www.jusletter.ch

Sébastien Fanti

Cybercriminalité, droit d'auteur et protection des données

Panorama législatif et jurisprudentiel en Europe et en Suisse

Après avoir mis en exergue les principales pistes suivies par les différents acteurs en Europe en matière de droit d'auteur, de jeux d'argent on-line, de responsabilité des intermédiaires techniques ou de cybercriminalité, l'auteur se penche sur les développements récents en Suisse et le droit désirable.

Catégorie(s) : Droit de l'informatique ; Droit d'auteur

Proposition de citation : Sébastien Fanti, Cybercriminalité, droit d'auteur et protection des données, in : Jusletter 31 mars 2008

Table des matières

I. Bref aperçu des développements les plus marquants intervenus en Europe

[Rz 1] La **France** connaît une véritable révolution juridique avec l'adoption ou les projets d'adoption de normes en matière de droits d'auteur, de cybercriminalité et de responsabilité des intermédiaires techniques notamment. S'agissant tout d'abord des droits d'auteur, l'adoption de la DADVSI (Loi sur le droit d'Auteur et les Droits Voisins dans la Société de l'Information[1]), après un vif débat et une décision de non-conformité partielle du Conseil constitutionnel[2], démontre que le problème du téléchargement des œuvres devient une priorité en France. À ce titre, la loi prévoit la poursuite des éditeurs et exploitants de logiciels de P2P[3] qui mettent à disposition des œuvres protégées sans autorisation des ayants-droits et sans inclure la gestion des mesures de protection technique[4]. La deuxième disposition phare de la loi concerne spécifiquement les utilisateurs de ces logiciels qui pourraient être poursuivis pour délit de contrefaçon pour une simple utilisation des logiciels de P2P (pair à pair), soit le download et l'upload. Le conditionnel est de mise, car l'article topique (L.2335-111) du Code de la propriété intellectuelle (CPI) a été déclaré non-conforme à la Constitution et entièrement censuré en raison de son caractère discriminatoire[5]. Il conviendra, conséquemment, d'attendre les premières décisions de justice pour savoir si le risque de condamnation est théorique ou réel. Quoi qu'il en soit, le débat relatif à la licéité du téléchargement à titre privé est loin d'être clos[6].

[Rz 2] Le 26 juillet 2007, le Ministère de la Culture et de la Communication a confié au Président directeur général de la FNAC, Monsieur Denis Olivennes[7] une mission sur la lutte contre le téléchargement illicite et le développement des offres légales d'œuvres musicales, audiovisuelles et cinématographiques[8]. Cette mission de réflexion et de concertation (soutenue par le Président de la République[9]) avait notamment pour but de favoriser la conclusion d'un accord entre professionnels permettant le développement d'offres légales d'œuvres en ligne et dissuadant le téléchargement illégal de masse. Le rapport Olivennes[10] sur le développement et la protection des œuvres culturelles sur les nouveaux réseaux a débouché sur la conclusion d'un accord entre les pouvoirs publics, les ayants droit de l'audiovisuel, du cinéma et de la musique, ainsi que les chaînes de télévision et les prestataires techniques[11].

[Rz 3] Cet accord renferme, selon le Président de la République, des « stipulations nouvelles et fortes ». D'un côté, il prévoit l'envoi de mails d'avertissements aux internautes qui font un mauvais usage de leur abonnement, des avertissements gradués en cas de récidive, voire la possibilité de suspendre temporairement l'accès à internet[12]. Les « pirates professionnels », soit ceux qui font sciemment du trafic et du commerce illicite de DVD et de fichiers contrefaits, resteront soumis au droit commun de la contrefaçon, et traités au sein de juridictions spécialisées. Les **fournisseurs d'accès** s'engagent quant à eux, en sus de l'envoi des messages d'avertissement et de l'exécution des décisions de sanctions, à mettre en œuvre des dispositifs de filtrage[13]. Les **professionnels de**

---

1 Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.

2 Décision du 27 juillet 2006 n° 2006-540 DC, décision qui a, de manière générale, durci la loi.

3 Contraction de peer-to-peer ; pair à pair ou d'égal à égal en français ; type de connexion réseau par laquelle deux machines communiquent d'égal à égal ; ce type de connexion permet à des millions d'internautes affiliés à un réseau de partager leurs fichiers stockés sur le disque dur de leur machine.

4 Article L.335-2-1 du Code de la propriété intellectuelle qui prévoit une sanction lourde puisque le juge pourra prononcer jusqu'à 3 ans d'emprisonnement et 300'000 Euros d'amende.

5 Point 65 de la décision du 27 juillet 2006 : « (…) *les particularités des réseaux d'échange de pair à pair ne permettent pas de justifier la différence de traitement qu'instaure la disposition contestée ; que, dès lors, l'article 24 de la loi déférée est contraire au principe de l'égalité devant la loi pénale ; qu'il y a lieu, sans qu'il soit besoin d'examiner les autres griefs, de le déclarer contraire à la Constitution* ».

6 La circulaire du 3 janvier 2007 du Ministre de la Justice : mentionne toutefois expressément qu'en matière de téléchargement d'œuvres proposées illégalement sur Internet, l'exception de copie privée n'a pas vocation à être retenue, en se fondant sur la loi et deux arrêts de la Cour de cassation.

7 Il convient de préciser que pour cette mission, M. Olivennes était assisté de trois autres membres de mission, raison pour laquelle on évoque régulièrement la Commission Olivennes.

8 Lettre de mission.

9 Discours du Président de la République du 23 novembre 2007.

10 Rapport officiel.

11 Liste des signataires de l'accord.

12 Cette démarche pédagogique sera selon les termes du Président de la République réservée aux pirates de bonne foi pour reprendre une expression propre à la politique fiscale. Elle repose sur le principe de la responsabilité de l'abonné du fait de l'utilisation frauduleuse de son accès, actuellement posé à l'article L. 335-12 du CPI, et sera pilotée par une autorité publique spécialisée, placée sous le contrôle du juge, de manière à garantir les droits et libertés individuels. Sur plainte des ayants droit, directement ou à travers les structures habilitées par la loi à rechercher les manquements au respect des droits, elle enverra sous son timbre, par l'intermédiaire des fournisseurs d'accès à Internet, des messages électroniques d'avertissement au titulaire de l'abonnement. En cas de constatation d'un renouvellement du manquement, elle prendra, ou saisira le juge en vue de prendre, des sanctions à l'encontre du titulaire de l'abonnement, allant de l'interruption de l'accès à Internet à la résiliation du contrat Internet.

13 Le filtrage consiste à retirer automatiquement les fichiers « pirates » des

la musique, du cinéma et de l'audiovisuel s'engagent à mettre plus complètement et plus rapidement leurs œuvres en ligne, et à supprimer tous les verrous techniques qui empêchent de copier et de transporter la musique. Ces améliorations qualifiées de majeures profiteraient pleinement aux consommateurs.

[Rz 4] Ce rapport a fait l'objet de larges critiques et certains acteurs majeurs ont tout simplement refusé de le parapher[14]. D'aucuns critiquent une approche politique, qu'il serait difficile de mettre en œuvre sur le plan juridique.

[Rz 5] L'exemple de l'utilisation de l'adresse IP qui se heurte à la définition des données à caractère personnel est régulièrement cité[15]. D'autres regrettent l'approche répressive et estiment qu'on a perdu une occasion de reformuler pour une longue période les fondements de l'industrie en mettant au point de nouveaux modèles économiques. Monsieur Denis Olivennes lui-même reconnaît[16] que « *Juridiquement, le système d'avertissement et de sanction n'est pas évident. Il faudra sans doute passer par une autorité indépendante chargée, sur plainte des ayants droit, de mettre en œuvre le dispositif. Bien sûr, il reste à transcrire tout cela dans le marbre de la loi.* ».

