille) de tester la sécurité des sites web, et de publier leurs trouvailles.

La Cour de cassation a ainsi confirmé le 27 octobre 2009 la condamnation du gérant d'une société de conseil en informatique, qui avait publié sur son site web les moyens permettant d'exploiter une faille informatique. Selon la Cour, il s'agissait d'une « mise à disposition, sans motif légitime », de moyens de piratage, alors que cette personne, de par son expertise, devait être particulièrement consciente du fait que ces informations risquaient d'être utilisées pour commettre des infractions.

Le site web zotuz.com, spécialisé dans la détection de failles dans les sites web, l'alerte de leurs propriétaires et l'information sur la sécurité, a lui aussi connu des difficultés avec ces articles du Code pénal, même s'il ne publie une faille qu'après sa correction.

Le vol de données

Une qualification juridique incertaine

On entend régulièrement parler dans la presse aussi bien de « vols de données personnelles » de clients, commis au détriment d'opérateurs ou de grandes entreprises, que de « vols de

données confidentielles » qui s'apparentent plutôt à de l'espionnage industriel. Dans ces dossiers, le terme de « vol » est utilisé par commodité de langage, mais il n'est pas toujours la qualification retenue juridiquement. En effet, pour qu'il y ait vol, selon la définition du Code pénal (article 311-1), il faut constater la « soustraction frauduleuse de la chose d'autrui ». Or, dans un vol de données, celles-ci ne sont pas « soustraites », mais recopiées ; elles demeurent à la disposition de leur légitime propriétaire qui ne peut donc pas déposer plainte pour « vol ».

Cette définition du vol par la « soustraction » date du Code Napoléon (1804). Remarquons que le droit romain était peut-être paradoxalement mieux adapté au vol de données, car les *Institutes* de l'Empereur Justinien, publiées en 529, définissaient plus largement le vol (*furtum*) comme « *contractatio rei fraudulosa* » : la manipulation frauduleuse d'une chose (livre IV, titre I, 1). Et de préciser « *furtum autem fit, non solum cum quis intercepti causa rem alienam amovet, sed generaliter cum quis alienam rem invito domino contractat* » : il y a vol, non seulement quand on déplace la chose d'autrui pour la dérober, mais de manière générale quand on en dispose sans la volonté du propriétaire (IV, I, 6).

Mais notre Code pénal moderne lie le vol à la disparition matérielle. Ainsi en avait jugé récemment le tribunal de grande instance de Créteil (23 avril 2013), qui rappelait que « en l'absence de toute soustraction matérielle de documents [...], le simple fait d'avoir téléchargé et enregistré sur plusieurs supports des fichiers informatiques (du légitime propriétaire) qui n'en a jamais été dépossédé, puisque ces données, élément immatériel, demeuraient disponibles et accessibles à tous sur le serveur, ne peut constituer l'élément matériel du vol, la soustraction frauduleuse de la chose d'autrui, délit supposant, pour être constitué, l'appréhension d'une chose ». Toutefois, la cour d'appel de Paris a infirmé ce jugement (5 février 2014), et a considéré au contraire que le vol de données était bien caractérisé par le fait de réaliser « des copies de fichiers informatiques

inaccessibles au public à des fins personnelles à l'insu et contre le gré de leur propriétaire ». Suite à ces appréciations divergentes de l'applicabilité de l'incrimination de vol, ce dossier se retrouve désormais devant la Cour de cassation, dont la mission est justement de dire comment on doit appliquer le droit.

Il est à noter que la même Cour de cassation avait validé le 9 septembre 2003 une condamnation pour vol, basée sur le fait « d'avoir en sa possession, à son domicile, après avoir démissionné de son emploi pour rejoindre une entreprise concurrente, le contenu informationnel d'une disquette support du logiciel Self Card, sans pouvoir justifier d'une autorisation de reproduction et d'usage du légitime propriétaire ». Elle a de nouveau validé le 4 mars 2008 une condamnation pour vol de données informatiques. Mais dans ces deux dossiers, la Cour n'a pas explicité comment l'incrimination de vol de données devait s'appliquer.

Lorsque l'on est victime d'un vol de données, d'autres solutions juridiques existent pour déposer plainte.

Si les données copiées sont des données personnelles (relatives à des personnes identifiées ou identifiables), le recours à l'article 226-18 du Code pénal (collecte frauduleuse de données personnelles) est possible.

Si le vol a été effectué via un accès frauduleux au système informatique (cas du hacking, du vol de mot de passe, du phishing...), l'article 323-1 du Code pénal trouvera à s'appliquer.

Si c'est une base de données qui a été recopiée, son propriétaire peut réclamer la protection accordée par l'article L. 341-1 du Code de la propriété intellectuelle, mais seulement si la constitution de la base a nécessité un investissement substantiel. La Cour de cassation a ainsi confirmé le 19 juin 2013 un arrêt refusant la protection d'une base de données en raison du caractère non substantiel des investissements réalisés.

Une évolution des textes

L'arsenal juridique vient récemment de s'enrichir de deux nouveautés.

