E.U. NETWORK OF INDEPENDENT EXPERTS ON FUNDAMENTAL RIGHTS
(CFR-CDF)
RÉSEAU U.E. D'EXPERTS INDÉPENDANTS EN MATIÈRE DE DROITS FONDAMENTAUX

Avis sur la protection de la vie privée sur Internet vis-à-vis des systèmes de protection des droits de propriété intellectuelle.

1er décembre 2003

Référence : CFR-CDF.avis4-2003

Le **Réseau UE d'Experts indépendants en matière de droits fondamentaux** a été mis sur pied par la Commission européenne (DG Justice et affaires intérieures), à la demande du Parlement européen. Depuis 2002, il assure le suivi de la situation des droits fondamentaux dans les Etats membres et dans l'Union, sur la base de la Charte des droits fondamentaux de l'Union européenne.

Le Réseau UE d'Experts indépendants en matière de droits fondamentaux se compose de Elvira Baltutyte (Lithuanie), Florence Benoît-Rohmer (France), Martin Buzinger (Rép. slovaque), Achilleas Demetriades (Chypre), Olivier De Schutter (Belgique), Maja Eriksson (Suède), Teresa Freixes (Espagne), Gabor Halmai (Hongrie), Wolfgang Heyde (Allemagne), Morten Kjaerum (Danemark), Henri Labayle (France), M. Rick Lawson (Pays-Bas), Lauri Malksoo (Estonie), Arne Mavcic (Slovénie), Vital Moreira (Portugal), Jeremy McBride (Royaume-Uni), Bruno Nascimbene (Italie), Manfred Nowak (Autriche), Marek Antoni Nowicki (Pologne), Donncha O'Connell (Irlande), Ian Refalo (Malte), Martin Scheinin (suppléant Tuomas Ojanen) (Finlande), Linos Alexandre Sicilianos (Grèce), Dean Spielmann (Luxembourg), Pavel Sturma (Rép. tchèque), Ineta Ziemele (Lettonie). Le Réseau est coordonné par O. De Schutter.
Les documents du Réseau peuvent être consultés via :
http://www.europa.eu.int/comm/justice_home/cfr_cdf/index_fr.htm

The **EU Network of Independent Experts on Fundamental Rights** has been set up by the European Commission (DG Justice and Home Affairs), upon request of the European Parliament. Since 2002, it monitors the situation of fundamental rights in the Member States and in the Union, on the basis of the Charter of Fundamental Rights.

The EU Network of Independent Experts on Fundamental Rights is composed of Elvira Baltutyte (Lithuania), Florence Benoît-Rohmer (France), Martin Buzinger (Slovak Republic), Achilleas Demetriades (Cyprus), Olivier De Schutter (Belgium), Maja Eriksson (Sweden), Teresa Freixes (Spain), Gabor Halmai (Hungary), Wolfgang Heyde (Germany), Morten Kjaerum (Denmark), Henri Labayle (France), M. Rick Lawson (the Netherlands), Lauri Malksoo (Estonia), Arne Mavcic (Slovenia), Vital Moreira (Portugal), Jeremy McBride (United Kingdom), Bruno Nascimbene (Italy), Manfred Nowak (Austria), Marek Antoni Nowicki (Poland), Donncha O'Connell (Ireland), Ian Refalo (Malta), Martin Scheinin (substitute Tuomas Ojanen) (Finland), Linos Alexandre Sicilianos (Greece), Dean Spielmann (Luxemburg), Pavel Sturma (Czeck Republic), Ineta Ziemele (Latvia). The Network is coordinated by Olivier De Schutter.
The documents of the Network may be consulted on :
http://www.europa.eu.int/comm/justice_home/cfr_cdf/index_en.htm

Table des matières

Introduction

Le présent avis aborde la question de savoir quelle est la protection des données à caractère personnel de l'internaute au regard de l'emploi, par les détenteurs de droits de propriété intellectuelle sur des matériaux accessibles via Internet, de technologies permettant l'identification de personnes ayant accès à ces matériaux. Selon le vœu de la Commission, une attention particulière a été portée à la question des données de trafic, et plus spécifiquement à la durée autorisée de leur conservation ainsi qu'aux avis rendus par les autorités nationales de contrôle de la protection des données.

La question suivante a été adressée aux Experts indépendants du Réseau :

Décrivez les réglementations nationales concernant la protection de données à caractère personnel des utilisateurs d'Internet, en particulier au regard de l'emploi par les détenteurs de droits de propriété intellectuelle sur des matériaux accessibles via Internet de technologies permettant l'identification des personnes y ayant accès. Veuillez identifier toutes règles pertinentes concernant la rétention des données de trafic ainsi que tout avis de l'autorité indépendante de contrôle en matière de protection des données.

Les experts d'Autriche, de Belgique, de Chypre, du Danemark, de Finlande, d'Allemagne, de Grèce, d'Irlande, d'Italie, du Luxembourg, de Malte, du Portugal, d'Espagne, de Suède, des Pays-Bas et du Royaume-Uni ont examiné cette question[1]. **Le présent avis couvre ainsi 16 Etats membres.**

Ces analyses nationales figurent en annexe. Elles sont précédées d'une description du cadre juridique dans lequel doit s'inscrire la conciliation à assurer entre les droits de propriété intellectuelle des auteurs ou de leurs cessionnaires d'une part, et le droit la protection des données à caractère personnel de l'utilisateur d'Internet d'autre part.

Le cadre juridique I. La protection de l'internaute au regard de ses données à caractère personnel

Au sein de l'Union européenne, la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, harmonise les conditions de protection du droit au respect de la vie privée.[2]

La directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, dénommée « Directive Vie privée et communications électroniques », complète et particularise les dispositions de la directive 95/46/CE dans le secteur des télécommunications.[3] Elle introduit la notion de données relatives au

[1] Le réseau UE d'experts indépendants compte actuellement 25 membres, représentant l'ensemble des pays membre de l'Union et des 10 pays candidats. Cet avis s'inscrit cependant dans le cadre du suivi du Rapport sur le situation de droits fondamentaux dans l'Union européenne et ses états membres en 2002. A l'exception de Malte et de Chypre, les nouveaux Etats membres ne sont dès lors pas couverts par le présent avis. L'expert indépendant couvrant la France n'a pas fourni de réponse.

[2] J.O. n° L 281 du 23 novembre 1995.
Les Etats membres de l'Union européenne ont par ailleurs tous ratifié la Convention n°108 du Conseil de l'Europe relative à la protection des personnes à l'égard du traitement informatisé des données à caractère personnel. Cette convention est en vigueur depuis le 1er octobre 1985.

[3] J.O. n° L 201/37 du 31 juillet 2002. Il faut encore mentionner la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (J.O. n° L 24 du 30 janvier 1998). Il ne sera fait référence à cette directive que dans la mesure où cela s'avérerait utile à une meilleure

trafic définies comme « toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation » (article 2 b)). Elle précise le régime juridique de ces données.

Les directives 95/46/CE et 2002/58/CE s'appliquent au traitement de données à caractère personnel, et notamment aux données de trafic, générées par l'utilisation d'Internet.[4]

Plus précisément, les articles 6 et suivants de la **directive 95/46/CE** traitent de la licéité des traitements de données à caractère personnel. L'article 6 § 1 prévoit ainsi que les données à caractère personnel doivent être traitées loyalement et licitement (a) et collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités (b). Ces données doivent également être adéquates, pertinentes et non-excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement (c). Elles doivent être exactes et si nécessaires, mises à jour (d). Enfin, elles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées par la suite.

Toute personne dispose d'un droit d'accès aux données recueillies le concernant ainsi que d'un droit de contestation et de rectification en cas de données erronées (article 12).

L'article 13 de la directive 95/46/CE prévoit cependant que les Etats membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus notamment à l'article 6 § 1 lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'Etat, la sécurité publique, la défense ou encore lorsqu'elle s'avère nécessaire à la prévention, la recherche, la détection et la poursuite d'infractions pénales.

La **directive 2002/58/CE** « Vie privée et communications électroniques » spécifie ces principes. Son article 5 garantit la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public ainsi que la confidentialité des données relatives au trafic afférentes à ces communications. Il est interdit à toute personne autre que les utilisateurs, d'écouter, d'intercepter, de stocker les communications et les données de trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance sans le consentement des utilisateurs concernés sauf lorsque la personne y légalement autorisée. Les données de trafic font l'objet de l'article 6 de la directive 2002/58/CE. Ces données doivent en principe être effacées ou rendues anonymes dès que la communication est terminée (article 6 § 1). Le Groupe de travail « Article 29 » sur la protection de données à caractère personnel est d'avis que « cette exigence est motivée par la sensibilité des données relatives au trafic, lesquelles révèlent des profils de communication individuels incluant les sources d'information et la localisation géographique de l'utilisateur (…) et les risques potentiels pour la vie privée résultant de la collecte, de la divulgation ou des utilisations ultérieures de ces données ».[5] Le traitement des données de trafic est cependant également admis dans le but d'établir les factures des abonnés et les paiements pour interconnexion (article 6 § 2). Toutefois, ce traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être contestée ou des poursuites engagées pour en obtenir paiement.

En résumé, le traitement des données de trafic est autorisé aux seules fins d'établissement et de facturation des communications. La durée de ce traitement est toutefois strictement limitée à celle nécessaire à la finalité pour laquelle ce traitement est autorisé. Dès 1999, le Groupe de travail « Article

---

compréhension de l'évolution du droit communautaire en la matière. Cette directive a en effet été abrogée par la directive 2002/58/CE.

[4] Groupe de travail « Article 29 » sur la protection des données à caractère personnel, document de travail relatif au traitement des données à caractère personnel sur Internet du 23 février 1998.

[5] Groupe de travail « Article 29 » sur la protection des données à caractère personnel, Recommandation 3/99 du 7 septembre 1999 du Groupe de travail « Article 29 » relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit

29 » sur la protection des données à caractère personnel s'inquiétait cependant des divergences au sein des Etats membres quant à la durée de conservation de ces données et recommandait une période maximale de 3 mois.[6]

L'article 15 § 1 de la directive 2002/58/CE, tout comme l'article 13 de la directive 95/46/CE rappelé ci-dessus, permet aux Etats membres d'adopter des mesures législatives visant à limiter la portée des droits et obligations prévus par la directive. Pareille limitation est admise lorsqu'elle constitue une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique, pour sauvegarder notamment la sécurité nationale ou *assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.*

C'est ce dernier motif de dérogation qui retiendra l'attention dans le cadre de la lutte contre les atteintes aux droits de propriété intellectuelle.

Le cadre juridique II. La criminalisation des atteintes aux droits de propriété intellectuelle

Au cours des dernières années, les initiatives internationales visant à incriminer l'infraction aux droits de propriété intellectuelle se sont multipliées.

Le 23 novembre 2001, 26 Etats membres du Conseil de l'Europe et 4 Etats non membres de celui-ci ont signé à Budapest la **Convention sur la Cybercriminalité**.[7] L'article 10 de cette convention engage les Etats parties à ériger en infraction pénale les atteintes aux droits de propriété intellectuelle.[8] L'incrimination des atteintes aux droits d'auteur et à d'autres droits de propriété intellectuelle fut justifiée par l'urgence qu'il y avait à protéger les droits d'auteurs « du fait des moyens offerts par Internet pour le transgresser ».[9]

A ce jour, l'ensemble des Etats membres de l'Union (15) et des nouveaux adhérents ont signé la Convention sur la Cybercriminalité du 23 novembre 2001 à l'exception de la Lettonie, de la République tchèque et de la Slovaquie. Seul le Danemark l'a ratifiée le 12 mai 2003. L'Union européenne a pour sa part, activement soutenu le projet de convention du Conseil de l'Europe. En mai 1999, les 15 Etats membres adoptaient une position commune sur le projet de texte de cette convention, approuvant l'introduction de mesures pour faciliter les enquêtes et les poursuites.[10]

Dans le prolongement des initiatives de l'Union européenne visant à harmoniser la protection des droits de propriété intellectuelle et à renforcer leur protection, la Commission européenne et le Conseil européen débattent actuellement d'une proposition de directive concernant les mesures et procédures autorisées pour assurer le respect de la propriété intellectuelle[11]. L'article 20 de la directive proposée

---

[6] Groupe de travail « Article 29 » sur la protection des données à caractère personnel, Recommandation 3/99 du 7 septembre 1999 du Groupe de travail « Article 29 » relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit.

[7] Convention sur la Cybercriminalité du 23 novembre 2001 (STE n°185).

[8] Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes. « Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.

1. Chaque partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle définie par la législation de ladite Partie, conformément aux obligations qu'elle a souscrites en application de la Convention universelle sur le droit d'auteur révisée à Paris le 24 juillet 1971, de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces Conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique. »

[9] Rapport du 10 avril 2001 de la Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe sur le projet de convention sur la Cybercriminalité ; disponible à l'adresse http://assembly.coe.int/documents/workingdocs/doc01/fdoc9031.htm).