[Rz 6] Les principales critiques[17] ont trait au rôle de l'autorité administrative indépendante (le recours au juge étant selon de nombreux juristes indispensable en cas d'atteinte aux droits individuels), à la procédure elle-même (qui ne respecterait pas les standards conventionnels dont le droit à un procès équitable), ainsi qu'au fait que l'adaptation en droit français de la directive européenne[18] est intervenue par le biais de la loi DADVSI adoptée un an plus tôt, une remise en question si rapide avec des spécificités franco-françaises nombreuses apparaissant à tout le moins inopportune, voire contraire à la directive. D'éminents juristes parviennent donc à la conclusion que « le droit a été piraté ». Certains[19] relèvent toutefois que la situation post-rapport Olivennes constitue un retour aux poursuites graduées existante avec la censure du Conseil constitutionnel de l'article 24 de la DADVSI. Il convient désormais d'attendre l'adoption des dispositions légales qui formaliseront (au printemps 2008, semble-t-il) l'accord adopté suite à ce rapport controversé. La principale problématique aura trait aux contradictions entre la position adoptée par la Commission Nationale Informatique et Libertés[20] (en matière de messages préventifs notamment) et celle qu'adoptera la future Autorité Publique de Lutte contre la Piraterie Numérique (issue du rapport Olivennes), le tout à l'aune de la récente décision de la Cour de justice des Communautés européennes dans l'affaire Promusicae (cf. note nº 16).

[Rz 7] Pour ajouter encore à la confusion, le rapport de la Commission pour la libération de la croissance française[21], présidée par Monsieur Jacques Attali et remis au Président de la République le 23 janvier 2008 préconise l'adoption de la licence globale[22].

[Rz 8] Ce rapport propose (décision nº 57) que soit mise en place une rémunération versée par « *les vrais bénéficiaires des téléchargements : les fournisseurs d'accès à Internet. Il convient de faire verser par les fournisseurs d'accès Internet une contribution aux ayants droit auprès des différentes sociétés de gestion collective des droits d'auteur, sous la forme d'une rémunération assise sur le volume global d'échanges de fichiers vidéo ou musicaux. Cette contribution, qui pourra être répercutée sur les usagers, assurera une rémunération juste des artistes, en complément des revenus du spectacle vivant, des CD, des DVD, des abonnements au téléchargement et de toute autre source de revenus à venir, sans pour autant pénaliser le développement d'Internet* ». Reste donc à savoir quel rapport (leurs contenus étant intrinsèquement contradictoires) obtiendra le soutien du Président de la République.

[Rz 9] Le Gouvernement semble avoir résolu cette épineuse question, puisqu'un avant-projet de loi Olivennes[23], est évoqué, avant-projet qui serait soumis d'urgence au Sénat en avril 2008[24]. Il est intitulé avant-projet de loi relatif à la Haute Autorité pour la diffusion des œuvres et la protection des droits d'auteur sur internet (Hadopi). Cet avant-projet stipulerait que des agents de l'État seraient habilités à exiger des fournisseurs d'accès à Internet (ci-après : FAI) l'identité des internautes sans recourir à une procédure judiciaire durant

réseaux ou des plateformes d'hébergement au fur et à mesure de leur apparition.

14 Dailymotion par exemple.

15 Cf. à cet égard la récente décision de la Cour de justice des Communautés européennes dans l'affaire Promusicae qui stipule notamment que l'adresse IP est une donnée personnelle ; cette décision est disponible sur le site de la Cour : http://curia.europa.eu.

16 Interview réalisée par le quotidien Le Monde le 23 novembre 2007.

17 Cf. à ce sujet, la critique de Me Gilles Devers sur son blog ou encore l'article de Me Stéphanie Sioën-Gallina intitulé « Quand la lutte contre la contrefaçon s'organise ».

18 Directive du Parlement européen 2001/29/CE et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

19 Dont Me Olivier Hugot, dans une interview réalisée par le Monde informatique.

20 Cf. www.cnil.fr/?id=1881 dont la position avait été censurée par le Conseil d'État sur la question de la surveillance des réseaux P2P par les sociétés de gestion collective, cf. www.cnil.fr/index.php?id=2344.

21 Rapport de la Commission pour la libération de la croissance française.

22 Le système de licence globale permet aux internautes de télécharger librement et gratuitement en échange d'une indemnité forfaitaire. L'Assemblée nationale avait ouvert la voie à son adoption fin 2005 avant qu'il ne soit enterré.

23 EXCLUSIF : Avant-projet de loi Olivennes, le texte complet.

24 La procédure d'urgence permet au gouvernement de faire adopter le texte sans la traditionnelle navette entre les deux chambres de l'assemblée. Pour mémoire, la loi DADVSI avait été adoptée en procédure d'urgence en 2006. Après sa lecture au Sénat, le texte pourrait être voté dès sa lecture à l'Assemblée nationale d'ici l'été.

laquelle un magistrat garantirait le respect des droits de la défense et des libertés individuelles. L'autre pomme de discorde a trait au fait que le responsable n'est pas celui qui télécharge, mais le titulaire d'abonnement à Internet dont l'accès est utilisé, y compris par une tierce personne, pour effectuer des téléchargements illicites. Une nouvelle version de l'avant-projet a été établie[25], suite à la consultation des juristes des différents ministères compétents. Ce deuxième avant-projet[26], entièrement revu dans ses mécanismes juridiques, crée une nouvelle infraction de nature pénale, à inscrire au Code de la propriété intellectuelle. Il s'agit « [du] fait, pour la personne titulaire d'un accès à des services de communication au public en ligne (un accès à Internet), de ne pas veiller, de manière répétée, à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires de droits lorsqu'elle est requise ». En théorie, en cas de violations répétées de l'obligation de veille, l'abonné est puni par défaut de la suspension d'un an de son abonnement à Internet, et de l'impossibilité de souscrire un nouvel abonnement pendant cette période.

[Rz 10] Dans la pratique, il est prévu une riposte graduée[27]. La Haute Autorité peut intervenir en amont[28], notamment en adressant un courriel de rappel de l'obligation de veille à la première infraction et un courrier recommandé en cas de récidive dans les 6 mois. En cas de nouvelle récidive, une transaction peut être proposée par la Haute Autorité à l'internaute permettant à ce dernier de transformer la sanction d'un an en une sanction d'un à six mois[29].

[Rz 11] Ce deuxième avant-projet fait l'objet de critiques toujours plus nombreuses. Les juristes lui font grief de créer une insécurité juridique[30] et d'être tout simplement trop complexe. La censure du Conseil constitutionnel français, dont le rôle est notamment de garantir le principe de légalité en matière de droit pénal[31] s'annonce, si cet avant-projet ne fait pas l'objet d'importantes modifications, presque une étape obligée. Ce, d'autant que la possibilité accordée aux agents de l'État d'obtenir, sur simple demande, l'identité de l'internaute suspecté d'infractions a été maintenue[32]. Le texte a certes été toiletté (on parle désormais d'un « service instructeur » dont les agents ne sont plus « nommés » mais « habilités » par les ministères, etc.), mais fondamentalement, le principe est demeuré identique. Ce deuxième avant-projet devrait faire l'objet de nombreuses modifications, tant son caractère bancal est mis en exergue par tous les juristes. Il conviendra donc d'attendre la présentation du texte au Sénat, pour autant que celui-ci ne fasse pas l'objet d'un nouveau toilettage.

[Rz 12] Le 14 février 2008, le Ministre de l'Intérieur, Mme Michèle Alliot-Marie a présenté publiquement son **plan de lutte contre la cybercriminalité** dont le but est clairement d'accroître la sécurité[33]. Ce plan s'articule autour de quatre axes complémentaires. Il est proposé une modernisation globale des moyens d'investigations[34], la création de nouvelles formes d'incrimination (dont l'usurpation d'identité sur Internet[35]) et la possibilité d'astreindre les pirates dans le cadre de travaux d'intérêt général à mettre leurs compétences au service de la collectivité, la possibilité de conduire des perquisitions à distance[36] et, finalement l'amélioration du signalement des sites illicites[37].