Le 22 octobre 2014, dans une affaire de détournement de fichiers par un salarié, la Cour de cassation a validé la condamnation pour abus de confiance. Or, l'article 314-1 du Code pénal définit l'abus de confiance comme « le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé ». N'étant pas des fonds ou des valeurs, on en déduit que pour la Cour de cassation les données sont des biens. Ce qui nous ramène à l'idée de vol : si les données sont des biens, la notion de vol de données devient plus naturelle.

Mais le législateur vient peut-être de rendre ces discussions inutiles. En effet, la loi antiterroriste du 13 novembre 2014 a modifié l'article 323-3 du Code pénal cité plus haut. Cet article réprimait jusqu'ici uniquement l'introduction frauduleuse de données dans un système informatique, leur modification ou leur suppression. Désormais, sont également interdits les faits « d'extraire, de détenir, de reproduire ou de transmettre » frauduleusement des données.

La nouvelle rédaction de l'article 323-3 permet donc de réprimer efficacement à l'avenir les vols de données. Elle rend inutile le recours à l'article 311-1 et les débats sur son applicabilité, d'autant plus que la sanction du vol « traditionnel » n'est que de trois ans de prison et 45 000 euros d'amende (article 311-3), soit moins que ce qui est prévu par le nouvel article 323-3 (cinq ans de prison et 75 000 euros d'amende, portés à sept ans et 100 000 euros s'il s'agit de données personnelles volées dans un système d'information de l'État).

Les attaques contre les internautes

Le phishing

Le phishing (ou hameçonnage) est une fraude qui consiste à envoyer des courriels aux internautes en se faisant passer, le plus souvent, pour leur établissement financier ou pour un prestataire commercial, et à leur extorquer des informations personnelles (identifiant, mot de passe, etc.), pour accéder à leur compte.

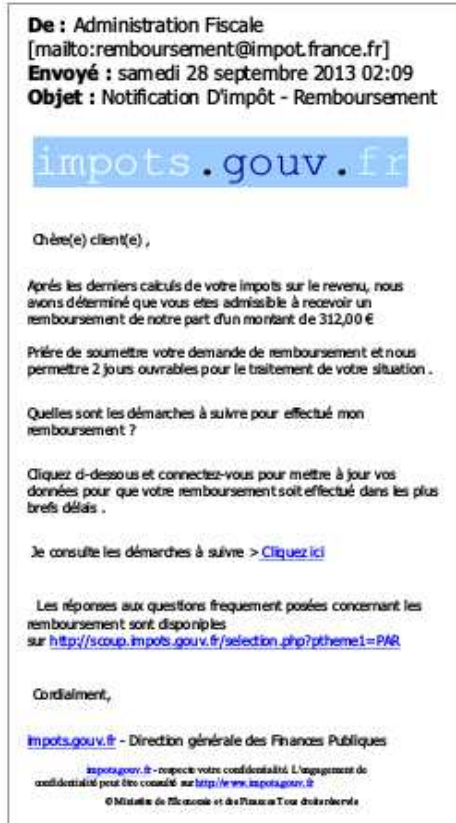


Fig. 8-2 >

Exemple de courriel envoyé pour phishing. Souvent, les phishings se signalent par les fautes d'orthographe qu'ils contiennent, mais ce n'est pas toujours le cas. Il faut se méfier même des courriels correctement rédigés.

Une variante assez répandue (appelée « arnaque nigériane ») consiste pour l'escroc à se faire passer pour une personne ayant, soit une fortune mais pas d'héritier, soit une fortune dont elle ne peut disposer sans effectuer un certain nombre de démarches (bloquée dans un pays en guerre, etc.). Le courriel reçu par l'internaute lui annonce, heureuse nouvelle, qu'il est désigné héritier, ou bien qu'on lui demande d'effectuer les démarches en question contre une commission substantielle. Dans les deux cas, il lui est demandé d'avancer un peu d'argent. Il va sans dire qu'une fois l'argent envoyé, l'internaute ne voit jamais la couleur du pactole promis.

Le 24 septembre 2007, le tribunal de grande instance de la Roche-sur-Yon a condamné pour escroquerie en bande organisée les auteurs d'une arnaque similaire, à des peines de trois à cinq ans de prison ferme.

En mai 2014, un étudiant de 21 ans a été arrêté à Nancy, pour avoir subtilisé grâce au phishing des numéros de cartes bancaires qui lui ont permis d'acheter en ligne pour des centaines de milliers d'euros d'articles de luxe et de technologie.

Le droit ne connaît pas le phishing en tant qu'infraction particulière. Toutefois, cette fraude combine de manière variable plusieurs phases qui peuvent chacune être sanctionnées. Le phishing débute ainsi par l'envoi d'un courriel non sollicité (spam), pratique visée par l'article L. 34-5 du Code des postes et des communications électroniques et réprimée par l'article R. 10-1 de ce même Code. Si le courriel piégé a été adressé intentionnellement à un internaute visé en particulier, dont l'adresse électronique aura été collectée de manière illícite, cette collecte frauduleuse de données personnelles est réprimée par l'article 226-18 du Code pénal. L'usurpation du nom et de l'identité visuelle d'un prestataire réel, pour tromper la victime et obtenir l'accès à son compte, grâce à un courriel et à un faux site crédibles, constitue ensuite une contrefaçon des droits intellectuels figurant sur un site (marque, logos, pages web, charte graphique, etc.) sanctionnée en droit des marques par les articles L.713-1 et suivants du Code de la propriété intellectuelle. Une fois le mot de passe de la victime obtenu frauduleusement, l'accès non autorisé au système d'information authentique et la modification intentionnelle de certaines données constituent une

atteinte aux STAD telle que définie aux articles 323-1 et suivants du Code pénal. Enfin, l'escroquerie au détriment de la victime peut être retenue comme incrimination principale sur le fondement des articles 313-1 et suivants du Code pénal.