[10] *Idem*, point II. B. 8.

[11] Proposal for a directive of the European Parliament and of the Council on measures and procedures to ensure the enforcement of intellectual property rights: COM(2003) 46 final (30.01.2003). Le projet de directive concernant les mesures

invite les Etats membres à sanctionner pénalement les infractions graves aux droits de propriété intellectuelle de même que les tentatives d'infractions. L'infraction est qualifiée de grave dès l'instant où elle est commise intentionnellement et à des fins commerciales.[12] La Commission européenne et le Conseil partent du constat que nonobstant l'Accord sur les droits de propriété intellectuelle liés au commerce (ADPIC) (TRIPS Agreement (Agreement on Trade Related aspects of Intellectual Property Rights)) applicable dans tous les Etats membres de l'Union, les titulaires de droits de propriété intellectuelle n'y bénéficient pas d'un niveau de protection équivalent. D'importantes disparités subsistent et une harmonisation s'impose.[13]

Le cadre juridique III. La conciliation d'intérêts légitimes : une interprétation équilibrée, respectueuse des droits fondamentaux, des articles 13 et 15 § 1 des directives 95/46/CE et 2002/58/CE

Dans sa recommandation 3/99 du 7 septembre 1999 relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit, le Groupe de travail « Article 29 » sur la protection des données affirme qu'il est « conscient du rôle important que peuvent jouer les données de trafic dans le contexte des enquêtes sur les crimes perpétués sur Internet, mais souhaite toutefois rappeler aux gouvernements nationaux les principes régissant la protection des droits et libertés fondamentaux des personnes physiques, et en particulier de leur vie privée et du secret de leur correspondance qui doivent être pris en compte dans ce contexte ». [14] Au-delà des seules données de trafic, les données à caractère personnel d'une manière générale sont concernées.

Tant la Convention sur la Cybercriminalité que la proposition de directive concernant les mesures et procédures autorisées pour assurer le respect de la propriété intellectuelle reconnaissent l'importance de la préservation du droit à la protection de la vie privée de l'individu à l'égard de ses données personnelles, y compris dans le contexte de la lutte contre les infractions. Lors des travaux préparatoires de la Convention sur la Cybercriminalité, la Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe s'était montrée très ferme à ce sujet en exigeant le respect strict de l'article 8 de la Convention européenne des droits de l'homme. Elle recommandait également d'inviter les Etats membres ou non membres du Conseil de l'Europe qui souhaitaient adhérer à la Convention sur la Cybercriminalité, à signer et ratifier rapidement la Convention n°108 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ou à légiférer en s'inspirant des principes contenus dans cette convention.[15] Le préambule de la Convention sur la Cybercriminalité renvoie également à différents instruments internationaux de protection de la vie privée et des données à caractère personnel tels l'article 8 de la Convention européenne de droits de l'homme, la Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. La proposition de directive de la Commission européenne et du Conseil européen concernant les mesures et procédures autorisées pour assurer le respect de la propriété intellectuelle déclare, quant à elle, ne pas porter atteinte à la directive 95/46/CE (article 2 § 3 a)).

---

et procédures autorisées pour assurer le respect de la propriété intellectuelle s'inscrit notamment dans la lignée du Livre Vert « *On combatting counterfeiting and piracy in the single market* ». et du Règlement (CE) du Conseil n° 3295/94 du 22 décembre 1994.

[12] Article 20 de la proposition arrêtée au 30 janvier 2003 (COM (2003) 46 final) : Member States shall ensure that all serious infringements of an intellectual property right, as well as attempts at, participation in and instigation of such infringements are treated as a criminal offence. An infringement is considered serious if it is intentional and committed for commercial purposes".

[13] L'ADPIC est adopté au sein de l'Organisation Mondiale du Commerce et en vigueur depuis le 1er janvier 1995. Aux termes de cet accord, certaines atteintes aux droits de propriété intellectuelle sont pénalement sanctionnées.

[14] Groupe de travail « Article 29 » sur la protection des données à caractère personnel, Recommandation 3/99 du 7 septembre 1999 du Groupe de travail « Article 29 » relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit

[15] Rapport du 10 avril 2001 de la Commission des questions juridiques et des droits de l'homme de l'Assemblée parlementaire du Conseil de l'Europe sur le projet de convention sur la Cybercriminalité (point II. B.) ; disponible à l'adresse http://assembly.coe.int/documents/workingdocs/doc01/fdoc9031.htm).

L'article 13 de cette directive 95/46/CE et l'article 15 § 1 de la directive 2002/58/CE autorisent l'adoption par les Etats membres de mesures dérogatoires au régime général de protection de la vie privée dans un but de prévention, de recherche, de détection et de poursuite des atteintes aux droits de propriété intellectuelle pénalement sanctionnées. Ces dérogations ne sauraient en tout état de cause être prises que dans les limites qu'impose l'article 8 de la Charte des droits fondamentaux de l'Union européenne ainsi que l'article 8 de la Convention européenne des droits de l'homme. A l'appui de la jurisprudence de la Cour européenne des droits de l'homme et plus particulièrement des arrêts Klass[16], Leander[17] et Malone[18], le Groupe de travail « Article 29 » sur la protection des données synthétise les exigences de la Cour au regard de mesures de surveillance mises en œuvre en application de l'article 8 § 2 de la Convention européenne des droits de l'homme. La mesure doit être prévue par la loi, nécessaire dans un société démocratique et conforme à l'un des objectifs légitimes énumérés par l'article 8 § 2 de la Convention. « La base juridique doit définir précisément les limites et les moyens d'application de la mesure. Les objectifs pour lesquels les données peuvent être traitées, la durée pendant laquelle celles-ci peuvent être conservées (éventuellement) et l'accès à celles-ci doivent être strictement limités. Une surveillance exploratoire à grande échelle ou générale doit être prohibée. Il s'ensuit que les administrations publiques ne peuvent se voir octroyer l'accès aux données relatives au trafic qu'au cas par cas et jamais de façon anticipée ou en règle générale. Ces critères coïncident avec les dispositions susmentionnées aux articles 13 de la directive 95/46/CE ».[19]

L'interdiction d'une réglementation relative à la conservation des données relatives au trafic qui ne prévoirait pas un certain nombre de garanties visant à imposer le respect de la proportionnalité de cette mesure, ressort également de l'arrêt *Rotaru c. Roumanie* rendu par la Cour européenne des droits de l'homme le 4 mai 2000. La Cour constate une violation de l'article 8 de la Convention européenne des droits de l'homme, en notant particulièrement que la loi roumaine en cause « ne définit ni le genre d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet des mesures de surveillance telles que la collecte et la conservation de données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre. De même, la loi ne fixe pas des limites quant à l'ancienneté des informations détenues et la durée de leur conservation ». Comme une des dispositions de la loi prévoyait la possibilité pour les services secrets roumains de reprendre, à toutes fins de conservation et utilisation, les archives ayant appartenu aux anciens organes de renseignements compétents sur le territoire de la Roumanie, la Cour regrette que cette disposition « ne renferme aucune disposition explicite et détaillée sur les personnes autorisées à consulter les dossiers, la nature de ces derniers, la procédure à suivre et l'usage qui peut être donné aux informations ainsi obtenues ». Elle note aussi que, « bien que l'article 2 de la loi habilite les autorités compétentes à autoriser les ingérences nécessaires afin de prévenir et contrecarrer les menaces pour la sécurité nationale, le motif de telles ingérences n'est pas défini avec suffisamment de précision »[20].

---

[16] Cour eur. D. H., *Klass c. Allemagne*, arrêt du 6 septembre 1978, Série A, n°28, pp. 23 et s.. Les requérants soutenaient que la législation allemande contestée portait atteinte à l'article 8 de la Convention européenne des droits de l'homme en ce qu'elle permettait à certaines autorités d'ouvrir et de contrôler la correspondance et d'intercepter et d'enregistrer les conversations téléphoniques. La Cour conclut à l'existence d'une ingérence mais admet que la législation contestée poursuit un des buts prévus à l'article 8 § 2 de la Convention européenne des droits de l'homme. Dans le cadre de l'examen auquel elle procède afin de déterminer si la mesure dérogatoire respect les limites de l'article 8 § 2, la Cour tient compte de deux paramètres importants : les progrès technologiques en matière d'espionnage et de surveillance et le problème du terrorisme. Toute mesure comportant une restriction à la vie privée doit être prise par l'Etat « conscient du danger, inhérent à pareille loi, de saper, voire de détruire la démocratie au motif de la défendre ». La Cour relève que la législation allemande dénoncée n'autorise pas une surveillance générale mais encadre les mesures de surveillance autorisées de conditions strictes : existence de soupçons graves, absence d'autres méthodes d'enquêtes moins intrusives susceptibles d'établir les faits, limitation de la mesure de surveillance à la seule personne soupçonnée et à celles avec lesquelles elle est en contact.

[17] Cour eur. D.H., *Leander c. Suède*, arrêt du 25 février 1987, Série A, n°116, pp. 14 et s.. La Cour y insiste comme elle l'avait fait dans l'arrêt Klass, sur la mise en péril de la démocratie par l'instauration de systèmes de surveillance permanents.

[18] Cour eur. D.H., *Malone c. Royaume – Uni*, arrêt du 2 août 1984, Série A, n°82, pp. 30 et s.

[19] Groupe de travail « Article 29 » sur la protection des données à caractère personnel, Recommandation 3/99 du 7 septembre 1999 du Groupe de travail « Article 29 » relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit.

[20] Cour eur. D.H., *Rotaru c. Roumanie* (req. n° 28341/95), arrêt du 4 mai 2000, §§ 57-58.

Le Réseau UE d'experts indépendants en matière de droits fondamentaux a déjà eu l'occasion de rappeler les données de la controverse qui a porté sur la compatibilité des exigences du droit au respect de la vie privée de la conservation des données de trafic, lorsque cette conservation excédait une durée déterminée[21]. La question de la durée de conservation des données de trafic a donné lieu à plusieurs prises de position importantes. Les Commissaires européens à la protection des données réunis à Cardiff au mois de septembre 2002 se sont déclarés inquiets de voir l'Union européenne s'engager dans l'examen de propositions d'accords qui auraient pour conséquence la conservation systématique et obligatoire des données de trafic relatives à l'usage de moyen de télécommunication. La déclaration des Commissaires rappelle les conditions strictes de l'application de l'article 15 § 1 de la directive 2002/58/CE en ces termes : « Lorsque les données de trafic doivent être conservées, sa nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou toute autre forme d'abus. La conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée par conséquent inacceptable ».[22] Le Groupe de travail « Article 29 » de protection des données a appuyé cette position, dans un avis 5/2002 qu'il a adopté le 11 octobre 2002[23].

Enfin, la directive 2000/31/CE énonce que « les Etats membres ne doivent pas imposer aux prestataires pour la fourniture des services visés aux articles 12, 13 et 14 [activité de simple transport, de stockage de copie de données temporaire et d'hébergement], une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement les faits ou circonstances révélant des activités illicites » (article 15).[24]

Synthèse sur la situation dans les Etats membres

Il ressort de l'étude comparative que trois ensembles de règles garantissent la protection de l'utilisateur d'Internet au regard de ses données à caractère personnel :

- Les législations nationales en matière de protection des données personnelles sont applicables aux données personnelles générées lors de l'utilisation d'Internet, les données d'identification en faisant partie. L'internaute bénéficie dès lors, au minimum, des garanties de protection prévues par la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (n°108), du 28 janvier 1981, et de la Directive 95/46/CE précitée, du 24 octobre 1995. La directive a été transposée par tous les Etats membres de l'Union européenne, à l'exception de la France. Elle a également donné lieu à des mesures de transposition à Chypre et à Malte.

- Certains Etats ont complété cet arsenal législatif de base en matière de protection des données par une législation spécifique aux données de télécommunication, transposant, le cas échéant, les dispositions de la directive 97/66/CE auxquelles se substituent aujourd'hui celles de la directive vie privée et communications électroniques 2002/58/CE.

- Des dispositions pénales sanctionnant les écoutes téléphoniques et/ou l'interception, la prise de connaissance du contenu de télécommunications viennent compléter la protection de

[21] Observation thématique n°1 : *L'équilibre liberté / sécurité dans les réponses de l'Union européenne et de ses Etats membres à la menace terroriste*, Rapport sur la situation des droits fondamentaux dans l'Union européenne et ses Etats membres en 2002, vol. 2, pp. 26-28.
[22] Le Groupe de travail « Article 29 » sur la protection des données a fait siennes les conclusions des Commissaires. Ces dernières sont jointes à son Avis 5/2002 sur la Déclaration des Commissaires européens à la protection des données adoptée lors de la Conférence internationale de Cardiff (9-11 septembre 2002), relative à la conservation systématique et obligatoire des données de trafic des télécommunications
[23] 11818/02/FR/final, WP 64.
[24] Directive 2000/31/CE du parlement et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société d'information et notamment du commerce électronique, dans le marché intérieur. J.O. L n°178 du 17 juillet 2000, p. 1.

l'internaute à l'égard de ses données personnelles. L'incrimination pénale de ces formes d'ingérences dans la vie privée et le secret des communications n'est cependant pas absolue. La prise de connaissance des communications reste généralement autorisée pour divers motifs de sûreté de l'Etat, de sécurité publique ou de prévention et de lutte contre les atteintes à la loi. De telles exceptions à l'interdiction d'ingérences dans la vie privée doivent faire l'objet d'une lecture restrictive. Une première étape de repérage ou d'interception autorisés ouvre alors la voie à l'identification de l'auteur de la (télé)communication.