[Rz 13] Ce plan suscite l'inquiétude, car on ignore pour l'heure le prix à payer en matière de restriction des libertés individuelles[38]. La plupart de ces dispositions, aussi ambitieuses que complexes à mettre en œuvre, entreront dans le cadre du projet de loi d'orientation et de programmation de la sécurité intérieure (LOPSI).

[Rz 14] En **Allemagne**, la problématique des cyberperquisitions[39] a retenu l'attention. La Cour constitutionnelle

---

25 Il ne s'agit toutefois que d'un nouveau projet d'étape.

26 EXCLUSIF - Qui obligera les FAI à filtrer les réseaux peer-to-peer ?

27 Nouvelle version par rapport à celle qui avait été formalisée auparavant dans la loi DADVSI.

28 Soit dès la constatation du premier manquement et avant l'ouverture de l'action publique.

29 Si l'abonné accepte cette transaction, et si elle est homologuée par le Procureur de la République, l'action pénale ne peut plus être engagée. En revanche si l'abonné refuse, la Haute Autorité peut mettre en mouvement elle-même l'action publique, mais l'abonné aura alors la possibilité de contester devant un juge la matérialité de l'infraction, et espérer ainsi annuler totalement la suspension.

30 Notamment quant à la définition même de l'infraction ; le terme « veiller » ne figurant dans aucun autre texte, son interprétation pourrait être soumise à un large arbitraire ; or, le principe de légalité impose des textes clairs et précis en matière pénale pour condamner quelqu'un.

31 Le Conseil est le juge de la conformité de la loi à l'ensemble des règles et principes à valeur constitutionnelle ; pour de plus amples informations voir « Les missions du Conseil ».

32 Les agents publics peuvent « notamment solliciter des opérateurs de communications électroniques l'identité du titulaire de l'abonnement utilisé à des fins [de contrefaçon] ».

33 « *Pour qu'il y ait de la liberté, il faut de la sécurité* », extrait de l'intervention du Ministre de l'intérieur.

34 Avec notamment d'extension de la conservation des données dont le délai sera alors d'un an, possibilité de captation à distance de données numériques sous le contrôle d'un juge, géo-localisation des utilisateurs d'internet.

35 Délit passible d'un an d'emprisonnement et de 15 000 euros d'amende.

36 Un renforcement de la coopération internationale sera, à cet égard, nécessaire.

37 Un site Internet de conseils et de prévention sera également créé en automne 2008. Son but sera de sensibiliser les internautes aux risques de la cybercriminalité et de permettre un signalement automatique et en temps réel de toute malversation constatée. Une plate forme européenne de signalement viendra compléter ce dispositif.

38 Pour de plus amples informations, cf. l'article de Me Philippe Wallaert intitulé «Un plan de lutte contre la cybercriminalité ambitieux et inquiétant ».

39 Soit les perquisitions en ligne.

allemande[40] a récemment (le 28 février 2008) annulé la loi en vigueur en Rhénanie du Nord-Westphalie sur les perquisitions en ligne[41]. La surveillance d'ordinateurs à distance ne sera possible qu'en cas de menaces concrètes contre des vies humaines ou contre l'État[42]. Un droit fondamental protège désormais la confidentialité et l'intégrité des systèmes techniques d'information en Allemagne. La loi de Rhénanie du Nord-Westphalie autorisait la police judiciaire (BKA) à s'introduire secrètement dans des ordinateurs personnels, au moyen de chevaux de Troie[43], afin d'y exercer des perquisitions. L'utilisation de ces perquisitions en ligne a été considérablement encadrée par le Tribunal constitutionnel. Elles seront admises, mais circonscrites, c'est-à-dire qu'elles ne pourront intervenir qu'en cas de « menace concrète » contre des vies humaines ou contre l'État (affaires de terrorisme). Par ailleurs, elles devront avoir été autorisées préalablement par un juge. De surcroît, les données recueillies lors de ces cyberperquisitions ne pourront pas être utilisées par la justice, si elles touchent à la vie privée des suspects. Les juges allemands ont tracé une limite raisonnable et pragmatique après avoir constaté que si, aujourd'hui, l'épanouissement de la personnalité de chacun s'effectue avec et via l'ordinateur et doit donc être, là aussi, protégée, on ne peut pas accepter que ces grands espaces de liberté soient utilisés par des criminels mettant en danger notre existence. Cet arrêt, considéré comme équilibré a été salué en Allemagne[44].

[Rz 15] L'**Angleterre** semble également vouloir adopter des dispositions légales du même type que les dispositions de riposte graduée que la France pourrait faire siennes à la suite du rapport Olivennes[45]. Le Gouvernement s'apprêterait en effet à publier un document consultatif sur un mécanisme de sanction visant à endiguer le téléchargement illégal sur Internet[46]. À la première infraction constatée, le fournisseur d'accès à Internet (FAI) enverrait un courriel d'avertissement à l'abonné suspecté de téléchargement illégal. Par la suite, si les symptômes venaient à persister, et une seconde infraction être avérée, la connexion serait alors suspendue. Enfin, ultime étape de la sanction, avant le recours aux tribunaux, la résiliation de l'abonnement pourrait intervenir au cas où le supposé pirate resterait de marbre face aux multiples injonctions reçues de la part de son FAI.

[Rz 16] Des projets de riposte graduée sont également annoncés au Japon et en Suède.

[Rz 17] Nous avons volontairement limité l'examen des développements récents intervenus chez nos voisins aux questions dont le caractère concernant est unanimement admis.

II. Bref survol des principales évolutions législatives et jurisprudentielles en Suisse dans le domaine d'Internet

[Rz 18] La Suisse peut, si l'on considère ce qui se passe actuellement chez nos voisins européens, être qualifiée de « havre de paix numérique ». Les dispositions légales n'y ont pas (encore) subi de modifications fondamentales avec des conséquences positives et négatives que nous allons discuter après la présentation du régime légal actuel.

a) La loi fédérale instituant des mesures visant au maintien de la sûreté intérieure

[Rz 19] Les **perquisitions en ligne** sans soupçon concret sont interdites jusqu'ici en Suisse. Cette question fait toutefois l'objet d'un examen dans le cadre de la révision de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI), loi qui est entrée en vigueur le 1er juillet 1998[47]. Cette loi vise à assurer le respect des fondements démocratiques et constitutionnels de la Suisse ainsi qu'à protéger les libertés de sa population[48]. Elle fait actuellement l'objet d'une révision en deux étapes[49]. La **première révision** , déjà achevée, concernait les mesures destinées à améliorer la lutte contre la propagande incitant à la violence et contre la violence lors de manifestations sportives (LMSI I). Les changements correspondants dans la LMSI sont entrés en vigueur en début 2007[50]. La **seconde révision** porte sur le renforcement de la sûreté intérieure par l'amélioration des mesures dans le domaine de la protection de l'État à titre préventif, notamment par la lutte contre le terrorisme. Cette seconde révision est désignée par l'abréviation LMSI II. Un

40 Bundesverfassungsgericht (BVerfG), soit la juridiction qui se prononce sur la conformité des lois avec la loi fondamentale de 1949 ; pour de plus amples informations : www.bverfg.de.

41 L'arrêt BVerfG, 1 BvR 370/07 du 27.02.2008.

42 Voir aussi NZZ du 20.03.08.

43 Programme malveillant qui, dissimulé à l'intérieur d'un autre programme en apparence inoffensif (par exemple un jeu ou un petit utilitaire), exécute des opérations nuisibles ou d'espionnage à l'insu de l'utilisateur.