LA LOI **Article 313-1 du Code pénal**

« L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

L'escroquerie est punie de cinq ans d'emprisonnement et de 375 000 euros d'amende. »

Le cas échéant, il peut se révéler également possible d'invoquer la responsabilité civile (article 1382 du Code civil), l'usurpation d'identité (article 434-23 du Code pénal) ou l'abus de confiance (articles 314-1 et suivants du Code pénal).

LA LOI **Autres articles utiles**

Article 1382 du Code civil :

« Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer. »

Article 434-23 du Code pénal, premier alinéa :

« Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. »

Article 314-1 du Code pénal :

« L'abus de confiance est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les représenter ou d'en faire un usage déterminé.

L'abus de confiance est puni de trois ans d'emprisonnement et de 375 000 euros d'amende. »

Condamnation pour escroquerie et accès frauduleux à un STAD

Visant à tromper la victime, personne physique, sur l'identité du prestataire auquel elle croit avoir affaire, et la victime, personne morale, sur l'identité de son client, cela afin d'accéder frauduleusement au compte de ce dernier, le phishing constitue une escroquerie, réalisée en accédant frauduleusement à un STAD et en y modifiant frauduleusement des données. C'est ce qu'a jugé, le 2 septembre 2004, le tribunal de grande instance de Paris, en condamnant un prévenu pour avoir « tenté de commettre des escroqueries au préjudice des sociétés Crédit Agricole, Crédit Agricole Région Normandie et Crédit Lyonnais, en employant des manœuvres frauduleuses, en l'espèce en copiant sur le site [xxx.com] qu'il avait créé, les pages d'accueil de ces deux banques afin de faire virer des sommes des comptes clients vers son compte ou celui de [son complice], [...], avoir, dans les mêmes circonstances de temps et de lieu, accédé frauduleusement au système de traitement automatisé de données du Crédit Lyonnais, particulièrement aux comptes de [ses victimes], et avoir modifié des données contenues dans ce système, notamment en ajoutant des relevés d'identité bancaire sur certains comptes, en modifiant le plafond de certains virements en effectuant un virement de 800 euros du compte N. sur le compte R. et de 15 000 euros du compte G. sur le compte A. ». Le prévenu a été déclaré coupable des faits de tentative d'escroquerie, accès frauduleux dans un STAD et modification de données résultant d'un accès frauduleux à un STAD, et condamné à un an d'emprisonnement avec sursis, à la confiscation des scellés, à environ 11 000 euros de dommages-intérêts et à 3 000 euros de frais de justice.

Il est à noter que dans ce dossier, le Crédit Lyonnais avait aussi porté plainte pour contrefaçon de marque, mais que la contrefaçon a disparu de la liste des infractions retenues dans la condamnation.

Condamnation pour contrefaçon

Lorsque, dans le but de tromper la victime, personne physique, l'auteur d'un phishing recopie dans un courriel ou sur une page web les signes distinctifs (logo, marque) d'une institution inspirant confiance, celui-ci commet une contrefaçon. À la différence de la précédente, cette solution permet de sanctionner pénalement l'auteur des faits, même s'il n'y a eu aucune victime physique.

Ainsi, un étudiant avait réalisé et mis en ligne en 2004 une copie de la page d'accueil de MSN, dans le but de récupérer les identifiants et les mots de passe d'abonnés. La fraude n'ayant apparemment pas réussi, il n'y a eu ni collecte frauduleuse de données, ni accès frauduleux à un STAD, ni escroquerie, ce qui empêchait une poursuite sur la base de ces infractions. Toutefois, Microsoft a déposé plainte pour contrefaçon de son site et de ses marques distinctives. Le prévenu a donc été poursuivi sur la base du Code de la propriété intellectuelle. Dans son jugement, le tribunal de grande instance de Paris l'a reconnu le 21 septembre 2005 coupable de détention de produits revêtus d'une marque contrefaite, d'usage ou apposition d'une marque sans l'autorisation de son propriétaire, de contrefaçon par édition ou reproduction d'une œuvre de l'esprit au mépris des droits d'auteur et de contrefaçon par diffusion ou représentation d'œuvre de l'esprit au mépris des droits de l'auteur. Prenant en compte la jeunesse du prévenu, son absence de casier judiciaire, la mauvaise qualité du site contrefait et le fait qu'aucune donnée n'avait été collectée, le tribunal a condamné le pirate à 500 euros d'amende avec sursis, à la confiscation des scellés et au versement à Microsoft de la somme de 700 euros de dommages-intérêts et de 300 euros de frais de justice.

Zoom Le recours au droit des marques est-il légitime ?