L'étude comparative des seize Etats membres envisagés dans cet avis a également montré que le terrorisme est très souvent invoqué pour justifier des dérogations aux règles générales de protection de la vie privée. Afin de se prémunir contre une éventuelle disparition de preuve, les données de trafic sont placées sous surveillance. La collaboration des fournisseurs d'accès et autres intermédiaires privés intervenant de près ou de loin dans la télécommunication est requise pour leur collecte et leur conservation et le défaut de collaboration pénalement sanctionnés. Cette multiplication de participants/collaborateurs privés, invités de la sorte à collaborer à la recherche d'infractions pénales, se manifeste également dans le cadre de la lutte contre les infractions aux droits de propriété intellectuelle. Les situations belge et néerlandaise sont éclairantes sur ce point. Les titulaires de droits de propriété intellectuelle, auteurs, cessionnaires, société de gestion de droits d'auteurs etc., s'invitent ou sont invitées par les autorités judiciaires à la recherche d'infractions.

Quant à la durée de conservation des données de trafic, les recommandations du Groupe de travail « Article 29 » et les vœux des Commissaires européens à la protection des données (Conférence de Cardiff – 2002), ne semblent trouver qu'un faible écho dans la législation des Etats membres. Des législations ciblées sur la lutte contre le terrorisme ou le grand banditisme, des projets de loi en cette matière se multiplient et consacrent des extensions variables des délais de conservation. Ces extensions ont parfois fait l'objet de vives critiques de la part des autorités nationales de contrôle de protection des données.

Les conclusions suivantes se dégagent. L'incrimination des atteintes aux droits de propriété intellectuelle ouvre la voie à l'application tant de l'article 13 de la directive 95/46/CE que, dès lors que ces atteintes seraient commises par le biais d'Internet, à l'application de l'article 15 § 1 de la directive 2002/58/CE. Aux termes de ces dispositions, les Etats membres peuvent en effet adopter des mesures législatives visant à limiter la portée des droits et des obligations que garantissent ces directives – et dont l'internaute peut invoquer le bénéfice – dès lors que cette limitation constitue une mesure nécessaire pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales. Ces dérogations ne sauraient toutefois être prises que dans les limites qu'impose l'article 8 de la Charte des droits fondamentaux de l'Union et de l'article 8 de la Convention européenne des droits de l'homme.

La formulation de l'article 15 § 1 de la directive 2002/58/CE énonce à cet égard de manière bien plus explicite que l'article 13 de la directive 95/46/CE, les exigences - directement inspirées de la Convention européenne des droits de l'homme - auxquelles doit répondre toute mesure de restriction. Alors que l'article 13 de la directive 95/46/CE se contente d'indiquer que la mesure dérogatoire envisagée devrait constituer une mesure nécessaire, notamment pour sauvegarder la prévention, la recherche, la détection et la poursuite d'infractions pénales, l'article 15 § 1 de la directive 2002/58/CE énonce expressément que la limitation envisagée doit constituer « une mesure nécessaire, appropriée et proportionnée au sein d'une société démocratique » et que toutes les mesures dérogatoires qui seraient prises à ce titre devraient l'être « dans le respect des principes généraux du droit communautaire y compris ceux visés à l'article 6 du Traité sur l'Union européenne ».[25]

[25] Article 6 du Traité de l'Union européenne :
« 1. L'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'homme et libertés fondamentales, ainsi que de l'état de droit, principes qui sont communs aux Etats membres.
2. L'Union respecte les droits fondamentaux tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions communes des Etats membres, en tant que principes généraux du droit communautaire.
3. L'Union respecte l'identité nationale de ses Etats membres.

Ce motif de limitation englobe non seulement la *poursuite* d'infractions pénales mais également *la prévention, la recherche et l'identification* de telles infractions. Il ne saurait cependant en aucune manière s'interpréter comme permettant l'instauration d'un régime de surveillance préventif permanent en vue de prévenir, rechercher et détecter tout comportement délictueux. Fut-ce dans la perspective de permettre aux autorités compétentes de vérifier l'application de la loi, il ne peut être question de la mise en place d'un système de surveillance exploratoire ou proactive du web ni de conservation systématique et obligatoire de données de trafic relatives à l'usage de tout moyen de télécommunication au-delà d'une durée justifiée. Les conclusions du Groupe de travail « Article 29 » sur la protection des données et les déclarations des Commissaires européens à la protection des données adoptée lors de la Conférence internationale de Cardiff ont, sur ce point, été rappelées précédemment.[26]

Les articles 13 et 15 § 1 respectivement des directives 95/46/CE et 2002/58/CE traitent invariablement de tout comportement pénalement sanctionné. Ils concernent donc notamment les atteintes aux droits de propriété intellectuelle qui sont pénalement sanctionnées.

La comparaison des analyses nationales démontre que les régimes dérogatoires mis en place, et l'interprétation des exigences préalables à celle-ci, varient sensiblement d'un Etat membre à l'autre. Or c'est précisément par la voie des législations nationales que s'opérera la conciliation entre la nécessité de garantir de manière efficace, par l'adoption de dispositions pénales, les droits de propriété intellectuelle d'une part, et le droit au respect de la vie privée d'autre part. Les recommandations et suggestions suivantes peuvent être faites afin de faciliter cette conciliation. Ces recommandations ou suggestions sont, le cas échéant, inspirées des législations et pratiques nationales en ce compris les avis des autorités indépendantes de contrôle de la protection des données[27] :

Exigence de proportionnalité.

L'opportunité de déroger aux garanties des directives 95/46/CE et 2002/58/CE en vue de prévenir, rechercher, détecter et poursuivre les infractions pénales doit être soigneusement analysée de même que la réalité du motif invoqué. Compte tenu de la formulation très large des articles 13 de la directive 95/46/CE et 15 § 1 de la directive 2002/58/CE, la simple possibilité de rattacher à ces dispositions une législation incriminant l'atteinte aux droits de propriété intellectuelle ne suffit aucunement à la justifier. Une telle législation ne devrait être adoptée que si d'autres alternatives moins attentatoires ne sont pas de nature à permettre un résultat équivalent. L'autorité indépendante de contrôle de la protection des données pourrait être utilement consultée à ce stade et, d'une manière générale, étroitement associée aux travaux préparatoires de la législation envisagée.

Trois conséquences plus précises découlent de l'exigence générale de proportionnalité. Elles constituent les recommandations 2, 3 et 4.

Interdiction de la surveillance permanente et exploratoire.

Ni la mesure législative adoptée ni les procédés techniques dont elle permettrait la mise en œuvre ne peuvent conduire à l'instauration d'une surveillance permanente et exploratoire. A cet égard, on soulignera l'avis du 12 novembre 2001 de la Commission belge pour la protection de la vie privée qui s'oppose à la recherche systématique et proactive des données à caractère personnel sur Internet dans

4. L'Union se dote des moyens nécessaires pour atteindre ses objectifs. »

[26] Groupe de travail « Article 29 » sur la protection des données à caractère personnel, Recommandation 3/99 du 7 septembre 1999 du Groupe de travail « Article 29 » relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit. Déclaration des Commissaires européens à la protection des données adoptée lors de la Conférence internationale de Cardiff (9-11 septembre 2002), relative à la conservation systématique et obligatoire des données de trafic des télécommunications

[27] L'Autorité grecque de protection des données recommande la garantie pure et simple de l'anonymat sur Internet. Voy. ce point : Groupe de travail « Article 29 » sur la protection des données, Recommandation 3/97 : l'anonymat sur Internet, du 3 décembre 1997.

le but de déceler des infractions au droit d'auteur.[28] De même, en ce qui concerne plus spécifiquement les données de trafic, leur conservation doit être limitée dans le temps. La législation qui consacrerait des dérogations doit être suffisamment précise et décrire tant les infractions visées que les techniques envisagées ; à défaut l'exigence de prévisibilité de la loi ne saurait être respectée.

Limitation dans le temps et évaluation régulière des législations justifiant des restrictions à la vie privée sur Internet.

Le cas échéant, cette législation sera limitée dans le temps. En tout état de cause, elle sera soumise à une réévaluation régulière de la nécessité de la maintenir en vigueur, ou d'en conserver la formulation. Une telle évaluation doit être, idéalement, l'œuvre d'une autorité indépendante, par exemple l'autorité indépendante de contrôle de la protection des données. A défaut, une évaluation parlementaire peut constituer une alternative

Limitation au strict nécessaire de l'ingérence dans la vie privée ou de la restriction aux droits de la personne concernée par le traitement des données.

Il convient également de limiter au maximum les garanties auxquelles il peut être porté atteinte et d'organiser, le cas échéant, des mesures progressivement intrusives. La conservation de données de trafic ne doit, par exemple, pas nécessairement s'accompagner d'une suppression de tout droit d'accès, de rectification ou d'opposition. Une analyse approfondie de l'incidence de chaque mesure dérogatoire envisagée sur les différents éléments constitutifs des protections offertes par les directives 95/46/CE, 2002/58/CE et par les législations nationales les transposant, s'impose. Le droit à l'information doit, tout particulièrement, être préservé dans toute la mesure du possible.

Rôle de l'Autorité indépendante de contrôle.

La consultation préalable systématique de l'autorité indépendante de contrôle de protection des données quant à la détermination des infractions visées, les procédés/procédures instaurées, les personnes habilitées à les mettre en oeuvre et la durée de conservation des données par exemple, doit être encouragée (voy. à cet égard la législation belge sur la criminalité informatique).

Respect des principes relatifs au traitement des données à caractère personnel.

Une fois collectées, le traitement de ces données devra intervenir dans le respect des droits et obligations garantis par les directives 95/46/CE et 2002/58/CE sauf les cas où la législation y porterait également légitimement atteinte. Il ne saurait cependant être fait exception au principe de finalité. Ainsi, les données de trafic conservées aujourd'hui au nom de la lutte contre le terrorisme ne pourraient fonder une inculpation pour des faits étrangers à des suspicions d'infractions de type terroriste. Dans son avis no 19/2002, l'autorité grecque de protection des données s'est prononcée en ce sens.

Transparence et identification claire des responsabilités.

Les autorités habilitées à mettre en œuvre les mesures attentatoires admises devraient être spécifiquement énumérées et leur rôle circonscrit.[29] La multiplication des intervenants, les demandes

[28] Avis d'initiative du 12 novembre 2001 concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications (disponible sur http://www.privacy.fgov.be.).

[29] La directive 2000/31/CE du 8 juin 2000 contient d'importantes dispositions sur cette question spécifique (voy. supra). Peu d'Etats membres ont cependant mentionné la transposition de celle-ci dans leur législation interne (voy. l'analyse belge et finlandaise). Il apparaît cependant évident que l'appréciation de la protection de la vie privée de l'internaute sera également fonction des obligations que l'Etat mettra à charge des fournisseurs de service, et autres intermédiaires des services de communication et des responsabilités que ces derniers auront à supporter du fait d'activités illicites commises par les utilisateurs d'Internet. L'on peut à cet égard se féliciter de la mention expresse dans la loi belge de ce que ces intermédiaires n'ont aucune obligation générale de recherche active des comportements illicites de leurs clients. Ce texte est l'exacte

de collaboration diverses, ne peuvent conduire à porter atteinte aux droits de la défense, au droit au silence, au droit ne pas plaider contre soi-même ni déplacer les responsabilités étatiques au seul niveau du privé. Les différents intervenants à la recherche et poursuite d'infractions pénales (par exemple des unités policières se consacrant spécifiquement à la criminalité informatique) devraient ainsi être particulièrement informés des limites de leur action et des droits des tiers. L'obligation d'informer les titulaires des données à caractère personnel traitées devrait s'accompagner du devoir de l'auteur du traitement d'être parfaitement informé des limites de ses propres interventions. Communication externe et communication interne vont de pair. La législation italienne fait sur ce point mention de l'adoption d'un Code de déontologie et de bonne conduite à l'attention des fournisseurs de service de télécommunication. La directive 2000/31/CE y encourage également.

Garantie d'un contrôle juridictionnel effectif.