44 Pour de plus amples informations, cf. Thomas Hoeren, Das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 zur Online-Durchsuchung, dans : Jusletter 3 mars 2008.

45 Cf. l'article du Times du 12 février 2008 y relatif.

46 Ce phénomène qui concernerait près de six millions d'abonnés au haut débit en Grande-Bretagne.

47 Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS 120).

48 Cf. message relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, p. 2, publié à la FF 2007 4773.

49 Étant précisé qu'une révision du Code pénal devrait en outre permettre d'introduire une mesure supplémentaire dans la lutte contre le racisme sous la forme d'une interdiction de port d'insignes racistes.

50 Le Conseil fédéral a décidé le 30 août 2006 de faire entrer en vigueur lesdites modifications le 1er janvier 2007. Ces dernières ont été adoptées par le Parlement lors de la session de printemps 2006, notamment en vue de l'UEFA EURO 2008 ; cf. à cet égard, la page spécifiquement consacrée au hooliganisme sur le site du Département fédéral de justice et police.

avant-projet a été établi par la Police fédérale (FEDPOL) le 31 janvier 2006 suivi d'un projet du Conseil fédéral publié le 15 juin 2007.

[Rz 20] Cet avant-projet de loi fédérale instituant des mesures visant au maintien de la sûreté intérieure[51] prévoit la perquisition secrète de systèmes informatiques, mais la mesure ne s'appliquerait qu'à titre exceptionnel, dans des conditions définies de manière stricte. L'article 18 de l'avant-projet limite tout d'abord le recours à des moyens spéciaux d'investigation (dont la perquisition secrète d'un système informatique) aux domaines du terrorisme, du service de renseignements politiques ou militaires prohibé, du commerce illicite d'armes et de substances radioactives ainsi que du transfert illégal de technologie. Le premier alinéa de la disposition indique que ces moyens spéciaux d'investigation doivent être utilisés pour déceler ou prévenir une menace concrète contre la sûreté intérieure ou extérieure.

[Rz 21] Il faut qu'avant d'utiliser des moyens spéciaux pour chercher à « déceler » ou à « prévenir » une menace, les organes de sûreté puissent déjà fonder des soupçons contre une personne, une organisation ou un groupement[52].

[Rz 22] Selon l'article 18n de l'avant-projet (intitulé perquisition secrète d'un système informatique), « *la perquisition secrète permet de rechercher, à l'insu du perturbateur présumé, des données enregistrées dans un système informatique, spécialement protégé contre tout accès indu, dont le perturbateur a la disposition, si des faits précis et récents permettent de supposer qu'il l'utilise pour y stocker des données qui servent son dessein* ».

[Rz 23] Sont concernées les données enregistrées électroniquement ou selon un mode similaire, qui sont spécialement protégées contre tout accès indu de tiers (champ d'application analogique à celui des articles 143 et 143 du Code pénal)[53]. La perquisition est ici, contrairement à celle opérée dans le cadre d'une enquête pénale, opérée à l'insu du perturbateur présumé[54]. La disposition ne permet toutefois qu'un hacking passif, ce qui signifie qu'il est proscrit d'implanter dans le système des éléments susceptibles de le bloquer, de le brouiller ou d'y détruire des données. Une telle atteinte à la sphère privée doit être justifiée par un intérêt public[55] et être proportionnée[56] au but visé (art. 36 Cst.). Aucun autre moyen[57] que celui de l'intrusion dans le système ne doit permettre de récolter lesdites informations. S'agissant de la procédure, il a été prévu qu'une Commission indépendante de contrôle des moyens spéciaux soit instituée (art. 18d de l'avant-projet), commission indépendante nommée par le Conseil fédéral. Le rôle de cette commission quasi judiciaire indépendante de l'administration serait notamment de contrôler que l'administration des moyens spéciaux requis soit conforme au droit. Le rapport explicatif expose les motifs pour lesquels, une telle commission a été préférée à une autorité judiciaire *stricto sensu*[58]. Nous y reviendrons ultérieurement compte tenu de l'importance de cette question. La Commission indépendante dispose de 72 heures pour délivrer son avis. Elle peut soit déclarer la demande non conforme au droit (avis négatif) ou la renvoyer à l'office fédéral pour complément d'information. Elle peut la déclarer totalement ou partiellement conforme au droit ou l'assortir de charges (avis positif). Si l'avis de la Commission est positif, l'Office soumet la demande de recherche spéciale d'informations au chef du département lequel est seul habilité à y donner suite (art. 18f al. 1 de l'avant-projet).

[Rz 24] Sur la base de l'avis de la Commission indépendante, le chef de département détermine le but, le perturbateur, les moyens et les charges (art. 18f alinéa 2 de l'avant-projet). Une procédure d'urgence a été prévue pour les cas où il y a péril en la demeure (art. 18g de l'avant-projet).

[Rz 25] Après la procédure de consultation, soit en avril 2007, le Conseil fédéral a mandaté le Département fédéral de justice et police (DFJP) aux fins d'élaborer un message[59] à l'intention du Parlement, respectivement de repréciser la nécessité du projet et d'examiner si les notions d'activités terroristes et d'extrémisme violent doivent figurer dans la loi. Le DFJP devait également, selon le mandat attribué par le Conseil fédéral, préciser plus clairement dans le message le processus de « double approbation » permettant d'ordonner la mise en œuvre de moyens spéciaux de recherche d'informations. L'avant-projet[60]avait en effet suscité

---

[51] Avant-projet et Rapport explicatif.

[52] Le rapport explicatif fait référence à cet égard à l'ATF 109 Ia 273, 288-289.

[53] Qu'adviendra-t-il si les données ne sont pas spécialement protégées, notamment dans un cas où les mesures élémentaires de sécurité n'ont pas été prises par le perturbateur présumé. Nous sommes d'avis que dans une telle hypothèse, le perturbateur devrait à tout le moins être informé de la surveillance spéciale, à moins que des intérêts publics prépondérants n'exigent le contraire. Il convient d'éviter l'absence de règles et, a fortiori, que les perquisitions soient opérées sans qu'une trace ne soit conservée, une grande partie des internautes n'ayant, statistiquement, pas pris les précautions visant à la sécurisation de leur système.

[54] Rapport explicatif, § 2.34, p. 60.

[55] Cf. à cet égard les explications détaillées figurant dans le rapport explicatif : §2.32, p. 57 ss et §2.9 p. 34 ss.

[56] Selon le rapport explicatif, § 2.34, p. 61, « dès lors qu'il est établi avec une certaine vraisemblance que le perturbateur présumé utilise un système et des réseaux informatiques pour stocker, pour lui-même ou à l'intention de tiers, des informations propres à constituer une menace concrète pour la sûreté intérieure ou extérieure, la perquisition d'un tel système est un moyen adéquat et nécessaire pour accéder auxdites données ».

[57] Classique tel que perquisition de locaux ou de véhicules ou l'observation physique. Il s'agirait en quelque sorte pour reprendre une locution bien connue des juristes de l'*ultima ratio*.

[58] Rapport explicatif, §2.23, p. 48 ss.

[59] Cf. message relatif à la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, publié à la FF 2007 4773.

[60] L'avant-projet avait déjà été remanié après une première consultation auprès des Offices en juillet 2005 ; une deuxième consultation est intervenue

de nombreuses critiques principalement en raison du choix d'une commission indépendante en lieu et place d'une autorité judiciaire[61], de l'absence de définition des notions de terrorisme et de l'extrémisme violent et de la procédure choisie pour ordonner et approuver les moyens spécieux de recherche. Il a notamment et principalement été décidé que la Commission indépendante serait remplacée par le Tribunal administratif fédéral[62]. La procédure de décision s'établit donc comme suit :

[Rz 26] L'utilisation de moyens spéciaux de recherche d'informations sera soumise à un double contrôle: à la demande de l'Office fédéral de la police, le Tribunal administratif fédéral examinera si les mesures sont conformes au droit (procédure d'autorisation). Dans le cadre de la décision rendue par le Tribunal administratif fédéral, le chef du DFJP et le chef du DDPS[63] examineront ensuite la demande sous l'angle politique et décideront d'un commun accord des mesures (procédure de décision). En cas de décision négative du Tribunal administratif fédéral, la procédure de décision sera annulée.