On peut toutefois s'interroger sur l'application directe du droit des marques au phishing. En effet, le droit des marques ne sanctionne l'usage non autorisé d'un signe distinctif que si cet usage compromet les fondions de la marque dans la vie des affaires, qui sont l'organisation de la concurrence et la garantie d'origine. Or, ce n'est pas dans le cadre de la vie des affaires que le fraudeur réalise le phishing : il ne cherche pas à capter la clientèle de la société usurpée. Au contraire, le phishing est réalisé dans le cadre d'une escroquerie. Néanmoins, il usurpe bien la fonction de garantie d'origine jouée par la marque, ce qui justifie le recours au droit de la contrefaçon.

L'efficacité de l'arsenal juridique ?

Ces différents dossiers montrent que, bien que l'infraction de phishing n'existe pas dans la loi, la répression peut se baser sur plusieurs autres infractions existantes. L'incrimination à retenir dépend du statut de la victime. Les prestataires de services sur Internet, dont le site web a été contrefait, peuvent déposer plainte pour contrefaçon ou pour accès frauduleux à leur STAD et modification frauduleuse des données. Les clients victimes peuvent déposer plainte pour escroquerie. La collecte frauduleuse de données, l'envoi de message non sollicité, ou l'abus de confiance, pourraient également constituer des fondements efficaces.

Il est à noter que l'usurpation d'identité peut moins facilement être invoquée par le client victime, car le Code pénal (article 434-23) ne réprime que « le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales ». Si l'usurpation d'identité consécutive au phishing n'a conduit qu'à détrousser la victime, cette dernière n'encourant pas de ce fait des poursuites pénales, elle ne peut invoquer l'article 434-23 du Code pénal.

Le véritable défi, qui concerne la police plus que la justice, consiste à identifier puis à interpeller le fraudeur, surtout si celui-ci agit depuis l'étranger. Il est à cet égard significatif de constater que, alors que toutes les grandes banques françaises ont été victimes de phishing depuis 2005, le nombre de fraudeurs arrêtés et condamnés reste infime.

Le spam

Le terme spam désigne tout courriel non sollicité. Il est souvent envoyé à des fins de prospection commerciale, que ce soit pour vendre des produits licites ou illicites. Le spam sert aussi de vecteur à de nombreuses escroqueries, comme le phishing, l'appel à des dons pour de fausses associations humanitaires, la proposition de faux produits d'épargne... Le spam a pris une ampleur extrêmement importante sur Internet, du fait de la quasi-gratuité pour l'émetteur qui rend cette pratique rentable : selon une étude des universités de Berkeley et San Diego publiée en 2008, il suffit qu'un spam sur 12,5 millions engendre une rentrée d'argent pour rendre l'activité rentable !

Considérant que le spam faisant la publicité d'un produit licite constitue un usage de l'adresse mail sans le consentement de son propriétaire et que les autres types de spam (publicités pour des contrefaçons, pour des stupéfiants, des armes ou des produits interdits) sont des fraudes, le législateur a décidé de réprimer cette pratique. L'interdiction du spam figure dans l'article L34-5 du Code des postes et communications électroniques interdisant plusieurs formes de prospection commerciale, dont le spam.

L'article L34-5 du CPCE

« Est interdite la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen. [...] Constitue une prospection directe l'envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services. »
Les sanctions sont précisées dans l'article R10-1 du même Code : il s'agit d'une contravention de 750 euros pour chaque message émis.

Par ailleurs, l'article L120-1 du Code de la consommation sert également à réprimer le spam, en classant comme pratique commerciale agressive et donc déloyale, le fait « de se livrer à des sollicitations répétées et non souhaitées par téléphone, télécopieur, courrier électronique ou tout autre outil de communication à distance ». Si un annonceur a confié sa promotion à un prestataire peu scrupuleux qui a recours à une base d'adresses collectées de manière illicite, la responsabilité de l'annonceur peut être engagée sur le fondement du Code de la consommation, en plus de celle du prestataire « spammeur » sur le fondement de l'article L34-5 du Code des postes et communications électroniques. L'annonceur honnête est donc fortement incité à veiller au respect par son prestataire des règles de démarchage.

La position de la Cnil

Cette prise en compte législative du spam doit être mise en relation avec la doctrine de la Cnil. Celle-ci distingue deux situations pour la prospection par courrier électronique. Pour la prospection envers des particuliers, le principe est l'interdiction des messages commerciaux sans accord préalable du destinataire, sauf dans deux cas : « si la personne prospectée est déjà cliente de l'entreprise et si la prospection concerne des produits ou services analogues à ceux déjà fournis par l'entreprise, [ou] si

la prospection n'est pas de nature commerciale (caritative par exemple) ». Dans ces deux cas, la personne concernée doit être informée au moment de la collecte de ses coordonnées que son adresse sera utilisée à des fins de prospection et doit pouvoir s'y opposer de manière simple et gratuite.

Considérant que la protection des données personnelles a pour but le respect de la vie privée, la Cnil en déduit que dans le cadre des activités professionnelles cette protection peut s'apprécier différemment. Ainsi, pour la prospection envers les professionnels, l'accord préalable n'est pas requis si l'objet de la prospection est en rapport avec l'activité de la personne visée. Celle-ci doit toutefois, lors de la collecte de ses coordonnées, être informée que son adresse sera utilisée à des fins de prospection et pouvoir s'y opposer de manière simple et gratuite.