Le contrôle judiciaire demeure primordial et l'ultime garde-fou contre d'éventuels abus. Même l'existence de garanties en amont, et même en présence d'un cadre législatif a priori satisfaisant par la conciliation qu'il opère entre la garantie des droits de propriété intellectuelle et le droit au respect de la vie privée sur l'Internet, ne dispensent pas de vérifier si le droit au juge est effectif.

réplique de l'article 15 de la directive 2000/31/CE. L'insécurité qui pouvait résulter pour eux de l'attribution dans leur chef de responsabilités toujours plus grande du fait de ces comportements délictueux se trouve ainsi rencontrée.

La situation dans les Etats membres

Austria

In Austria, the fundamental right to the protection of personal data is laid down foremost in the Data Protection Act 2000 (Datenschutzgesetz[30]). The Act however does not contain specific reference to the use of personal data on the Internet. This is due to the fact that Parliament preferred to phrase the protective provisions in a very general and neutral manner, focusing on all possible aspects of dealing with personal data irrespective of the medium used, in order not to prejudice future developments and technical progress. Thus, s. 4 gives a wide definition of the use of data, meaning for the purposes of the law identifying, collecting, recording, copying, retrieving, displaying, utilising, imparting, blocking, deleting, destroying, or any other way of dealing with data. What is important is that the provisions of the Act have direct horizontal effect and apply equally to the use of data in Austria by state agents and private persons. For complaints about misuse of personal data by state agents and invoking disclosure rights the competent authority is the independent Data Protection Commission, whereas in case of a private perpetrator jurisdiction lies with the ordinary courts. A two-tier test is employed as regards the admissibility of the use of personal data: first, anyone collecting data must show a legitimate and well-determined purpose (s. 6) and second, the use of personal data is only permissible if either there exists a special legal authorisation or obligation to that end, or an informed consent was given by the person concerned, or if vital interests of the concerned so require, or finally, if preponderant legitimate interests of a third party so require (s. 8(1)).

For operators of telecommunication services specific provisions in the Telecommunications Act 2003 (Telekommunikationsgesetz[31]) hold more stringently that the processing of personal data is only permitted for the immediate business purpose of providing telecommunication services. Traffic data records therefore may not be kept longer than is needed for billing or debt collection reasons.

So far, it appears, neither the Data Protection Commission nor the courts have rendered any reported decision that would touch on data protection on the Internet. However, given the legal framework, it nevertheless seems feasible to address some of the typical Internet-related fields of concern. As regards cookies, i.e. text files that store information of the user on the users's own PC, the information stored is in most cases computer-related and therefore contains what is called indirect personal data, which do not come under the scope of the Act. However when such data are combined with truly personal data, e.g. when an online order is made by credit card or after any registration with the use of a password, then it can be linked to a certain person and help establish a personal user profile. Moreover, it is assumed, one cannot speak of informed consent of the type required by law if an Internet user simply ticks the "yes" box in the pop-up window asking 'Do you agree that a cookie is placed on your PC?'. The same is true with logfiles that are primarily used for technical surveillance of a system by the administrator, but may also be taken to find out about certain user behaviour. Under Austrian law it would therefore appear to be illegal to store any person-related cookies on the PC after the communication or business transaction (e-commerce) is over, or logfiles on the server of an Internet provider beyond what is technically necessary, without obtaining in each case the prior informed consent of the user.

[30] Federal Law Gazette (BGBl.) No. I 165/1999 as amended by No. I 136/2001.
[31] Federal Law Gazette (BGBl.) No. I 70/2003.

Belgique

L'actualité de la question

Le 12 novembre 2001, la Commission belge pour la protection de la vie privée rendait un avis d'initiative important que les faits résumés ci-après lui avaient suggéré.[32] Afin d'identifier les internautes qui proposent au téléchargement un nombre élevé de fichiers musicaux, l'IFPI Belgium - *International Federation of Phonographic Industry*.- procède à des recherches sur le site Internet de Napster ainsi que sur des sites apparentés (tels Gnutella et autres). Connecté anonymement à l'un de ces sites, le représentant de l'IFPI effectue une recherche afin de visualiser la liste des internautes qui proposent des morceaux d'un artiste belge déterminé et sélectionne le pseudonyme de l'un deux afin de commencer à télécharger le morceau choisi. Durant ce téléchargement, le responsable de l'IFPI utilise une fonction logicielle spécifique qui lui permet d'identifier l'adresse IP utilisée par l'internaute. Dans une seconde phase, il est demandé à différents fournisseurs d'accès à Internet d'effectuer eux-mêmes des recherches afin de prendre contact avec la personne qui, à la date et à l'heure communiquée, a utilisé l'adresse IP repérée par l'IFPI Belgium. L'IFPI demande alors au fournisseur d'accès d'envoyer à la personne concernée une lettre d'avertissement, avec demande de cesser la diffusion des morceaux concernés et de les effacer de son disque dur. Si cette lettre n'est pas suivie d'effet, la politique de l'IFPI est de dénoncer les faits aux autorités judiciaires de poursuite (parquet).

Dans cet avis du 12 novembre 2001, la Commission belge pour la protection de la vie privée s'est attachée à examiner dans quelle mesure la recherche d'infractions au droit d'auteur commises sur Internet, selon la méthode décrite ci-dessus, par des groupes professionnels ou des sociétés de gestion de droits d'auteur, est compatible avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications. Cet avis est annexé au présent document.

Afin d'offrir une description de l'état du droit belge sur la question de savoir quelle est la protection dont bénéficie l'internaute à l'égard de ses données à caractère personnel au regard de l'emploi par les détenteurs de droits de propriété intellectuelle sur des matériaux accessibles via Internet, de technologies permettant l'identification de personnes y ayant accès, il faut tenir compte des dispositions applicables en matière de protection des données à caractère personnel et de secret des télécommunications[33] Les grandes lignes de la loi du 8 décembre 1992 sur la protection des données à caractère personnel et l'article 109ter D de la loi du 21 mars 1991 seront exposés. Une attention particulière sera accordée aux données relatives à des suspicions ayant traits à des infractions compte tenu de la volonté accrue , tant dans les termes du droit international que dans la réalité de la pratique des autorités judiciaires nationales, de tenir en échec les atteintes aux droits d'auteur et compte tenu d'autre part de la multiplication des mécanismes de recherche et d'identification mis en place à cette fin. (point 2). De la législation belge relative aux droits d'auteur et aux droits voisins, l'on retiendra qu'elle assortit de sanctions pénales les atteintes aux droits de propriété intellectuelle (point 3). [34] Cette incrimination justifiera notre examen des techniques (repérage, identification, conservation des données de trafic) susceptibles d'être mises en œuvre par les autorités judiciaires de poursuite et, plus particulièrement, des atteintes à la vie privée que leur application implique et « légitime ». La question des données de trafic sera examinée à ce titre. Un point particulier sera enfin, consacré à l'obligation de collaboration des intermédiaires privés (fournisseurs d'accès, opérateurs) (point 4).

[32] Avis d'initiative du 12 novembre 2001 concernant la compatibilité de la recherche d'infractions au droit d'auteur commises sur Internet avec les dispositions juridiques protégeant les données à caractère personnel et les télécommunications (disponible sur http://www.privacy.fgov.be.).

[33] Sur ce dernier point, seuls les aspects pertinents au regard de l'identification seront mentionnés ; les questions de prise de connaissance de contenu seront simplement évoquées.

[34] La question de savoir si tel ou tel comportement sur Internet constitue ou non une infraction à la législation belge relative aux droits d'auteur ne fait pas l'objet de la présente analyse.

Les dispositions pertinentes en matière de protection des données à caractère personnel et des télécommunications

Aux termes de ***l'article 22 de la Constitution*** belge, « chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visés à l'article 134 garantissent la protection de ce droit ». Aux fins du présente avis, il faut tenir compte de deux législations qui assurent en droit belge, la mise en œuvre de cette garantie constitutionnelle.

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard de traitements de données à caractère personnel

La ***loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard de traitements de données à caractère personnel*** a été profondément réformée par la loi du 11 décembre 1998 transposant la directive européenne du 24 octobre 1995 (95/46/CE). Dans sa version réformée, la loi du 8 décembre 1992 est entrée en vigueur le 1er septembre 2001. Le législateur belge n'a par contre, à ce jour pas encore transposé l'ensemble des dispositions de la directive 2002/58/CE.[35]

Applicabilité de la loi du 8 décembre 1992

- *La notion de données à caractère personnel*

La loi du 8 décembre 1992 s'applique à tout traitement de données à caractère personnel (article 3 § 1), c'est à dire à tout traitement d'informations concernant une personne physique identifiée ou identifiable. Une personne est considérée « identifiable » « dès qu'elle peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale » (article 1).

La Commission pour la protection de la vie privée estime dans un avis du 22 novembre 2000 que tant selon la directive européenne 95/46/CE que selon l'exposé des motifs de la loi du 8 décembre 1992 « la personne concernée ne doit pas être nécessairement identifiée / identifiable par le responsable du traitement mais par n'importe quelle personne, par quelque moyen qui puisse être raisonnablement mis en œuvre par cette personne » et que « outre les informations communiquées volontairement par l'utilisateur dans le cadre de réponses à un formulaire, des informations transmises de manière invisible par l'utilisateur (informations relatives aux pages visitées, préférences en matière de langue, adresse e-mail etc.) peuvent être collectées via un identifiant tel que le *cookie* ou l'adresse IP (lorsque celle-ci est permanente) de l'utilisateur. La loi s'applique au profil de l'utilisateur ainsi constitué, sans qu'il soit nécessaire, aux termes de la loi, que le responsable du traitement dispose du nom ou de l'adresse de l'utilisateur. Il est en tout état de cause possible, par l'intermédiaire du fournisseur d'accès Internet, d'obtenir des informations complémentaires relatives à l'utilisateur (et de retrouver par exemple son numéro de téléphone, son nom ou son adresse) ».[36]

Les données fréquemment utilisées sur Internet telles l'adresse IP, mais aussi le bavardage des navigateurs (ensemble d'informations que le logiciel de navigation transmet à l'insu de l'utilisateur lors de l'utilisation du language html), les données générées par les *cookies*, les programmes Java ou

[35] La loi du 11 mars 2003 sur certains aspects juridiques des services de l'information (M.B., 17 mars 2003, pp. 12962-12970), transposant les dispositions de la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique, dans le marché intérieur, assure en effet également la transposition d'une partie de la directive 2002/58/CE en ce qui concerne l'usage publicitaire du courrier électronique.

[36] Commission belge pour la protection de la vie privée, avis d'initiative du 22 novembre 2000 relatif à la protection de la vie privée dans le cadre du commerce électronique. La Commission belge pour la protection de la vie privée tranche ainsi la question controversée de l'extension de la notion de donnée à caractère personnel aux données créées par les *cookies*. Elle anticipe ainsi, avec plusieurs années d'avance, les exigences de la directive 2002/58/CE.

Activex et les numéros d'identification des microprocesseurs sont donc des données à caractère personnel au sens de la loi belge susmentionnée. [37]

- *La notion de traitement*

Le traitement de données à caractère personnel est entendu comme toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel (article 1 § 2).

Les opérations de simple collecte de données à caractère personnel qui sortaient du champ d'application de la loi du 8 décembre 1992 dans sa version originelle, font partie des traitements visés par la loi révisée en 1998. Un site ou un service dont l'accès donne lieu à la collecte de données à caractère personnel, tel l'encodage d'une adresse électronique ou d'autres données personnelles, est donc soumis à la loi dès l'instant de la collecte. La consultation des données a également été incluse dans la sphère légale en Belgique à l'occasion de la réforme de 1998.[38]

Les données relatives aux infractions

Dans l'avis du 12 novembre 2001, la Commission belge pour la protection de la vie privée qualifie les données collectées au terme de la procédure mise sur pied par l'IFPI et les Ministères de la Justice et des Télécommunications, de données relatives à des « suspicions ayant trait à des infractions ». Telles données, recueillies aux termes d'une procédure mise en place aux fins délibérées de recherche d'infractions commises ou susceptibles d'être commises, constituent des données protégées par l'article 8 de la loi du 8 décembre 1992 telle que modifiée en 1998. Cette disposition interdit le traitement de données à caractère personnel relatives à des litiges soumis aux cours et tribunaux ainsi qu'au juridictions administratives, *à des suspicions, des poursuites ou des condamnations ayant trait à des infractions,* ou à des sanctions administratives ou des mesures de sûreté (article 8 §1).

L'article 8 § 2 prévoit des exceptions à cette interdiction de principe du traitement des données relatives à des suspicions ayant trait à des infractions, et ce dans le cas de traitements effectués :

---

[37] Certains auteurs belges estiment que le caractère identifiable d'une donnée doit être considéré d'une part de manière *intrinsèque* (de quelle donnée s'agit-il ?) mais également de manière *extrinsèque* au regard de la capacité technique, appréciée *in concreto*, du responsable du traitement et des garanties spécifiques offertes par ce dernier quant à l'absence de recherche d'identification. De l'avis de ces auteurs, le seul critère de la possibilité technique « *in abstracto* » ne peut être raisonnablement retenu ; cette interprétation de la législation belge excluant l'existence de toute donnée « anonyme », mises à part les données statistiques. L'interprétation retenue par la loi et la Commission belge pour la protection de la vie privée résulterait, toujours selon eux, d'un regrettable amalgame entre identification d'une personne et lisibilité des données. Voy Th. Verbiest, E. Wéry, *Le droit de l'Internet et de la société de l'information: droits européen, belge et français,* Bruxelles, Larcier, 2001, pp. 412-413.