[Rz 27] La personne visée devra être informée ultérieurement qu'elle a fait l'objet d'une surveillance spéciale, sauf dans des cas précis où des intérêts publics prépondérants l'exigent et où la protection de tiers serait compromise. Le Tribunal administratif fédéral ou les chefs du DFJP et du DDPS déterminent les exceptions à l'obligation de communiquer dans le cadre d'une procédure analogue à celle applicable lors de l'emploi de moyens spéciaux de recherche d'informations (procédure d'approbation ou procédure de décision).

[Rz 28] Le message élaboré par le DFJP a été transmis par le Conseil fédéral au Parlement le 15 juin 2007. Le Conseil fédéral sollicitait à son terme l'approbation du projet[64] de révision de la loi fédérale instituant des mesures visant au maintien de la sécurité intérieure. S'agissant des points litigieux déjà évoqués, il convient de préciser ce qui suit :

- Bien que sollicitée par différents participants à la consultation, l'extension du champ d'application des recherches spéciales d'information à l'extrémisme violent, au service de renseignements économiques et à la criminalité organisée a été écartée. En matière de la lutte contre la criminalité organisée, le Conseil fédéral estime qu'il faut d'abord attendre les résultats du projet d'efficacité[65].
- La procédure d'approbation (art. 18d du projet) est ainsi décrite :[[[List-Break]]]
- « L'Office fédéral de la police dépose une demande écrite dûment motivée, sur la base de laquelle le Tribunal administratif fédéral vérifie les mesures demandées (procédure d'approbation). C'est seulement une fois que le Tribunal administratif fédéral a approuvé la mesure que le chef du DFJP examine la demande, consulte le chef du DDPS et, en cas d'accord réciproque, décide de façon définitive d'ordonner l'exécution de la mesure (procédure de décision). La demande est donc soumise à un examen judiciaire, et à un examen (double lui aussi) portant sur différents points relevant de la politique de l'État (effectué par le pouvoir exécutif). L'utilisation de moyens spéciaux de recherche d'informations n'est autorisée que si et dans la mesure où toutes les instances donnent leur accord »[66]. La procédure a été consolidée par rapport à celle soumise à la consultation et elle est désormais plus claire comme la description ci-avant permet de le constater.
- La procédure de décision (art. 18e du projet) a également fait l'objet de précisions importantes. Ainsi, il est désormais expressément mentionné que la décision doit être prise dans les limites de la décision du Tribunal administratif fédéral, qui sera en conséquence jointe à la demande[67]. La décision (politique) prise par le chef du DFJP et le chef du DDPS doit l'être d'un commun accord. À défaut, même en cas d'approbation par le Tribunal administratif fédéral, l'utilisation des moyens spéciaux ne peut être ordonnée.
- En ce qui concerne l'obligation de communiquer, il a été prévu que lorsqu'une opération est terminée, l'Office fédéral de la police doit, en principe, communiquer à la personne concernée dans un délai d'un mois qu'elle a fait l'objet de recherches. Selon le Conseil fédéral, il n'est pas possible d'étendre l'obligation de communiquer à la recherche générale d'informations ou à toutes les personnes visées par la surveillance, comme certains participants l'avaient souhaité. Ce choix est motivé par le souci d'éviter des lourdeurs administratives et par la difficulté d'identifier toutes les

auprès des Offices en février 2006 avant une plus large consultation organisée par le DFJP du 5 juillet au 15 octobre 2006 ; c'est dire le caractère sensible du sujet.

61 Cf. à cet égard le rapport du 30 janvier 2007 sur le résultat de la consultation relative à la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure et l'avis du Préposé fédéral à la protection des données et à la transparence.

62 Selon toute vraisemblance, l'abandon du choix de la commission indépendante de contrôle des moyens spéciaux (commission quasi judiciaire indépendante de l'administration) au profit du Tribunal administratif fédéral est intervenu entre la publication de l'avant-projet de la FEDPOL (31 janvier 2006) et la période de consultation qui a débuté en juillet 2006 ; les motifs ne ressortent pas du rapport sur les résultats de la consultation, ni d'une autre publication, ce qui est inhabituel.

63 Abréviation du Département fédéral de la défense, de la protection de la population et des sports.

64 FF 2007 4873.

65 Message, §3a, ad article 18a, p. 4831.

66 Message, §3a, ad article 18d, p. 4835.

67 Message, §3a, ad article 18e, p. 4835.

personnes supplémentaires dont celles présentes par hasard[68].[[[List-Break]]]

- Relevons finalement relativement à cette problématique que toutes les questions n'ont pas été résolues, le Conseil fédéral proposant (sic !) que[69] « dans la mesure du nécessaire, le département abordera cette problématique lors des délibérations aux Chambres sur la présente révision et proposera des solutions ».
- La **perquisition secrète d'un système informatique** a également fait l'objet de certaines précisions intéressantes[70]. Le message cite tout d'abord quelques exemples, soit la recherche d'adresses dans l'ordinateur portable d'un perturbateur présumé ou le décodage d'un courriel chiffré, qui aurait pu être constaté, mais pas être mis en évidence, lors d'une surveillance autorisée de la correspondance. Le message fait également état de la propagande de nature djihadiste qui s'impose, selon le Conseil fédéral, comme un champ d'application concret.

[Rz 29] Le message comporte encore nombre d'inconnues sur des questions centrales qui vont certainement susciter un vif débat au Parlement. Pour l'heure, le projet de loi est soumis à l'examen des différentes commissions des affaires juridiques (du Conseil national et du Conseil des États)[71].

b) La lutte contre la cybercriminalité[72]

[Rz 30] Cette épineuse question a fait l'objet de nombreuses études et interventions diverses pour aboutir, le 22 février 2008, à une annonce du Conseil fédéral[73] qui a surpris plus d'un observateur. Auparavant[74], une commission d'expert baptisée « cybercriminalité » avait été désignée avec pour but d'élaborer des solutions visant à régler la question de la responsabilité pénale des différents prestataires pour les contenus illégaux véhiculés sur le réseau[75]. En automne 2002, suite à l'opération baptisée «Genesis», le DFJP a chargé l'Office fédéral de la police de formuler - de concert avec des représentants des autorités policières et judiciaires ainsi que des autorités de poursuite pénale - des propositions visant à améliorer la collaboration entre la Confédération et les cantons en matière de lutte contre la cybercriminalité[76].

[Rz 31] Le 10 décembre 2004, le DFJP mettait en consultation deux projets de loi[77]. L'un visait à réglementer spécifiquement la responsabilité pénale des différents prestataires Internet pour les contenus illégaux véhiculés sur le réseau. L'autre avait pour but de doter les autorités fédérales de nouvelles compétences en matière d'investigation.

[Rz 32] Le **premier projet**[78] (également intitulé avant-projet A) prévoyait que le fournisseur de contenus soit toujours punissable en tant qu'auteur des contenus illégaux qu'il publie sur Internet. Quant au fournisseur d'hébergement, c'est-à-dire celui qui met à la disposition de ses clients (les fournisseurs de contenus) une certaine capacité de mémoire, il était également passible de sanctions pénales, en tant que coauteur, instigateur ou complice, lorsqu'il tolérait intentionnellement que l'on charge sur son serveur des informations illégales. Toutefois, s'il apprenait, ultérieurement, que les données stockées sur son serveur constituaient des contenus illégaux, il n'était punissable que s'il omettait d'en prévenir l'utilisation ou de transmettre aux autorités de poursuite pénale les avertissements qui lui auront été adressés à ce propos par des tiers. Finalement, le fournisseur d'accès était également punissable en tant que coauteur, instigateur ou complice, s'il avait participé activement à l'infraction commise par le fournisseur de contenu. En revanche, s'il s'était limité à assurer l'accès de l'utilisateur à Internet selon un procédé entièrement automatisé, il devait être exempté de toute sanction pénale.