Dans tous les cas, chaque message doit préciser l'identité de l'expéditeur et proposer un moyen simple de s'opposer à la poursuite de la prospection.

Signaler un spam

Lorsque l'on reçoit un spam, le premier réflexe est de le mettre à la poubelle. Toutefois, il peut se révéler plus judicieux de le signaler aux autorités compétentes, pour les aider à lutter plus efficacement contre ces pratiques.

En France, l'association Signal Spam regroupe les autorités (Cnil, police, gendarmerie), les fournisseurs d'accès à Internet (Orange, SFR, etc.) et les associations de marketing et d'annonceurs dont l'objectif est d'éradiquer le démarchage malhonnête. Son site www.signal-spam.fr propose aux internautes de « signaler » les spams reçus, c'est-à-dire de les transférer à l'association. Ses différents membres agiront ensuite chacun dans sa sphère de compétence : enquête policière, plainte pour contrefaçon, blocage par les FAI du site émetteur, etc.



Fig. 8-3 > La page d'accueil du site Signal Spam

La répression du spam

Le Code des postes et communications électroniques n'érige le spam qu'en contravention, ce qui limite son intérêt pour dissuader les spammeurs. En revanche, une sanction plus lourde est possible en recourant aux autres qualifications comme les atteintes aux données personnelles ou aux STAD, mais aussi aux textes réprimant la contrefaçon, ou au droit des contrats.

Des jurisprudences montrent que des faits de spam ont pu être sanctionnés sur le fondement de l'entrave au fonctionnement d'un STAD (article 323-2 du Code pénal), la collecte massive des adresses dans des annuaires ou l'envoi massif de messages ayant perturbé le bon fonctionnement des systèmes concernés. Dans ces affaires, l'entrave au fonctionnement du système n'était pas intentionnelle, mais constituait un « dommage collatéral » du spam : il s'agissait dans un cas de la

saturation de messageries de Minitel rose par des publicités pour des services concurrents (cour d'appel de Paris, 5 avril 1994) et dans l'autre de l'envoi massif de messages vers les forums de discussion d'un grand magasin, invitant les autres internautes à envoyer à leur tour des messages en forme de pétition (cour d'appel de Paris, 30 mars 2005).

Une telle incrimination suppose qu'il y ait bien eu entrave, c'est-à-dire que le fonctionnement du système a réellement été affecté. Elle n'est donc utilisable que pour certains cas de spam.

Le plus souvent, le spammeur s'est procuré l'adresse mail des destinataires d'une manière déloyale ou frauduleuse. L'infraction de collecte déloyale, frauduleuse ou illicite de données personnelles est ainsi constituée (article 226-18 du Code pénal). La Cour de cassation a confirmé le 14 mars 2006 la condamnation d'un émetteur de spam sur ce fondement.

Si le spam propose des produits contrefaits, la société détentrice des droits authentiques peut également attaquer le spammeur pour contrefaçon.

Enfin, l'interdiction de la pratique du spam figure de manière explicite dans le contrat qui lie l'internaute à son fournisseur d'accès Internet. Ce dernier est donc fondé à couper l'accès aux émetteurs. Le tribunal de grande instance de Paris a ainsi confirmé le 15 janvier 2002 la légalité de cette coupure de l'abonnement, condamnant en outre le spammeur à payer 1 500 euros à chacun de ses fournisseurs. Dans une affaire similaire, le tribunal de commerce de Paris a condamné le 5 mai 2004 un spammeur pour violation des dispositions contractuelles le liant à son fournisseur d'accès Internet, AOL, et à son prestataire de messagerie Hotmail, Microsoft. En effet, cette personne avait utilisé son accès AOL et ses adresses de messagerie Hotmail pour diffuser des spams. Or, les contrats d'ouverture de compte et les conditions générales d'utilisation, aussi bien d'AOL que de Hotmail, inter-

disent expressément le spam ; l'acceptation de ces clauses est techniquement indispensable à l'ouverture du compte. Le tribunal a donc condamné le spammeur à 5 000 euros de dommages et intérêts à chacune des sociétés.

Que faire face à une infraction informatique ?

Deux cas peuvent se présenter : l'internaute peut être soit lui-même victime d'une attaque contre son ordinateur, ses données ou ses biens, soit simplement être témoin et constater une infraction (publicité pour une contrefaçon, commentaires racistes sur un blog, présence d'une image pédopornographique sur un site...). Les démarches à suivre diffèrent selon les situations.

Signaler une infraction

Si l'internaute constate une infraction en ligne, mais n'est pas victime, il peut la signaler aux autorités sur le site :

www.internet-signalement.gouv.fr

S'il s'agit d'un spam, l'internaute est renvoyé sur la plateforme :

www.signal-spam.fr

S'il s'agit d'un problème de consommation, de qualité ou de sécurité de produits commerciaux, il est invité à s'adresser à la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

Pour les autres infractions (incitation à la haine raciale ou à la violence, trafic de stupéfiants ou d'armes, injure ou diffamation, escroquerie...), l'internaute doit préciser où et quand il a observé le contenu illicite. Ce signalement peut rester anonyme s'il le souhaite.