[38] L'étendue du phénomène à rencontrer peut être détaillée. Au cours de l'année 2002, le Département des Sciences de la Communication de la Faculté des Sciences sociales de l'Université de Leuven a mené une recherche consistant en l'examen de 250 sites Internet sélectionnés sur la liste officielle des entreprises belges, au moyen d'un questionnaire portant sur la manière dont la protection des données personnelles des visiteurs de ces sites était respectée (M. M. Walrave, *E-Privacy .be – protection des données en ligne : amélioration de la protection des données das les sites web belges, un an après l'entrée en vigueur de la 'nouvelle' Loi vie privée*, Leuven, 2002 (disponible sur http://www.droit-technologies.org.). 93 % des sites visités collectent d'une façon ou d'une autre des données personnelles. Seuls 55% de ces sites mentionnent un texte reprenant leur politique en matière de protection des données. Dans seuls 26% des cas cette information est directement liée au(x) formulaire(s) électronique(s) dans lesquels les internautes confient leurs données. La mention du responsable du traitement apparaît dans 74% des cas; le but du traitement (trop souvent formulé de manière peu explicite) dans 88 %; la mention du droit d'accès dans 73%, les modalités d'exercice du droit de correction dans 43% et l'opposition de l'internaute au traitement est concrètement possible dans 25% des cas uniquement. Les 45% restant des sites consultés collectent des données personnelles mais évitent totalement la question de la protection de la vie privée et des données à caractère personnel de l'internaute. Par ailleurs, sur 67% des sites utilisant des *cookies*, seuls 12% en informent leurs visiteurs. L'étude s'est également attachée à examiner la qualité de la politique de protection des données affichée par le site de l'entreprise concernée. Celle-ci fut globalement jugée insatisfaisante (absence de réponse, réponse très vague, peu avertie, voire incorrecte).

« a) sous le contrôle d'une autorité publique ou d'un officier ministériel au sens du Code Judiciaire, lorsque le traitement est nécessaire à l'exercice de leurs tâches ;
b) par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'une décret ou d'une ordonnance ;
c) par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leur propre contentieux l'exige ;
(…) ».

Avant l'adoption de la loi du décembre 1998, l'article 8 § 2 c) mentionnait qu'une personne physique ou morale pouvait traiter des données judiciaires, aux seules fins de gestion de son contentieux *lorsque ce traitement avait pour objet des litiges soumis aux cours et tribunaux ainsi qu'aux juridictions administratives*. Cette dernière condition a été supprimée dans la version amendée et actuellement en vigueur de la loi. Cependant, l'exposé des motifs de la loi de 1998 précise que cette exception sous l'article 8 § 2 c) a été prévue « pour la gestion du contentieux propre à la personne concernée ou pour des avocats ou d'autres conseils juridiques qui doivent traiter des données judiciaires afin de défendre les intérêt de leurs clients (…) ». L'exposé des motifs évoque également en ce sens « le traitement parfois nécessaire de données personnelles par des préposés de compagnies d'assurances ou organisations représentatives des intérêts des travailleurs ». La Commission pour la protection de la vie privée en conclut que le traitement de données relatives à des suspicions, des poursuites ou des condamnations ayant trait à des infractions n'en demeure pas moins permis *uniquement* dans le cadre de litiges soumis aux tribunaux.

De manière générale, l'on ne saurait interpréter la possibilité exceptionnelle prévue à l'article 8 § 2 de la loi du 8 décembre 1992, de traiter des données relatives à des suspicions ayant trait à des infractions pour des besoins de gestion d'un contentieux, comme ouvrant la voie à une collecte autorisée de données en vue d'établir une infraction. La possibilité de traitement de données relatives à des suspicions ayant trait à des infractions existe une fois ces données collectées. Elle n'autorise pas la collecte elle-même. Le fait que la notion de « traitement » (v. supra) englobe l'activité de collecte ne peut être de nature à contredire cette conclusion.

Dans son avis du 12 novembre 2001, la Commission belge pour la protection de la vie privée indique qu'à l'évidence, la question du respect du droit d'auteur est propre à l'auteur de l'œuvre concernée. Les maisons de disques sont également habilitées à revendiquer la protection des droits de propriété intellectuelle dont elles ont obtenu la cession. [39] Qu'il s'agisse de leur contentieux propre n'est pas contesté. La Commission conclut cependant qu'une maison de disques, l'IFPI ou la SABAM sont autorisées à traiter des données relatives à une infraction précise qu'elles ont pu constater, dans la mesure où elles se situent dans une phase au moins préparatoire à un litige et ce, en application de l'article 8 § 2 c) susvisé. Cette disposition ne les **autorise cependant pas à rechercher systématiquement et de façon proactive des données à caractère personnel sur Internet dans le but de déceler des infractions au droit d'auteur.**

La même conclusion s'impose quel que soit le cas de figure visé par l'article 8 § 2.

La Loi du 21 mars 1991 relative aux entreprises publiques économiques

L'article 109ter D de la **Loi du 21 mars 1991 relative aux entreprises publiques économiques**[40] (dite loi Belgacom) prévoit que :

[39] Pour en revenir au cas d'espèce s'étant présenté en Belgique, IFPI est contractuellement habilité à représenter ses membres – soit les maisons de disques – en justice de même que la SABAM – Société belge des auteurs, compositeurs et éditeurs.- qui dispose quant à elle de compétences en matière de gestion des droits des artistes.
[40] Certaines dispositions de la loi-programme de décembre 2002 ont introduit de modifications de certaines dispositions de la Belgacom en lien avec l'article 109terD. Un des amendements a été annulé par la Cour d'Arbitrage. Voy. C.A., arrêt n°69/2003 du 14 mai 2003.

> « Sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information, l'identification ou les données visées ci-après, il est interdit à quiconque, qu'il agisse personnellement ou par l'entremise d'un tiers :
> 1° de prendre frauduleusement connaissance de l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature transmis par voie de télécommunications, en provenance d'autres personnes et destinées à celles-ci (modifié par l'article 13, § 2, 1° de la loi du 30 juin 1994);
> 2° de transformer ou de supprimer frauduleusement par n'importe quel procédé technique l'information visée au 1° ou d'identifier les autres personnes;
> 3° de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne; (...) 4° de révéler ou de faire usage quelconque de l'information, de l'identification et des données obtenues intentionnellement ou non, et visées aux 1°, 2°, 3°, de les modifier ou de les annuler ».

Selon l'avis du 12 novembre 2001 de la Commission belge pour la protection de la vie privée, la prise de connaissance intentionnelle de l'adresse IP de l'internaute dans le cadre du téléchargement d'un fichier musical comme dans le cas d'espèce dont elle s'était saisie, tombe dans le champ d'application, sinon du 1°, en tout cas du 3° de l'article 109ter D interdisant la prise de connaissance de données de communications, telles que des données de connexion à l'Internet.[41]

En conclusion, l'interception, au sens de l'article 109ter D de la loi « Belgacom », et le traitement, au sens de la loi du 8 décembre 1992 (en ce compris leur collecte), de données relatives aux adresses IP et de manière générale de données à caractère personnel générées par l'utilisation d'Internet constituent dès lors- sauf le cas précis de l'article 8 § 2 c) de la loi du 8 décembre 1992 dans le cadre d'une procédure contentieuse, une violation de chacune de ces législations.

La protection du droit d'auteur

Aux termes de la ***Loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins***, les infractions au droit d'auteur sont pénalement sanctionnées. Le mécanisme d'identification des internautes contrevenant mis en place par le protocole d'accord entre les ministères de la Justice, de Télécommunications et l'ISPA, visait ainsi à dénoncer l'infraction au parquet (articles 80 à 86).[42] L'article 74 de la loi prévoit que « (...) la preuve d'une représentation, d'une exécution, d'une reproduction ou d'une exploitation quelconque (...) pourra résulter des constatations d'un huissier de justice, ou jusqu'à preuve du contraire de celles d'un agent désigné par des sociétés de gestion, agréé par le Ministre ayant le droit d'auteur dans ses compétences et assermenté conformément à l'article 572 du Code judiciaire » .

Selon l'avis de la Commission belge pour la protection de la vie privée, ce pouvoir de constatation ne permet toutefois pas aux agents concernés de disposer de compétences particulières en matière d'investigation. Ils n'ont pas de compétence d'officier de police judiciaire, et ne peuvent procéder à une interception de données de télécommunication protégées par la loi ou à une surveillance systématique du réseau.

---

[41] Le fait que la personne responsable de la prise de connaissance soit ou non partie à la communication importe peu dans le cadre de cette disposition. En effet, celle-ci a un champ d'application plus large que l'article 314 bis du Code pénal, qui ne s'applique pas lorsque la personne qui enregistre une communication est partie à cette communication, et qui protège uniquement le contenu des communications. Article 314 bis du Code pénal (extrait) :

> §1 : Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents francs à dix mille francs ou d'une de ces peines seulement, quiconque :
>
> 1° soit intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter , prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications.

La divulgation d 'informations illégalement recueillies à des tiers est également sanctionnée de même que la tentative de commettre les infractions visées par l'article.

[42] En date du 23 novembre 2001, la Belgique a signé - mais pas encore ratifié - la *Convention sur la Cybercriminalité* adoptée dans le cadre du Conseil de l'Europe le 23 novembre 2001. Rappelons qu'à l'article 10 de cette convention, les Etats parties s'engagent à adopter les mesures législatives et autres nécessaires pour ériger en infraction pénale les atteintes à la propriété intellectuelle définies par chaque état conformément à ses engagements internationaux.

La recherche des infractions en milieu informatisé

La **Loi sur la criminalité informatique du 28 novembre 2000**[43], introduit dans le Code pénal plusieurs infractions dont l'ordinateur est la cible ou l'outil d'infraction et que les catégories traditionnelles d'infractions ne parvenaient pas à appréhender jusqu'alors dans leur globalité (la fraude informatique, le faux en informatique, l'accès non autorisé, le sabotage ou l'introduction de virus).[44] Les questions de procédure pénale forment la deuxième partie de la loi (voy. infra). Ces innovations procédurales s'appliquent à toutes les formes de délinquance informatique spécifiquement incriminées par les dispositions de son premier volet (voy. ci-dessus) mais également aux infractions "classiques" dont la preuve ne peut être rapportée que par la voie de données informatiques.[45] La loi du 28 novembre 2000 emporte ainsi modification du Code d'instruction criminelle, adaptant la procédure pénale aux nécessités de la recherche d'infractions en milieu informatisé d'une part, et de la loi Belgacom déjà évoquée d'autre part. Cette dernière adaptation retiendra notre attention (4.2.)

Certains auteurs estiment que la loi du 28 novembre 200 sur la criminalité informatique constitue la base légale exigée par l'article 8 § 2 de la Convention européenne des droits de l'homme. Selon eux, les ingérences dans la vie privée régulièrement commises par les autorités judiciaires dans les systèmes informatiques ou l'interception de télécommunications numériques, se trouveraient désormais légalement justifiées.[46] La Commission pour la protection de la vie privée ne partage pas ce point de vue. Les principales critiques et commentaires qu'elle formule à l'encontre de la loi du 28 novembre 2000 seront exposées ci-après. Préalablement, l'on rappellera les dispositions du Code d'instruction criminelle permettant le repérage et l'identification des télécommunications (4.1.).

Le repérage et l'identification des télécommunications (articles 88 bis et 46 bis du Code d'instruction criminelle)

Dans un premier temps limité aux appels téléphoniques[47], étendu ensuite à toutes formes de télécommunications par la loi du 10 juin 1998[48], le repérage des télécommunications permet au juge d'instruction de prendre connaissance des données d'appel de moyens de télécommunications à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés et à faire procéder à la localisation de l'origine ou de la destination de télécommunications.[49] Au départ du repérage effectué, le juge d'instruction peut établir l'identité de l'utilisateur grâce au mécanisme de l'identification prévu par l'article 46bis de CIC, en recueillant telles données d'identification auprès des services de télécommunication auxquels l'utilisateur est abonné et en exigeant d'un fournisseur d'accès qu'il lui communique les coordonnées de la personne à laquelle une adresse IP a été octroyée .[50]

---

[43] F. de Villenfagne, S. Dusollier, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *Auteurs et Médias*, 2001, pp. 60-81.

[44] On ne peut exclure que certaines infractions ne soient commises par des procédés incriminés par cette législation, tels le *hacking* ou la fraude informatique. Un concours d'infraction est donc possible. Cette question ne sera cependant pas examinée ici.