[Rz 33] Le **deuxième projet**[79] (également intitulé avant-projet B) avait quant à lui pour but d'améliorer les modalités de la collaboration entre autorités fédérales et autorités cantonales en matière de poursuite des auteurs d'infractions relevant de la cybercriminalité. Il s'agissait de cas dans lesquels il n'a pas encore été possible de déterminer le canton ou les cantons compétents pour conduire la poursuite pénale parce que les auteurs présumés n'ont pas encore été identifiés. Pour garantir que de telles infractions soient poursuivies rapidement et avec toute l'efficacité voulue, il avait été prévu que le Ministère public de la Confédération et la Police judiciaire fédérale aient la compétence de procéder aux premières investigations urgentes. En outre, il était stipulé dans ce projet que la Police judiciaire fédérale a un droit exprès d'adresser des

68 Message, §3a, ad article 18i, p. 4839.

69 Message, §3a, ad article 18i, p. 4840.

70 Message §3a, ad article 18m, p. 4845.

71 Pour de plus amples informations, cf. le site de la commission.

72 Soit les actes pénalement répréhensibles qui sont commis au moyen des technologies de l'information et des réseaux de communication électroniques.

73 Renforcer l'efficacité de la lutte contre la cybercriminalité – Le Conseil fédéral augmente les ressources disponibles et intensifie la collaboration internationale.

74 Par décision du DFJP du 22 novembre 2001.

75 Rapport rendu par cette commission « cybercriminalité ».

76 Propositions formulées par le groupe de travail.

77 Cf. à cet égard le Rapport à l'appui d'avant-projets de modification du Code pénal suisse et du Code pénal militaire concernant la responsabilité pénale des prestataires et les compétences de la Confédération relatives à la poursuite des infractions commises par le canal des médias électroniques (cybercriminalité).

78 Inspiré principalement par les travaux de la commission d'expert « cybercriminalité ».

79 Inspiré quant à lui des travaux du groupe de travail « Genesis » institué par le DFPJ en 2002.

instructions aux autorités cantonales de poursuite pénale, cela afin de coordonner l'exécution des enquêtes.

[Rz 34] La procédure de consultation[80] relative à ces deux projets de loi a duré plus d'un an et la synthèse des résultats a rapidement permis de constater l'existence de fortes résistances principalement en ce qui concernait le premier projet. Le Conseil fédéral a rendu en février 2008 un rapport[81] intitulé « Cybercriminalité, Responsabilité pénale des prestataires et compétences de la Confédération en matière de poursuite des cyberinfractions », rapport au terme duquel il parvient à différentes conclusions[82] dont celles-ci s'agissant du **premier projet** (avant-projet A) :

- Le premier projet a donné lieu à de vives controverses. Après avoir diligenté des études complémentaires au terme de la procédure de consultation, il apparaît que les modifications proposées ne permettraient pas de mettre fin à l'insécurité juridique, mais seraient au contraire sources de nouvelles incertitudes.
- La jurisprudence rendue depuis l'année 2001 démontre que le risque évoqué, par le passé, de jugements contradictoires ne s'est pas réalisé. De surcroît, les entreprises suisses n'ont pas subi d'inconvénients de concurrence et de localisation. L'absence de réglementation expresse des responsabilités n'a pas non plus nui à la lutte contre la cybercriminalité.
- Une réglementation d'une nature plus technique serait vite dépassée compte tenu de l'évolution rapide qui caractérise les cyberréseaux. Mieux vaut donc en rester aux réglementations générales qui sont bien connues.

[Rz 35] Le Conseil fédéral est donc d'avis que « *puisque le régime en vigueur n'a encore induit aucune conséquence négative pour les prestataires pas plus qu'il n'a eu de répercussions fâcheuses en matière de poursuites pénales, même au bout de plusieurs années, force est de conclure qu'il n'y a pas lieu de légiférer* ». Il recommande logiquement au Parlement de renoncer à une réglementation explicite de la responsabilité pénale des prestataires.

[Rz 36] Le **deuxième projet** a reçu un accueil plus enthousiaste. Il est toutefois devenu sans objet depuis l'adoption du Code de procédure pénale suisse (abrégé CPP)[83]. L'article 27 alinéa 2, CPP statue une compétence de la Confédération de procéder aux premières investigations en cas d'infractions qui ont été commises, en tout ou partie, dans plusieurs cantons ou à l'étranger et pour lesquelles la compétence de la Confédération ou d'un canton n'est pas encore déterminée. Cette compétence s'étend à toutes les infractions, ce qui règlera bien des problèmes.

[Rz 37] Se fondant sur les constatations énoncées dans son rapport, le Conseil fédéral est d'avis[84] que l'accent doit être mis sur un renforcement de la surveillance des activités déployées sur Internet[85] et sur une ratification de la Convention nº 185 du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001[86]. Selon le Conseil fédéral, le droit suisse satisfait dans une large mesure aux exigences posées par cette convention en matière de lutte contre les infractions commises par le canal des médias électroniques. La nécessité d'adapter les normes du code pénal et du code de procédure pénale pour les rendre compatibles avec cette convention fait actuellement l'objet d'un examen approfondi. Le processus de mise en œuvre de cet instrument international est donc, d'ores et déjà, entamé.

[Rz 38] Rappelons tout de même que la Convention sur la cybercriminalité date de 2001 et que la doctrine[87] a régulièrement invité les autorités politiques à ratifier cette convention en mettant en exergue le fait que bien qu'elle soit imparfaite, elle avait tout de même le mérite de traiter des perquisitions informatiques transnationales et de mettre sur pied un système d'entraide policière et judiciaire dont la plus grande efficacité devrait diminuer la tentation du recours à des moyens critiquables[88].

[Rz 39] À titre personnel, la position du Conseil fédéral ne peut emporter l'adhésion. La cybercriminalité est en constante mutation et le nombre de victimes de nouvelles infractions ne cesse de croître. Citons, à titre exemplatif, l'usurpation d'identité numérique qui fait l'objet d'une incrimination dans le plan français de lutte contre la cybercriminalité. Actuellement, ce comportement ne paraît pas punissable en tant que tel en droit suisse. Or, il devient récurrent et, si une autre norme[89] n'est pas violée, pourrait demeurer impuni. Les conséquences peuvent toutefois être considérables tant sur le plan personnel que patrimonial, comme dans le cas de ce mari et père de famille dont un internaute avait usurpé l'identité pour s'inscrire sur un site de rencontres étranger. Sa femme ayant découvert ce qu'elle croyait être une trahison demanda le divorce et le mari dut se contenter des excuses de l'auteur et

---

80 Cf. la synthèse des résultats de la procédure de consultation de février 2006.

81 Rapport du Conseil fédéral.

82 Rapport du Conseil fédéral, § 3.1, p. 7 et 8.

83 Publié à la FF 2007 6583.

84 Cf. communiqué de presse du 28 février 2008.

85 Principalement dans le domaine du terrorisme. Pour le Conseil fédéral: « Seule une surveillance systématique de ces sites est de nature à permettre aux autorités de prendre à temps les mesures préventives ou répressives qui s'imposent pour prévenir des attentats terroristes contre la Suisse ou contre des ressortissants suisses à l'étranger » ; on ignore toutefois quels seront les moyens réellement supplémentaires à disposition.