FIG. 8-4 > Formulaire de signalement

Le signalement est ensuite traité par les services de police spécialisés.

Déposer une plainte

Si l'internaute est victime d'une infraction informatique (diffamation en ligne, escroquerie, vol de numéro de carte bancaire, infection de l'ordinateur par un malware qui bloque son fonctionnement en exigeant une rançon...), il doit porter plainte auprès du commissariat de police ou de la gendarmerie. Si la plainte implique un site étranger non représenté

en France (par exemple Facebook, Amazon, etc.), il faudra éventuellement demander l'envoi d'une réquisition spécifique (en anglais) au siège social du site. Pour exécuter cette procédure délicate de droit international, il est souhaitable que le commissariat demande l'assistance des services spécialisés – Office central de lutte contre les infractions aux technologies de l'information (police) ; division de lutte contre la cybercriminalité (gendarmerie) ; brigade d'enquête sur les fraudes aux technologies de l'information (préfecture de police de Paris).

Un service de préplainte en ligne est disponible sur le site www.pre-plainte-en-ligne.gouv.fr, mais il se limite aux atteintes aux biens (vols, dégradations, escroqueries). Il aide à rédiger la plainte que l'on doit ensuite aller signer au commissariat ou à la gendarmerie. Le site permet de prendre un rendez-vous avec le service de son choix.

Il convient de réunir tous les éléments de preuve disponibles : nom ou pseudonyme et adresse mail du suspect éventuel, copie des textes, des images ou de la vidéo en cause, adresse des pages web concernées, nom du site web, si possible relevé de connexion de l'ordinateur (*log*) et tout autre renseignement pertinent. Un constat d'huissier peut éventuellement se révéler utile.

La cour d'appel de Paris a rappelé le 27 février 2013 les bonnes pratiques à respecter par les huissiers pour que leur constat soit valide et ait force probante : « description du matériel ayant servi aux constatations, indication de l'adresse IP de l'ordinateur ayant servi aux opérations de constat, caches de l'ordinateur vidés préalablement à l'ensemble des constatations, désactivation de la connexion par proxy, suppression de l'ensemble des fichiers temporaires stockés sur l'ordinateur ainsi que l'ensemble des cookies et l'historique de navigation ». La cour a par ailleurs précisé que les normes Afnor existantes pour la réalisation des constats ne constituent qu'un recueil de recommandations de bonnes pratiques et que leur respect n'a pas un caractère obligatoire, du moment que l'huissier respecte l'ensemble des règles jurisprudentielles relatives à la force probante des constats effectués sur Internet.

Attention, pour les diffamations et injures, la plainte doit être déposée dans les trois mois suivant la mise en ligne du texte litigieux. Après ce délai, on ne peut plus poursuivre l'auteur du texte, mais on peut faire retirer le contenu litigieux s'il est reconnu par un juge comme illicite (voir le chapitre 1 sur la liberté d'expression).

Si la plainte concerne les données personnelles de l'internaute, celui-ci doit d'abord contacter le responsable du traitement en cause. Si son droit d'accès, de rectification ou d'opposition n'est pas respecté dans un délai de deux mois, l'internaute peut alors saisir la Cnil sur son site web (www.cnil.fr/vos-droits/plainte-en-ligne). La Cnil interviendra auprès du responsable du traitement et pourra le cas échéant faire usage de ses pouvoirs de contrôle et de sanction (voir le chapitre 3 sur les données personnelles).