[45] Loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.,* 3 février 2001 (entrée en vigueur le 13 février 2001)., pp. 2909-2914.

[46] C. Meunier, La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique, *Rev. dr. pénal*, 2001, pp. 611 et s..

[47] Loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prie de connaissance et l'enregistrement de communication et de télécommunications privées.

[48] Loi du 10 juin 1998, modifiant la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prie de connaissance et l'enregistrement de communication et de télécommunications privées, *M.B.,* 9 septembre 1998.

[49] Article 88 bis du *Code d'instruction criminelle* (extraits) :

> Lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunication ou la localisation de l'origine ou de la destination de la télécommunication nécessaire à la manifestation de la vérité, il peut faire procéder, en requérant au besoin le concours technique de de l'opérateur d'un réseau de télécommunication ou du fournisseur d'un service de télécommunication
> 1° au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés ;
> 2° à la localisation de l'origine ou de la destination de télécommunications.
> (…)

[50] Article 46bis du *Code d'instruction criminelle* (extraits) :

> § 1 : En recherchant les crimes et délits, le procureur du Roi peut par une décision motivée et écrite requérir l'opérateur d'un réseau de télécommunication ou le fournisseur d'un service de télécommunication :

L'obligation d'enregistrement et de conservation par les opérateurs de réseaux de télécommunication (article 109ter E de la loi "Belgacom" du 21 mars 1991 portant réforme de certaines entreprises publiques économiques): la délicate question des données de trafic

La loi du 28 novembre 2000 relative à la criminalité informatique a apporté une modification substantielle à l'article 109ter de la loi du 21 mars 1991 rappelé précédemment. Jusqu'à l'adoption de cette loi du 28 novembre 2000 relative à la criminalité informatique, les fournisseurs de service et opérateurs de réseaux de télécommunication n'étaient assujettis à aucune obligation légale de conservation des données d'appel et d'identification. Le stockage de telles informations répondait généralement aux besoins de tarification des connexions à Internet dans le respect des prescriptions de la directive 97/66/CE aujourd'hui abrogée et de la directive 2002/58/CE (article 6) qui ne permettent/aient la collecte et le stockage de données relatives au trafic de leurs abonnées et utilisateurs par les opérateurs et fournisseurs que dans l'optique de l'établissement de la communication et de leur facturation. [51]. Des dérogations sont toutefois admises en application de l'article 15 § 1 de la directive 2002/58/CE, notamment en vue de la prévention, la recherche, la détection et la poursuites d'infractions.[52]

Aux termes du nouvel article 109 ter E, § 2 alinéa 1er, il est prévu que « le Roi fixera, par arrêté délibéré en Conseil des Ministres, les obligations pour les opérateurs de réseaux de télécommunication et les fournisseurs de services de télécommunication d'enregistrer et de conserver, pendant un certain délai en vue de l'investigation et de la poursuite d'infractions pénales, dans les cas à déterminer par arrêté royal délibéré en Conseil des Ministres et sur proposition du Ministre de la Justice et du Ministre qui a les Télécommunications, les Entreprises et les Participations publiques dans ses attributions, les données d'appel des moyens de télécommunication et les données d'identification d'utilisateurs de services de télécommunication. Ce délai, qui ne peut jamais être inférieur à 12 mois, ainsi que les données d'appel et d'identification, seront déterminés par arrêté royal délibéré en Conseil des Ministres et après avis de la Commission pour la protection de la vie privée ».[53]

Les principales critiques formulées à l'encontre de cette disposition au regard des exigences que requièrent le respect de la vie privée et de la protection des données à caractère personnel, peuvent être synthétisées comme suit :

- Le principe de légalité voudrait que toute exception soit précisément définie dans la loi et non laissée à l'appréciation de l'exécutif.

- L'exigence de conservation s'applique aux données d'appel et aux données d'identification. Ces deux concepts sont cependant peu définis. Si l'on transpose à l'environnement numérique les composantes des données d'appel « classiques », l'adresse IP de l'ordinateur émetteur et récepteur de la communication, les adresses des sites visités, la durée de ces visites, les adresses e-mails des messages échangés par l'émissaire et le destinataire et l'identification de personnes relativement aux moyens de paiement concerné lorsque le sujet de l'obligation de conservation est un prestataire de tels paiements électroniques en feront partie. Ces données recoupent des éléments permettant d'identifier l'utilisateur de services et constituent à l'évidence des données à caractère personnel protégées par la législation belge relative à la protection de la vie privée de

---

1° d'identifier l'abonné ou l'utilisateur habituel d'un service de télécommunication ;
2° de communiquer les données d'identification relatives aux services de télécommunication auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.
(…)
§ 2 : Chaque opérateur de réseau de télécommunication et chaque fournisseur d'un service de télécommunication qui est requis de communiquer les données visées au paragraphe premier, donne au procureur du Roi ou à l'officier de police judiciaire les données qui ont été demandées (…).

[51] Relevons cependant que la multiplication des systèmes de connexion permanente, tarifiée forfaitairement, annihile l'intérêt de la conservation de telles données.

[52] Aux termes de cette disposition, ces restrictions à la vie privée ne peuvent toutefois intervenir que dans les limites qu'impose le respect des droits fondamentaux, et notamment de la vie privée telle qu'elle est garantie par l'article 8 § 2 de la Convention européenne des droits de l'homme. (voy. l'introduction générale du présent document).

[53] C'est nous qui soulignons.

1992. Le risque de glissement de l'identification de l'appel à l'identification du contenu que permettent aisément certaines technologies a également été dénoncé.[54]

- La Commission belge pour la protection de la vie privée a critiqué le caractère disproportionné de conservation envisagée de ces données et l'instauration d'une surveillance policière généralisée visant tout utilisateur d'un service de télécommunication que ni l'article 13 de la directive 95/46/CE ni l'article 15 § 1 de la directive 2002/58/CE ne peuvent légitimer. Les dérogations permises au titre de cette dernière disposition à la limitation de collecte de données personnelles dans le cas de prévention, recherche, détection et poursuite d'infractions pénales, ne donnent « pas un blanc seing pour établir une surveillance exploratoire et proactive des télécommunications ». [55]

- La fixation de la durée de conservation est laissée à l'appréciation du Roi après avis de la Commission pour la protection de la vie privée. Il ne peut cependant être inférieur à 12 mois. Ce délai excède celui proposé par la Recommandation en la matière du Groupe de travail Article 29[56], et par la déclaration des Commissaires européens à la protection des données à caractère personnel adoptée lors de la Conférence internationale de Cardiff (9-11 septembre 2002)[57].

- Les « opérateurs de réseau de télécommunication et les fournisseurs de réseaux de télécommunication » sont tenus à une obligation d'enregistrement et de conservation,. Ces expressions incluent les fournisseurs de courriers électroniques, les services d'accès, les services de forums de discussion ou encore les prestataires de services à valeur ajoutée (cryptographie, services bancaires etc.).[58]

L'obligation de collaboration des fournisseurs d'accès et autres intermédiaires

Outre l'article 109 ter E susvisé, la loi du 11 mars 2003 relative à certains aspects juridiques de la société d'information traite également de la responsabilité des intermédiaires et la collaboration qui leur est demandée par les autorités judiciaires.[59] Sous certaines conditions, les destinataires de l'obligation de conservation aux termes de l'article 109 ter E de la loi du 21 mars 1991 commentée ci-dessus (loi Belgacom), en sont exemptés. La loi précise en outre que ces prestataires de services à la société de l'information ne sont pas tenus à une obligation de surveillance continue (article 21..[60] La

[54] D'autant que la prise de connaissance du contenu des télécommunications est consacrée aux articles 90 ter et 90 quarter du Code d'instruction criminelle. Dérogeant à l'interdiction de principe de la loi 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, l'interception pourra être opérée par un juge d'instruction, à l'égard d'infractions énumérées à l'article 109ter du C. I. C. dont question ci-dessus.

[55] Avis de la Commission belge pour la protection de la vie privée du 13 décembre 1999 portant sur les projets de loi relatifs à la criminalité informatique.

[56] Groupe de Travail « Article 29 » sur la protection des données, Recommandation 3/99 du 7 septembre 1999 relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du droit. Voy. aussi Groupe de Travail « Article 29 » sur la protection des données, Recommandation concernant certaines exigences minimales pour la collecte en ligne de données à caractère personnel dans l'Union européenne, adoptée le 17 mai 2001 (disponibles sur http://www.europa.eu.int/comm/internal_market/fr/media/dataprot/wpdosc/index.htm.

[57] Aux termes de cette déclaration, les Commissaires européens à la protection des données concluent que la conservation systématique et obligatoire des données relatives à l'usage de télécommunication pour une durée d'1 an ou plus est jugée comme un moyen disproportionné et inacceptable, fut – ce par dérogation admise en application de l'article 15 § 1 de la directive 2002/58/CE (à l'époque article 14 de la directive 97/66/CE) à la règle générale selon laquelle les données de trafic sont conservées aux seules fins d'établissement et de facturation des communications.

[58] La Commission pour la protection de la vie privée s'est à plusieurs reprises, au gré des initiatives parlementaires ou de l'exécutif, déjà exprimée sur différents aspects de cette collaboration imposée aux opérateurs et fournisseurs de service. Voy Avis du 11 janvier 2001 relatif au projet d'arrêté royal portant exécution des dispositions de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, et de l'article 109ter E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques ; et l'avis portant le numéro 12/1999 (disponibles sur http://www.privacy.fgov.be).

[59] Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.,* 17 mars 2003, pp. 12963.

[60] Section 4 : Surveillance, de la loi susvisée :

disparité des termes d'une législation à l'autre, l'absence de renvoi entre elles et les formulations parfois sibyllines sont regrettables et ne permettent pas, ou pas encore compte tenu de leur caractère récent, de se prononcer sur l'impact de ces nouvelles dispositions.

Dans son avis du 12 novembre 2001, la Commission pour la protection de la vie privée avait, rappelé le prescrit de l'article 105 nonies de la loi du 21 mars 1991 aux termes duquel :

> « § 4 : (...) les données visées peuvent être traitées par l'opérateur d'un réseau public de télécommunication ou par le fournisseur d'un service de télécommunication offert au public pour détecter les fraudes. Les données traitées pour détecter les fraudes sont communiquées aux autorités compétentes pour la recherche ou la poursuite d'infractions pénales au cas où il y a indication qu'une infraction pénale a été ou pourrait être commise ».

De l'avis de la Commission, cette autorisation de traiter des données de télécommunication constitue « une **exception** au principe d'interdiction des interceptions; [et] une **nouvelle finalité** par rapport à celle(s) poursuivie(s) par les fournisseurs de télécommunication Elle doit donc être interprétée de façon restrictive, en particulier en ce qui concerne la notion de fraude (…) ».

Conclusion

En conclusion, la volonté accrue de tenir en échec les infractions aux droits de propriété intellectuelle ne doit pas conduire à passer sous silence les nécessités du respect de la vie privée de l'internaute tel qu'il est consacré par l'article 8 de la Convention européenne des droits de l'homme et par la loi belge du 8 décembre 1992. Si l'identification d'auteurs présumés d'actes illicites effectués via le service de télécommunications - et leur communication aux autorités (judiciaires) compétente venaient à être autorisées, cette autorisation ne pourrait s'étendre jusqu'à donner des pouvoirs d'investigation propres qui pourraient être exercés d'initiative par l'intermédiaire privé, qui se substituerait de cette manière aux autorités compétentes. D'éventuelles dérogations autorisées ne peuvent permettre une collaboration permanente entre entreprises et fournisseurs et une identification systématique des usagers, sous peine de transformer les fournisseurs d'accès en auxiliaires de police dans le cadre d'enquêtes à caractère général. Fut-ce dans un contexte de multiplication des infractions au droit d'auteur, l'exigence de protection de la vie privée fait obstacle au développement de méthodes de surveillance exploratoire, globale, indépendamment d'instructions relatives à des infractions particulières.[61]

Cyprus

The Processing of Personal Data (Protection of the Person) Laws of 2001 to 2003 [*Ο Περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμος του 2001 ως 2003*] does not directly refer to protection of data of the users of the Internet. Instead the Law provides for a general protection of personal data. Pursuant to section 3, the Law applies to processing which is wholly or partially automated, and to non-automated processing of personal data, which are included or will be included in a record. Automation is an automatic execution of an operation without the intervention of a person, except for the initial command. This is done through a machine or their system of operation. This covers a broad spectrum indicating that data protection of users of the Internet may be protected pursuant to this Law.

Pour la fourniture des services visés aux articles 18, 19 et 20 [activité de simple transport, activité de stockage sous forme de copie temporaire de données, activité d'hébergement], les prestataires n'ont aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.
Le principe énoncé à l'alinéa 1er ne vaut pas pour les obligations à caractère général. Il n'empêche pas les autorités compétentes d'imposer une obligation temporaire de surveillance dans un cas spécifique, lorsque cette possibilité est prévue par la loi. C'est nous qui soulignons.