86 Convention sur la cybercriminalité; Rapport explicatif.

87 Notamment Jean Treccani, Internet et souveraineté, in : L'individu face aux nouvelles technologies, Surveillance, identification et suivi, Schultess 2005, p. 109.

88 Jean Treccani, *loc. cit.*, p. 109.

89 Notamment celles en matière de protection de l'honneur ou du patrimoine.

d'une somme modeste sur le plan civil à l'aune des souffrances ressenties et des conséquences patrimoniales subies (appauvrissement consécutif au divorce).

III. Protection des données et droit d'auteur

[Rz 40] Les législations en matière de protection des données[90] et de droit d'auteur[91] ont fait l'objet de modifications importantes récemment entrées en vigueur[92]. Compte tenu de la complexité et de l'ampleur du sujet, nous limiterons notre analyse à un cas où les normes en matière de droit d'auteur et de protection des données trouvent application simultanément.

[Rz 41] Le Préposé fédéral à la protection des données et à la transparence (en abrégé : PFPDT) s'est récemment prononcé sur la problématique de la traque des internautes en vue d'assurer la défense des intérêts des détenteurs de droits d'auteur. Il a émis une recommandation[93] extrêmement instructive, étant immédiatement précisé que celle-ci n'ayant pas été suivie d'effets, le Tribunal administratif fédéral sera conduit à se prononcer sur cette affaire[94]. En substance, il s'est agi d'examiner si les recherches effectuées dans les réseaux P2P dans le but de déceler des violations du droit d'auteur commises au sein des sites d'échange de fichiers musique et vidéo sur Internet étaient ou non licites. Une entreprise dont le siège se trouve en Suisse a développé un logiciel spécial qui lui permet de déceler de manière automatisée les œuvres protégées par le droit d'auteur qui sont illégalement proposées pour téléchargement dans des réseaux P2P. Le logiciel en question essaie alors de télécharger les contenus concernés et enregistre les traces électroniques laissées par l'utilisateur du logiciel P2P mettant à disposition les œuvres protégées. Ces données – enregistrées à l'insu des personnes concernées, y compris du détenteur de l'accès Internet qui peut être de bonne foi – sont communiquées périodiquement à l'étranger aux détenteurs des droits d'auteur de l'œuvre concernée ou à leurs représentants légaux[95]. Le PFPDT a examiné le caractère licite du traitement de données à l'aune des principes applicables en cette matière. S'agissant du **principe de licéité**[96], le Préposé est d'avis qu'un tel traitement de données (soit la collecte systématique des adresses IP dans des réseaux P2P) doit faire l'objet d'une base légale explicite en raison du fait que le traitement a lieu à l'insu des personnes concernées, de manière proactive et dans le but ultérieur d'introduire des procédures pénales. La base légale devrait également régler la question de la valeur probante des données ainsi collectées ainsi que leur admissibilité en tant que preuves. Le **principe de finalité**[97] est également violé en raison du but poursuivi (la traque des violations du droit d'auteur) non conforme au but initial des réseaux P2P (l'échange de contenus). Ce changement de finalité ne figure dans aucune loi et n'est pas reconnaissable pour les détenteurs du logiciel et les titulaires de l'adresse IP.

[Rz 42] Le **principe de la bonne foi**[98] n'est également pas respecté dans le cadre de cette collecte de données. De ce principe découle celui de la transparence, selon lequel un traitement de données doit être reconnaissable pour la personne concernée[99]. Or, en l'occurrence, la collecte de données a lieu à l'insu de toutes les personnes concernées (détenteur de l'accès Internet ou la personne mettant effectivement à disposition les fichiers protégés) et elle doit donc être qualifiée de collecte secrète. En déposant une plainte pénale dans le seul but de constater l'identité du détenteur de l'accès Internet afin de faire ensuite valoir des prétentions civiles envers ce dernier, les détenteurs des droits d'auteur ou leurs représentants légaux contournent le secret des télécommunications valable dans le domaine civil et commettent un **abus de droit**. Cette démarche doit être considérée comme contraire au principe de la bonne foi, dans la mesure où le droit d'accès au dossier est utilisé pour revendiquer des dommages-intérêts à un détenteur d'accès Internet qui peut être de bonne foi, ceci souvent sans même attendre la fin de la procédure pénale et la condamnation de ce dernier (et donc sans savoir si celui-ci a effectivement commis une infraction au droit d'auteur). Le Préposé ajoute qu'il lui paraît contraire au secret des télécommunications d'accéder à l'identité du détenteur de l'adresse IP sans qu'une base légale ne le prévoie expressément[100]. Relativement au respect du **principe de proportionnalité**, il précise que les ayant droits peuvent faire valoir leurs prétentions en dommages-intérêts à l'égard de la personne ayant commis l'infraction au droit d'auteur par la voie d'une action civile jointe à l'action pénale et que ce n'est que dans ces conditions que le principe est respecté.

[Rz 43] Après être parvenu à la conclusion que les principes

[90] Pour de plus amples informations, cf. les explications disponibles sur le site du Préposé fédéral à la protection des données et à la transparence.

[91] Pour un résumé de la procédure d'adoption des nouvelles dispositions légales et de leur contenu, cf. la page du site de l'Institut fédéral de la Propriété Intellectuelle (IPI) y consacrée et sur le site spécialement développé dans le cadre de la révision du droit d'auteur.

[92] Au 1er janvier 2008 pour les modifications de la loi fédérale sur la protection des données à l'exception de l'article 17a et à une date à déterminer par le Conseil fédéral pour la loi fédérale sur le droit d'auteur, étant précisé que le délai référendaire est venu à échéance le 24 janvier 2008.

[93] Résumé de la recommandation.

[94] En conformité avec l'article 29 alinéa 4 LPD.

[95] Cf. résumé de la recommandation, p. 1.

[96] Article 4 al. 1 LPD.

[97] Article 4 al. 3 LPD.

[98] Art. 4 al. 2 LPD.

[99] En d'autres termes, la personne concernée doit en être informée ou elle doit s'y attendre au vu des circonstances.

[100] Il n'existe en effet aucun pendant civil à la loi fédérale sur la surveillance de la correspondance par poste et télécommunication.

fondamentaux en matière de protection des données n'étaient pas respectés et avoir mis en exergue une atteinte à la personnalité au sens de l'art. 12 LPD, le Préposé examine si un **motif justificatif** au sens de l'article 13 LPD existe. Selon l'art. 13 al. 1 LPD, une atteinte à la personnalité n'est pas illicite si elle peut être justifiée par le consentement de la victime, par un intérêt privé ou public prépondérant ou par la loi. Les personnes concernées n'étant pas informées et n'ayant de ce fait pas pu consentir au traitement de données et aucun intérêt public ne pouvant être invoqué (ni l'existence d'une base légale), seule demeure ouverte la question de l'intérêt privé prépondérant. Dans la mesure où la démarche de collectes constitue un contournement du secret des télécommunications dans le domaine civil et que cette pratique porte atteinte aux droits de la personnalité d'un nombre indéfini de détenteurs d'accès Internet qui sont de bonne foi, l'engagement d'une procédure pénale ne peut dans ce cas pas être considérée comme un motif justificatif suffisant tant qu'il n'est pas garanti que les identités des détenteurs d'accès Internet qui sont de bonne foi soient protégées dans le cadre d'une procédure pénale. En conclusion, il n'existe pas de motif justificatif, raison pour laquelle une recommandation est émise à l'endroit de la société visant à ce que celle-ci mette fin immédiatement au traitement de données qu'elle effectue. Le PFPDT défend le point de vue qu'une telle atteinte au secret des télécommunications nécessite une base légale dans le domaine civil, le législateur n'ayant pas souhaité octroyer de renseignements dans le cadre de prétentions civiles[101].