Index

3D Secure 172

4G 5

A

AAI 139

adresse IP 140, 157

Amazon 159

amnistie 28

anonymat 35, 102, 105, 169, 174

apologie de crime 25–26, 51

Apple 116

ARJEL 182

arrêt Nikon 186, 194

aspiration de site 209

audit de sécurité 207

autorité administrative
indépendante

voir AAI

avatar 102, 111, 118

B

biométrie 114

bitcoin *voir* monnaie virtuelle

Blu-Ray 136

bonne foi 21

BYOD 195

C

CA 16

carte bancaire 170

carte d'identité électronique 114

Cnil 58, 63, 65–67, 73, 76–77,

80, 83–84, 96, 101, 139,

166, 168, 230–231

Code civil 30, 42, 54, 69–70,

161, 175, 180, 187, 225

Code de la consommation 146,

158–160, 162–163, 165,

175, 230

Code de la propriété

intellectuelle 109, 122–123,

130, 136–137, 142, 145,

147, 224, 227

Code des postes et des

communications

électroniques 149

voir CPCE

Code du commerce 176

Code du travail 194–196

Code monétaire et financier

171–173, 181

Code pénal 20, 68, 81, 83–85,

98, 106–108, 118–119,

166, 187, 200, 203, 205,

209–212, 215–217, 219,

224–225, 232–233

code PIN 170, 173

collecte déloyale 233

Commission nationale de

l'informatique et des libertés

voir Cnil

concurrence déloyale 131

conditions d'utilisation 1

- confidentialité 186, 199
 - Conseil constitutionnel 39–40, 45, 54, 115, 206
 - contrefaçon 140, 146, 148, 151
 - cookie 80–82
 - copie privée 128, 134, 137
 - correspondance privée 13
 - courriel 13, 186
 - CPCE 80, 165–166, 224, 229–230, 232
 - création
 - base de données 142
 - citation 128
 - contrefaçon 131–132, 138
 - copie privée 128, 134, 137
 - copie transitoire 129
 - diffusion 133
 - discours destiné au public 128
 - divulgateur 126
 - exception d'enseignement 128
 - exploitation 121, 126
 - légitime rétribution 122
 - licence logicielle 129
 - logiciel 142
 - parodie 129
 - représentation 126
 - reproduction 121, 123, 126, 129, 132
 - site web 142, 147
 - crime organisé 217
 - cryptogramme visuel 170
 - cybercriminalité 203
 - accès ou maintien frauduleux dans un STAD 204, 206–207, 209, 216, 226
 - arnaque nigériane 224
 - attaque informatique 216
 - contre les systèmes informatiques 203
 - contrefaçon 227, 232–233
 - copie d'un site web 209
 - entrave au fonctionnement d'un STAD 212–214
 - escroquerie 226
 - malware 217–218
 - modification frauduleuse des données d'un STAD 215–216
 - phishing 223, 226, 228
 - répression du piratage 216
 - sanction 227
 - suppression des données d'un STAD 216
 - trafic de logiciels de piratage 217
 - cybersquatting 150–151
 - cybersurveillance 118
- D**
- Dailymotion 48, 139
 - Déclaration universelle des droits de l'homme 12, 35, 40, 54, 56
 - Deep Packet Inspection *voir* DPI
 - déni de service 213
 - devoir du créateur de site web 76
 - conservation des données de connexion 83
 - cookie 81
 - devoir d'information 77
 - formalité administrative 77
 - prospection commerciale 79
 - sécurité des données 78

- DGCCRF 166, 168, 234
 - diffamation 14, 46
 - publique 19, 197
 - Digital Rights Management
 - voir* DRM
 - directeur de publication 37, 39, 41, 46
 - dissimuler l'expéditeur 81
 - donnée confidentielle 185, 198, 200–201, 207
 - donnée personnelle 57–58, 60, 69, 76–78, 80, 84, 92, 103, 105, 194, 207, 210, 231–232
 - « sensible » 63
 - accès manuel 65
 - collecte 100, 215, 232–233
 - consentement à un
 - traitement 62
 - divulgaration à l'insu 97
 - droit d'accès 62
 - droit d'opposition 62
 - droit de modification 62
 - durée de conservation 62
 - exportation hors UE 63
 - finalité d'un traitement 62
 - généalogie 130
 - information sur un
 - traitement 62
 - protection 43, 61, 63, 101
 - qualité 62
 - sécurité 62
 - valeur 58
 - DPI 8
 - DRM 133, 136–137, 139
 - droit
 - américain 13
 - français 13
 - droit à l'image 98
 - droit d'auteur 121, 132–133
 - auteur salarié 142
 - citation 128
 - copie privée 128
 - discours destiné au public
 - 128
 - droit de représentation 126
 - droit de reproduction 126
 - exception d'enseignement
 - 128
 - exception de parodie 129, 132
 - moral 126
 - patrimonial 126, 133, 145
 - photo 124, 127
 - site web 147
 - tableau 125
 - tweet 125
 - droit de l'internaute
 - droit à l'anonymat 102
 - droit au déréférencement 75
 - droit d'accès et de
 - rectification 73
 - droit d'opposition 72, 165
 - droit de consentement 71, 80
 - faire valoir ses droits 76
 - droit de propriété 61
 - droit de réponse 29, 31
 - droit prétorien 48, 143, 177
- E**
- e-administration 2
 - e-banque 2
 - eBay 159, 174, 176
 - e-commerce 2, 73, 79, 153, 167
 - achat en ligne 154

- conclusion de l'achat 161
- délai de livraison 160
- détail de l'offre 157
- droit de rétractation 162–163, 175
- en cas de litige 166
- fisc 175
- garantie 160, 175
- identification du prestataire 156
- information du consommateur 162
- offre promotionnelle 165
- paiement en ligne 169
- pharmacie en ligne 155
- place de marché 159
- publicité par courriel 165
- réclamation 158
- responsabilité du prestataire 158
- éditeur 43
- employeur 186
- e-réputation 91, 111
 - mensonge 103
 - nettoyage 99
 - protection 102
- espace public 199
- espionnage 207
- exception de vérité 27
- exigence de sécurisation 211
- F**
- Facebook 13, 18–19, 24, 42–43, 60, 68, 74, 92–95, 100, 105, 109, 116, 147, 195, 198
- FAI 2, 4, 19, 38, 49, 192, 231, 233
- faute grave 199
- Fevad 167
- fnac.com 159
- fournisseur de service 49
- G**
- G29 101
- géolocalisation 105
- Google 68, 116–117, 195
- Google Suggest 21
- H**
- hacking 217
- Hadopi 136, 138, 141
- hameçonnage
 - voir cybercriminalité, phishing
- hébergeur 36, 38, 43–44, 48–49, 51, 98, 117, 148, 159, 177
- I**
- identité numérique 106, 206
 - preuve 111, 113, 179
 - signature électronique 179–180
 - usage 112
 - usurpation 106, 109, 224
- incitation 23, 25
 - à la haine 51
- infraction informatique 234
 - déposer une plainte 235
 - signalement 234
- injure 14
 - privée 20
 - publique 17–19, 21
- Internet
 - abonnement 3–6
 - coût 3
 - débit 3

financement 9
mobile 5
neutralité 6–7

J

jurisprudence 16, 85, 165, 173,
175–176, 186, 188–189,
194, 196, 201, 206,
213–214, 219, 232