[61] Avis de la Commission belge pour la protection de la vie privée du 12 novembre 2001 et du 13 décembre 1999.

Even though there is direct legislation concerning data protection of users of the Internet, the Cyprus Data Protection Commissioner has informed us that appropriate legislation will be drafted in the foreseeable future probably in the form of secondary legislation.

In relation to technological devices used by holders of intellectual property rights on material accessible via the Internet the Law of Copyright and Neighbouring Rights of 1976 to 2002 [*Οι Περί του Δικαιώματος Πνευματικής Ιδιοκτησίας Νόμοι του 1976 μέχρι 2002*] does not provide for something specific like this. The intellectual property right holder has the exclusive right, within the Republic, to carry out the reproduction in any form, to display, to communicate to the public, to broadcast and many other associated rights. The Internet has no boundaries and the material may be accessible from different parts of the world, thus the rights of the holders to display, as understood in the Law, rest within the Republic. It remains that there is no direct legislation with regards to the Internet. Such legislation should be enacted in line with the harmonisation process and the infiltration of the Internet into the every day life of Cypriots.

Denmark

The Danish Constitution of 1953 contains two provisions relating to privacy and data protection. Section 71 provides for the inviolability of personal liberty. Section 72 provides for the inviolability of "the dwelling" and of the secrecy of communication.[62]

The Act on Processing of Personal Data entered into force on July 1, 2000.[63] The law divides personal information into three categories: ordinary, sensitive and semi-sensitive and provides different conditions for the processing of each.[64] A broad exemption from the Act is provided for law enforcement activities.[65] An independent agency, the Data Protection Agency ("DPA") (*Datatilsynet*), enforces the act. It mainly deals with specific cases on the basis of inquiries from public authorities or private individuals, or cases taken up by the agency on its own initiative[66].

Other laws regulating the processing of personal information by the public sector include the Public Administration Act of 1985, the Publicity and Freedom of Information Act of 1985, the Public Records Act of 1992, and the National Registers Act of 2000. These laws set out basic data protection principles and determine what data should be available to the public and what should be kept confidential.[67] Sectoral laws also provide special protections for medical information[68] and credit card details[69] and lay down restrictions on direct marketing (including spam).[70]

Wiretapping is regulated by the Penal Code.[71] Statistical data on the interference of communications by the police show that out of 2,178 requests, the courts approved 99%.

In March 2001, Denmark amended its laws on search and seizure in accordance with its obligations under the Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS"). The Administration of Justice Act now authorizes physical searches for copyright infringements without "prior notification of the defendant if it is assumed that the notification would cause a risk of removal,

[62] Constitution of Denmark 1953, available at <http://www.uni-wuerzburg.de/law/da00t___.html>.
[63] The Act on Processing of Personal Data, Act No. 429 of May 31, 2000 (*Lov om behandling af personoplysninger*), available at http://147.29.40.90/_GETDOC_/ACCN/A20000042930-REGL
[64] Peter Blume *et al.*, Nordic Data Protection 19-20 (DJOF Publishing Copenhagen 2001).
[65] *Id.* at 23.
[66] In 2002 the DPA received 785 inquiries and complaints and initiated 117 investigations.
[67] Peter Blume *et al.*, *supra* at 13.
[68] Patients' Rights Act of 1998.
[69] Credit Cards Act of 2000.
[70] Marketing Practices Act of 2000.
[71] Penal Code Section 263.

destruction or modification of objects, documents, information in computer systems or anything else that are comprised by the petition for investigation." The Act took effect on April 1, 2001.[72]

In December 2002 the EU Copyright Directive (EUCD) was implemented in Danish legislation as an amendment to the Act on Copyright.[73] The most radical change was the circumvention of DRM systems. The Act on Copyright already included an article that prohibited distribution or (with a commercial intent) possession of technical means that had the sole purpose to circumvent technical measures to protect works in digital form. However, with the implementation of EUCD, circumvention itself was made illegal.

A new anti-terrorism bill became law in June 2002.[74] Among other things, the legislation establishes mandatory registration and storage of traffic data for one year by telecommunications and Internet providers. It also gives law enforcement the power to secretly install snooping software on the computers of criminal suspects. The software will record keystroke data and transmit it electronically to the law enforcement agency. This power may only be used for serious crimes and will require an interception warrant.

On June 4, 2003, the Parliament enacted a bill to combat organized crime. The Act amends the Administration of Justice Act and Penal Code and expands the possibility for the police secretly to install snooping software on criminal suspects' computers[75]. This is an extension of the anti terrorism Act, mentioned above.

Finland

Constitutional framework for considering the protection of personal data of the users of the Internet, as well as intellectual property rights

Section 10 of the Constitution of Finland – "Section 10 - The right to privacy" – provides as follows:

> "Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act. The secrecy of correspondence, telephony and other confidential communications is inviolable. Provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act."[76]

The protection of personal data is not limited to any specific media of communications. Accordingly, it also covers the users of the Internet. Moreover, the protection of personal data includes protection against interference of both public authority and other individuals or private organizations. Limitations on the protection of personal data are only permissible under certain conditions laid down by an Act.

Constitutional protection of intellectual property rights is, in turn, based on Section 15 of the Constitution of Finland. According to this provision, "[T]he property of everyone is protected." The constitutional protection of intellectual property rights also covers the Internet.

Legislative framework

---

[72] "Denmark Enacts Anti-Piracy Search and Seizure Law," Cluebot, July 20, 2001 http://www.cluebot.com/article.pl?sid=01/06/26/042210

[73] Act. No. 164, 12 March 2003.

[74] Law No. 378, June 6, 2002, Law Concerning the Change of Penal Code, Administration of Justice Act, Law of Competition and Consumer Regulation of the Telecommunications Market, Law of Small Arms, Law of Extradition and Law of Extradition of Criminals to Finland, Iceland, Norway And Sweden.

[75] Section 791 b. *Retsplejeloven* (Administration of Justice Act) § 791b. *See* <http://www.retsinfo.dk>.

[76] The Finnish Constitution in English can be found here: http://www.om.fi/constitution/.

The Personal Data Act (*Henkilötietolaki*, Act No 523 of 1999) regulates the processing of personal data. The main objective of the Act is to secure, in the processing of personal data, the appropriate protection of private life, as well as to promote the development of and compliance with good processing practice.

Furthermore, *Act on the Protection of Privacy and Data Security in Telecommunications* (Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta, Act No 565 of 1999) regulates the data security of public telecommunications and the protection of the privacy and the legitimate interests of subscribers and users in telecommunications. This Act applies to public telecommunications and to telecommunications operated by means of public telecommunications services as well as to the provision of subscriber directories. However, the processing of personal data in telecommunications is governed by specific provisions on the processing of personal data – Personal Data Act, see above – unless otherwise provided for in this Act. The Act also applies to telecommunications from or to a telecommunications network other than a public telecommunications network through the latter network if the telecommunications network other than a public telecommunications network has been connected as part of a public telecommunications network or to a subscription of a public telecommunications network. However, the Act does not apply to television and radio broadcasting.

The *Act on the Exercise of the Freedom of Speech* in Mass Communication (Laki sananvapauden käyttämisestä joukkoviestinnässä, Act No of 2003) is also of significance for the protection of personal data of the users of the Internet, although the basic objective of this Act is to regulate the exercise of the freedom of speech, including online freedom of speech. Certain provisions of this Act specifically aim at preventing crimes which can be committed by using various means of expression, e.g. the publication of such information in the Internet that amounts to the invasion of personal reputation.[77]

The Act combats against "online crimes" by setting some restrictions and obligations. To start with, the Act obliges the Internet publishers to store the web publications or programs for three weeks.[78] Furthermore, it allows the removal of material put to a web page that violates someone's right to private life or personal reputation.[79]

The *Act on information society services* (*Laki tietoyhteiskunnan palvelujen tarjoamisesta*, Act No 458 of 2002), entered into force on 1st July 2002: The main purpose of the Act is to promote the freedom of so-called information society services. This Act implements Directive 2000/31/EC of the European Parliament and of the Council concerning on-line services in a communication network.

The Act includes a number of provisions which are of significance from the view point of the protection of personal data and/or copyright or related rights. Under this Act, the service provider is not liable for the possible illegal content of the information transmitted if its activity is of a mere

[77] Section 8 of Chapter 24 of the Penal Code (Act No 531 of 2000) criminalises invasion of personal reputation as follows: "(1)A person who unlawfully (1)through the use of the mass media, or (2)in another manner publicly spreads information, an insinuation or an image of the private life of another person, so that the act is conducive to causing that person damage or suffering, or subjecting that person to contempt, shall be sentenced for an invasion of personal reputation to a fine or to imprisonment for at most two years.
(2) The spreading of information, an insinuation or an image of the private life of a person in politics, business, public office or public position, or in a comparable position, shall not constitute an invasion of personal reputation, if it may affect the evaluation of that person's activities in the position in question and if it is necessary for purposes of dealing with a matter with importance to society."

[78] The original proposal was that the publishers must store the web publications or programs for two or three months. See governmental bill (HE 54/2002vp). It seems that keeping the publication available would be sufficient to comply with the archiving requirement. However, it is still unclear whether the three weeks is counted from the moment that the web publication was first published or from the moment when the publication was last available to the public.

[79] Originally, the proposal was that publishers and service providers must log practically all Internet traffic**.** The reasoning was that the compulsory archival of the log information is necessary because it is the only way to find out the identities of those who write anonymously and at the same time commit a crime. However, the Finnish parliament passed the bill with several modifications, one of which was that *mandator*y storing of traffic data was removed from the Act.

technical nature and does not involve participation in the producing of the illegal information. Regarding information which has been stored by the service provider at the request of the recipient of the service, the provider has a duty to disable access to information which infringes copyright or other related rights if requested by the copyright holder or his or her representative (Section 15).

Access to information which is in breach of the Penal Code, especially provisions on the prohibition of ethnic agitation and the dissemination of depictions of obscenity, shall be prevented on the service provider's own initiative. A court may also order the service provider to prevent access to information which is clearly illegal or is being transmitted illegally (Section 16). Before the decision is made, the service provider and the information producer must be heard, unless this is impossible because of the extreme urgency of the matter. The service provider and the information producer may request the court to reverse its decision.

The entry into force of Act on Information Society Services also entailed amendments to three other Acts. Commercial communications per e-mail must be clearly identifiable as such (Act No 459 of 2002, amending Act No 565 of 1999 on protection of privacy in telecommunication). The commercial purpose of a communication as well as the natural or legal person on whose behalf the commercial communication is made shall be clearly identifiable (Acts No 460 of 2002 and No 461 of 2002, amending the Consumer Protection Act (Act No 38 of 1978 and Act No 1061 of 1978) concerning inappropriate procedures in business activities).

Finland is also a contracting party to the *Wassenaar Treaty* which includes cryptographic export controls.

Current Finnish legislation concerning intellectual property rights already applies to the Internet, too. However, a complete reform of copyright legislation is currently envisaged. The new law would also implement the EU copyright directive. The new law is targeted to enter into force in January 2004.

Case law, national practices or other relevant information

Until now, *Internet service providers* (ISPs) have not been required to give over user information due to copyright cases. There have there been no cases of the removal of domains due to trademark/copyright laws.

Copyright has not been used to limit the freedom of speech on the Internet. However, one NGO (antipiracy.fi) has advocated for this kind of right. This organization wants to get user names and IPs if they find someone distributing infringing content in P2P networks.

ISPs who host content for their clients are not under a duty to monitor pages, communications or actions of users including. They are not liable in terms of the law for the actions of their users. However, ISP may become liable if it fails to take down illegal message or page after a formal notification.

In Finland, there are no mandatory requirements that the users of the Internet identify themselves or that users' activities are being logged.

Germany

The relevant law is the *Gesetz über den Datenschutz bei Telediensten* (*Teledienstedatenschutzgesetz* – TDDSG) [Act on the Protection of Personal Data Used in Teleservices (Teleservices Data Protection Act)] of 22 July 1997 in the wording of a last amendment of December 2001. Together with the Gesetz über die Nutzung von Teleddiensten (Teledienstegesetz) [Act on the Using of Teleservices (Teleservices Act)] it is part of a complex of laws regarding information and communication services.

The Teledienstegesetz rules the homogeneous economic general conditions for using the electronic information and communication services (among others the Internet).

The Teledienstedatenschutzgesetz (TDDSG) as a special law to the Bundesdatenschutzgesetz [Federal Data Protection Act] protects the personal data of the users of teleservices upon the collection, processing, and utilization of such data by service providers.The provider may process and use the personal data collected for performing teleservices or for other purposes only if permitted by a specific regulation or if the user has given his consent (section 3 § 2). Among others sections 5 and 6 TDDSG are specific regulations in the sense of section 3 § 2. The provider may collect, process, and utilize a user's personal data without his consent only to the extent they are needed for the concluding, determining the terms of, or modifying a contractual relationship with him on the use of teleservices (contractual data, section 5), required to facilitate and invoice the use of teleservices (utilization data, section 6). Utilization data include, in particular, (a) characteristics that identify the user, (b) information on the beginning, end, and extent of each use, (c) information on the teleservices accessed by the user.