[Rz 44] La société concernée ayant communiqué au Préposé son intention de ne pas se soumettre à la recommandation émise, le Tribunal administratif fédéral devra se prononcer.

[Rz 45] À notre sens, il s'agit de la meilleure solution pour tous les acteurs de ce marché, dans la mesure où une jurisprudence bien établie sera toujours préférable à une recommandation[102] fut-elle de la qualité de celle émise par le PFPDT dans le cas d'espèce. À cet égard, la jurisprudence rendue dans l'affaire Promusicae[103] par la Cour de justice des Communautés européennes pourrait constituer la pierre angulaire de la réflexion du Tribunal administratif fédéral.

IV. Conclusion et droit désirable

[Rz 46] En matière de **droit d'auteur,** la solution helvétique même si elle est encore source d'incertitudes[104] et d'inégalités a le mérite de ne pas évoluer au gré des intérêts partisans et des interventions politiques comme cela est le cas, actuellement, en France. On ne peut que stigmatiser l'effervescente agitation de nos voisins français qui conduit, à force de nouvelles normes, pour la plupart inapplicables, à un chaos législatif et judiciaire. Il s'agit du parfait exemple où Internet est devenu le **terreau de solutions juridiques destructrices**, ne satisfaisant personne et en totale inadéquation avec la réalité économique du monde numérique. Aujourd'hui, les acteurs certainement échaudés par les changements continus de régime juridique sont, semble-t-il, mûrs pour envisager l'introduction d'une licence globale[105]. Cette licence globale représente aux yeux de tous (partisans comme adversaires) une solution juridique **novatrice**. Ses opposants soutiennent que la clé de répartition des montants ainsi collectés demeure le problème principal. Ils devront toutefois le résoudre seuls, notamment dans le cadre de la célèbre affaire Napster où malgré les sommes obtenues, la répartition n'a pas encore eu lieu entre les détenteurs de droits. Il faut toutefois admettre que le vif débat qui a lieu en France n'a pas son pendant en Suisse. Lors de la modification des normes en matière de droit d'auteur, seules quelques voix se sont élevées pour soit critiquer le nouveau régime légal, soit proposer d'autres alternatives. Nous ne sommes certes pas un pays où la production représente une part importante de notre économie, mais cette absence d'échanges sur une question aussi fondamentale nuit à l'adoption future de normes garantes des intérêts de chacun (auteurs et consommateurs).

[Rz 47] Notre pays s'est cependant montré exemplaire dans le domaine de la traque des internautes par les représentants des titulaires de droit d'auteur.

[Rz 48] En cette matière complexe[106], les internautes qui ont le droit de savoir ce qu'il advient de leurs données personnelles ont bénéficié d'une réaction aussi salutaire qu'efficace des services du PFPDT. Comment pourrait-on autoriser des sociétés privées dont les sièges varient régulièrement au gré des intérêts économiques et fiscaux à se substituer à l'État sans qu'aucune garantie ne soit fournie au citoyen. Espérons que les hommes politiques qui pourraient être sollicités pour l'établissement d'une base légale formelle autorisant cette traque percevront le danger que représente la collecte de données aussi sensibles. Les progrès réalisés permettent aujourd'hui d'affirmer qu'une utilisation malveillante est possible et que rien ni personne ne pourra garantir que ces données représentant pour certaines une valeur économique

[101] La voie de l'action de droit civil étant ouverte dans une telle hypothèse.

[102] Non contraignante faut-il le rappeler.

[103] La récente décision de la Cour de justice des Communautés européennes dans l'affaire Promusicae stipule notamment que l'adresse IP est une donnée personnelle ; cette décision est disponible sur le site de la Cour : http://curia.europa.eu.

[104] Aucune décision n'ayant été rendue à ce jour et à notre connaissance, en matière de téléchargements de fichiers sur des bourses d'échanges. La majorité de la doctrine part toutefois du principe que le téléchargement à usage privé, assimilable à une copie privée, est admis selon le droit en vigueur. Il est par contre prohibé de mettre des fichiers à la disposition d'autres utilisateurs sur le disque dur de son propre ordinateur, à savoir de télédécharger (« upload ») des contenus protégés par des droits d'auteurs.

[105] Le système de licence globale permet aux internautes de télécharger librement et gratuitement en échange d'une indemnité forfaitaire.

[106] Et même si le Tribunal administratif fédéral ne s'est pas encore prononcé.

importante ne seront pas transférées puis traitées dans un État moins soucieux des grands principes applicables en matière de **protection des données**. La plus grande prudence s'impose donc.

[Rz 49] À défaut, il serait possible à un simple quidam muni d'un logiciel spécialisé[107] de s'instaurer en « magistrat instructeur du Net », alors que pour des questions aussi sensibles que la **sécurité intérieure**, d'aucuns s'opposent à ce que la police (bien que devant respecter des conditions légales expresses) puisse exercer une surveillance. Le projet présenté au Parlement fédéral n'est certes pas encore mûr, mais il répond à un besoin incontestable. La récente décision de la Cour constitutionnelle allemande en matière de **cyberperquisitions** répond à nombre d'interrogations et pourrait ainsi inspirer la résolution de cette épineuse question. L'affaire des fiches est encore bien présente dans tous les esprits et seule une procédure transparente sera à même d'emporter l'adhésion des citoyens de notre pays. Dans ce domaine également il conviendra d'être inspiré et novateur.

[Rz 50] Finalement, la lutte contre la **cybercriminalité** est le parent pauvre de l'évolution normative dans notre pays contrairement à ce qui se passe en France notamment. Après avoir sollicité des avis d'experts, envisagé des solutions diverses, le Conseil fédéral a opté pour un statu quo **destructeur**. Qui n'a pas eu connaissance des mésaventures d'un ami, d'un parent qui s'est fait « arnaquer » sur Internet ? Qui n'a pas hésité quant au comportement à adopter à la lecture d'un courriel au contenu aguicheur ? Le manque de courage politique et de vision à long terme[108] ne saurait masquer les carences du droit actuel. Certains comportements sont impunis, d'autres difficilement punissables. La solution boiteuse adoptée aura un coût, pour l'internaute principalement. Même si la question de la responsabilité ne peut être résolue à la satisfaction de tous, il eut été possible, à l'instar de nos voisins français de mettre en place différents outils visant à restaurer la confiance du consommateur dans l'économie numérique. Ainsi, un observatoire de la cybercriminalité aurait pu être créé avec son pendant sur Internet, à savoir un site de conseils et de prévention, site constamment mis à jour et qui aurait pu recenser les principales arnaques et les principaux problèmes. L'internaute s'y serait adressé comme à un référent en cas de doute, ce qui aurait également permis de réunir les forces en présence.

[Rz 51] Cet observatoire composé d'experts de différents milieux (administration, police, justice, consommateurs, prestataires techniques, etc.) aurait régulièrement formulé à l'intention de l'autorité politique des propositions, visant, dans un deuxième temps à accroître l'efficacité de l'appareil législatif et répressif. Il eût également été possible de formuler de nouvelles normes pénales, technologiquement neutres, visant à sanctionner les nouveaux types de criminalité. Cette tâche, accomplie par nos voisins, n'était pas insurmontable pour peu que l'on prenne la peine de procéder différemment. La tâche à accomplir est importante, mais, inspiré par les solutions adoptées par les autres pays européens, le Conseil fédéral se devait d'éviter de cristalliser notre régime juridique en cette matière et de reporter à demain ce qui aurait dû être réglé aujourd'hui.

Sébastien Fanti, avocat notaire, à Sion est spécialisé en droit des réseaux informatiques.

---

* * *

[107] Dont le développement est un jeu d'enfant pour un informaticien.

[108] Il aura fallu 7 ans pour que le Conseil fédéral décide de ratifier la Convention sur la cybercriminalité.