L

leboncoin.fr 159, 174
légalité du contenu
 contrôle 44
 réapparition de contenu
 supprimé 47, 49
liberté d'expression 12
LinkedIn 95
liste de diffusion 33
logiciels espions 208
loi du 29 juillet 1881 14,
 20–21, 23, 25–27, 29–31,
 37, 39
loi Gayssot 26
loi Godfrain 203
loi Informatique et Libertés 21,
 51, 58, 65–70, 73, 75–77,
 81, 83–84, 130, 139, 166,
 194
 champ d'application 64
 condition de localisation 66
 hors UE 68
loi LCEN 29, 31, 36, 38,
 43–47, 49, 51, 69, 98, 154,
 156–157, 159, 217

M

marketplace

voir place de marché
m-commerce 167
Microsoft 116
modération 38
monnaie virtuelle 169, 181
MSN 20
MySpace 95

N

négationnisme 26
nom de domaine 148, 150–151
nom de marque 150

O

obfuscation 99
One-time password
 voir OTP
open data 130
open source 130
opt-in 82
opt-out 82
ordre public 12–13
OTP 114

P

P2P 139
Paylib 173
PayPal 116–117, 169, 174
pédophilie 118
pédopornographie 51
peer-to-peer
 voir P2P
personne morale 36
personne physique 36
phishing 108, 113, 223
plainte contre X 19
pornographie 186
prescription 28, 30
 délai 29

PriceMinister 159, 174–175
 producteur 38–39, 41
 propriété intellectuelle 121
 littéraire et artistique
 122–123
 logiciel et base de données
 122
 propriété industrielle 122
 prospection
 commerciale 80
 politique 80
 religieuse 80
 syndicale 80
 prud'hommes 198
 pseudonyme 102, 105, 111,
 117–118
 puce e-services 115

Q

QPC 17, 28, 40
 quadruple play 4
 question prioritaire de
 constitutionnalité
 voir QPC

R

référé 19–20
 réhabilitation 28
 réseau anonymisé 105
 réseau social 91, 98, 102, 105,
 109, 119, 185, 195, 197
 désinscrire 92
 donnée personnelle 92, 94
 effacer les traces 92
 forum 93
 responsabilité de ses actes 35,
 37, 39, 41
 en cascade 37, 40
 hébergeur 43

ressource radio 5
 rétro-ingénierie 145
 revue de presse 128, 131

S

sanction 19–20, 23, 25–27,
 31–32, 39, 41–42, 60, 80,
 83–85, 98, 106–107, 119,
 125, 131–133, 137, 140,
 148, 150–151, 154, 166,
 182, 187, 198, 200–201,
 205–207, 209, 213,
 215–216, 219, 225–226,
 230
 financière 18
 secret professionnel 36
 sécurité informatique 210
 chercher des failles de
 sécurité 219
 publier des failles de sécurité
 219
 service web 2, 10
 signaler un contenu illicite 42
 signal-spam 231
 site web personnel 36, 43
 spam 71, 73, 166, 213, 224,
 229
 répression 232
 signalement 231
 STAD 204, 216, 232
 streaming 133, 138–139
 sursis 19
 système de traitement
 automatisé des données
 voir STAD

T

TCP-IP 6, 140
 téléchargement illégal 133,

138–140
 télétravail 195
 TGI 16, 119
 The Onion Router
 voir TOR
 TI 16
 TOR 106
 transaction en ligne 153, 179
 banque en ligne 179
 entre particuliers 159, 174,
 176
 jeu en ligne 181
 monnaie électronique 181
 point de fidélité 181
 Transmission Control Protocol
 voir TCP-IP
 tribunal 16
 Conseil constitutionnel 17,
 28
 cour d'appel
 voir CA
 Cour de cassation 16–17
 d'instance
 voir TI
 de grande instance
 voir TGI
 triple play 4
 Twitter 13, 19, 24, 43, 51, 68,
 95, 195

U

Uniform Resource Locator
 voir URL
 URL 149

V

vente liée 146
 Viadeo 18, 95

vie privée 13, 54, 57, 60,
 69–70, 81–82, 84–85,
 101, 103, 119, 183, 186,
 192, 231
 Code civil 98
 d'un tiers 97
 vie professionnelle
 accès aux courriels d'un
 employé 186
 accès aux documents 188
 accès aux fichiers d'un
 employé 186, 190,
 192
 analyse des connexions 185
 BYOD 184, 191–193
 document personnel 189
 filtrage des connexions 185
 pornographie 186
 réseau social 185, 195, 197
 secret professionnel
 200–201
 sécurité 193
 télétravail 184, 191, 195
 Virgin 100
 VLC 136

W

Western Union 169, 174, 176

Y

Yahoo! 68
 YouTube 48, 139