According to section 8 TDDSG the Federal Commissioner for Data Protection shall observe the development of data protection with regard to teleservices and shall make relevant comments. In his Acivity Report 2001 and 2002 of 7 May 2003 (*Bundestagsdrucksache* 15/888), p. 20 no.1.8 and p. 76 no 11.2.2) he has pointed out the relevance of the application of the TDDSG in the practical use. He says that more and more providers of the Internet implement the rules of this act. But he criticizes that in the result an overall improvement of the data protection with teleservices cannot be noticed

Grèce

Le problème de la protection des données à caractère personnel au regard de l'emploi par les détenteurs de droits de propriété intellectuelle sur des matériaux accessibles via Internet de technologies permettant l'identification des personnes y ayant accès ne s'est pas encore posé en Grèce. De plus, la directive « vie privée et communications électroniques » (directive 2002/58 du Parlement européen et du Conseil, du 12 juillet 2002) n'a pas encore été transposée en droit interne. Dans l'état actuel du droit grec, les utilisateurs d'Internet pourraient invoquer les garanties de la loi no 2774/1999, sur la « Protection des données à caractère personnel dans le secteur des télécommunications » (transposant en droit interne la directive no 97/66 du Parlement européen et du Conseil) contre les éventuelles atteintes au droit au respect de leur vie privée.

L'art. 5 de la loi susmentionnée prévoit que les données de trafic concernant les abonnés et les utilisateurs traitées en vue d'établir des communications et stockées par le fournisseur d'un réseau de télécommunications ou d'un service de télécommunications accessible au public doivent être effacées ou rendues anonymes dès que la communication est terminée. Certaines données, énumérées dans le par. 2 du même article, dont le numéro ou le poste de l'abonné, peuvent être traitées, pendant une durée limitée, dans le but d'établir les factures des abonnés et aux fins de paiement pour interconnexion. Sur demande de l'utilisateur ou de l'abonné, le fournisseur d'un réseau de télécommunications ou d'un service de télécommunications accessible au public doit éliminer les trois derniers chiffres des numéros appelés ou encore tous les numéros appelés, immédiatement après l'envoi de la facture (par. 3). Le traitement des données de trafic et de facturation doit être confié à des personnes agissant sous l'autorité des fournisseurs susmentionnés, chargées d'assurer la gestion de la facturation ou du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de télécommunications du prestataire (par. 4).

Le traitement des données de trafic est soumis aux principes généraux régissant la protection de toutes les données personnelles dans le secteur visé par la loi. Le traitement est permis uniquement (a) lorsque l'abonné ou l'utilisateur a donné son consentement informé quant à la nature des données, les finalités et l'étendue du traitement, les destinataires ou les catégories de destinataires des données ou (b) lorsque le traitement est nécessaire à l'exécution d'un contrat auquel l'abonné ou l'utilisateur est

partie ou à l'exécution de mesures précontractuelles prises à la demande de l'abonné (art. 4 par. 2). De plus, le traitement doit être limité à ce qui est absolument nécessaire au regard de ses finalités (art. 4 par. 3). Le consentement explicite et révocable, donné, en plus, par écrit, de la personne intéressée est nécessaire pour le transfert des données à des tiers, en vue, notamment, de leur utilisation à des fins de prospection commerciale. La fourniture des services visés par la loi ne peut pas dépendre du consentement de l'utilisateur ou de l'abonné pour le traitement des données à d'autres finalités (art. 4 par. 4). Selon le par. 6 du même article, le fournisseur des services de télécommunication accessibles au public doit permettre l'utilisation et le paiement anonyme ou par pseudonyme, si cela est techniquement possible (l'avis de la Commission Nationale des Télécommunications et des Postes pouvant être sollicité sur ce point).

Dans un avis rendu en 2002[80], l'Autorité indépendante pour la protection des données personnelles a estimé que les données de trafic et de facturation qui concernent les abonnés et utilisateurs des services de télécommunication accessibles au public sont des données à caractère personnel. L'échange de ces données entre des fournisseurs de services de télécommunication est permis, sans autorisation de l'Autorité, si les utilisateurs ou les abonnés en sont informés lors de la conclusion des contrats y relatifs et que l'échange est nécessaire pour la facturation des services fournis.

Dans un autre avis intéressant concernant les atteintes potentielles à la vie privée sur Internet, l'Autorité a estimé que la "fouille" ("data mining") de données personnelles, listes et adresses électroniques ne légitime pas l'utilisation de ces données à des finalités autres que celles pour lesquelles elles ont été enregistrées[81].

Ireland

In Irish law there is an unspecified constitutional right to privacy the precise parameters of which remain unclear. The right has been developed in case law on a number of occasions but has only been dealt with through legislation in specific areas, e.g. the tapping of telephonic communications and general data protection.

The independent authority charged with the protection of personal data is the Office of the Data Protection Commissioner (www.dataprotection.ie/). The most recent legislation dealing with the powers and functions of that body is the Data Protection (Amendment) Act, 2003 (No. 6 of 2003).

In relation to the retention of traffic data, the practice in Ireland is to retain such data for a period of three years. This is done on the basis of ministerial or executive direction (pursuant to Section 110(1) of the Postal and Telecommunications Services Act, 1983 (as amended)) and serious concerns have been expressed by the Data Protection Commissioner about both this practice and its insufficient legal basis[82].

Although it is planned to introduce legislation in this area and there has been some public debate on the matter the requirements of combating crime would appear to be given greater weight than the right to individual privacy as things stand. This may lead to the Data Protection Commissioner taking infringement proceedings against the Irish Government in the event of inactivity on the legislative side on the basis of his understanding of the aforementioned direction as a temporary holding measure.

[80] Avis no 78/2002.
[81] Avis no 19/2002.
[82] Statement of Data Protection Commissioner at the Forum on the Retention of Communications Traffic Data, 24th February, 2003. (Accessible via www.dataprotection.ie).

Italie

Par le décret législatif du 30 juin 2002 n° 196 - Code en matière de protection de données personnelles (*Decreto legislativo 30 giugno 2002 n. 196 - Codice in materia di protezione di dati personali*), l'Italie a consolidé les dispositions existant en la matière dans un texte unique, en apportant également des modifications à la discipline en vigueur. Le Code entrera en vigueur au 1er janvier 2004.

Sous le titre X (Communications électroniques), le code prévoit trois parties: I - Services de communication électronique, II - Internet et réseaux télématiques, III - Vidéosurveillance.

Les dispositions concernant les données de trafic sont prévues sous la première partie.

> "Article 123 (Données relatives au trafic)
> 1. Les donnés relatives au trafic, concernant les abonnés et les utilisateurs, traitées par le fournisseur d'un réseau public de communication ou d'un service de communication électronique accessible au public sont effacées ou rendues anonymes lorsque elles ne sont plus nécessaires à la transmission de la communication électronique, exception faite des dispositions des paragraphes 2, 3 et 5.
> 2. Le fournisseur est autorisé au traitement des données relatives au trafic strictement nécessaires à la facturation de l'abonné, ou au paiement en cas d'interconnexion, pour une période non supérieure à six mois, cela dans le but de garder une documentation en cas de contestation de la facture ou pour obtenir le paiement, exception faite d'une ultérieure spécifique conservation nécessaire à la suite d'un litige en justice.
> 3. Le fournisseur d'un service de communication électronique accessible au public peut traiter les données mentionnées au paragraphe 2 dans la mesure et pendant la durée nécessaires à la commercialisation de services de communication électronique ou à la fourniture de services à valeur ajoutée, cela seulement si l'abonné ou l'utilisateur ont manifesté leur consentement, qui est révocable à tout moment.
> 4. En fournissant les informations prévues à l'article 13, le fournisseur du service informe l'abonné ou l'utilisateur de la nature des données de trafic soumises au traitement et de la durée du traitement dans les buts des paragraphes 2 et 3.
> 5. Le traitement des données personnelles relatives au trafic est consenti uniquement aux personnes chargées du traitement qui opèrent au sens de l'article 30 sous l'autorité directe du fournisseur du service de communication électronique accessible au public ou, selon les cas, du fournisseur du réseau public de communications et qui s'occupent de la facturation ou de la gestion du trafic, de l'analyse pour des clients, de la vérification des fraudes ou de la commercialisation des services de communication électronique ou de la prestation de services à valeur ajoutée. Le traitement est limité à ce qui est strictement nécessaire au déroulement de ces activités et doit assurer l'identification de la personne chargée qui accès aux données même au moyens d'une opération d'interrogation automatisée.
> 6. L'Autorité pour les garanties dans les communications peut obtenir les données relatives à la facturation ou au trafic nécessaires à la résolution des disputes concernant, en particulier, l'interconnexion ou la facturation. »

Rien n'est dit quant à Internet et aux autres réseaux télématiques. L'article 133, inclus sous la partie II du titre X, prévoit: "Le Garant (*de la protection de données personnelles*) promeut, au sens de l'article 12, la souscription d'un code de déontologie et de bonne conduite pour le traitement des données personnelles effectué par les fournisseurs de services de communication et information offerts à travers de réseaux de communication électronique, ayant égard en particulier aux critères qui assurent et uniformisent une information et une conscience plus adéquates des utilisateurs de réseaux de communication électronique gérés par des sujets publics et privés par rapport aux genres de données traitées et aux modalités de traitement, en particulier à travers des informations fournies de manière aisée et interactive, afin de favoriser une transparence et un corrections plus amples à l'égard des utilisateurs et le plein respect des principes prévus par l'article 11 (…).

Le code de déontologie mentionné à l'article 133 n'a pas encore été émis.

Luxembourg

Le Grand-Duché de Luxembourg ne s'est pas encore doté de réglementations nationales concernant la protection de données à caractère personnel des utilisateurs d'Internet, en particulier au regard de l'emploi par les détenteurs de droits de propriété intellectuels sur des matériaux accessibles via Internet de technologies permettant l'identification des personnes y ayant accès. En particulier, le Grand-Duché de Luxembourg n'a pas pris les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive 97/66/CE du Parlement européen et du Conseil, du 15 décembre 1997, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO L 281 du 23.11.1995). A plus forte raison, la directive 2002/58/CE n'a-t-elle pas encore été transposée.[83]

Le 11 juillet 2003, un projet de loi sur la protection des données en matière de communications électroniques a été déposé (Projet de loi, 1. relatif aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques ; 2. portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle ; 3. Portant modification de la loi du 2 août 2002 relative à la protection de la personne à l'égard du traitement des données à caractère personnel, Documents parlementaires n° 5181).

Il n'y a, dans le domaine concerné, pas d'avis de la Commission nationale pour la protection des données.

Malta

This is, for Malta, a rather novel problem and it is only recently that it has been specifically regulated by national legislation. Two Acts of the Maltese Parliament have specifically dealt with these issues; they are the Data Protection Act[84] and the Electronic Commerce Act[85]. Both Acts purport to regulate matters and aspects of technological transmission of data and information.

The Data Protection Act is meant, among other things, to safeguard the privacy of the individual in respect of personal data. The Act is meant to give effect to and purports to be in accordance with the Data Protection Directive (95/46 EC)[86]. The Act implements the principle that the data subject must be aware and informed of the intended uses to be made of data obtained from him. The Act also sets up the independent Data Protection Commissioner to safeguard the interests posed by data transfer and privacy.

The other Act pertinent to this discussion is the Electronic Commerce Act. Two points have to be made in relation to the Act as far as the subject matter of the present discussion is concerned: first, the Act empowers the Minister responsible for Communications to make regulations derogating from or restricting cross border transactions where such is necessary because of public policy, the protection of public health, public security, and consumer protection[87]; second the Act creates a new sub title in the Criminal Code referring to computer misuse[88]. Broadly the Act makes criminal the unlawful access to and use of information supported on computer systems as well as the misuse of the hardware itself. The relevant sections cover a broad range of illicit activity from accessing data, software, or

[83] Pour une constatation de ce manquement, voy. C.J.C.E., 6 mars 2003, Commission des Communautés européennes c/ Grand-Duché de Luxembourg,aff. C-211/02, pas encore publié au Recueil.
[84] Chapter 440 of the Laws of Malta enacted by Act XXVI of 2001 and brought into force by a number of legal notices spanning the years 2002 to 2003.
[85] Chapter 426 of the Laws of Malta enacted by Act III of 2001 and brought into force on the 10th May 2002.
[86] White Paper on the Legislative Framework for Information Practices, May 2000, Office of the Malta Prime Minister, Part III: The Data Protection Bill explained, para 1.2.
[87] Section 25 of the Electronic Commerce Act.
[88] Sections 337(B) to 337(G) of the Criminal Code, Chapter 9 of the Laws of Malta.

supporting information in computers, to using, copying and modifying same, as well as interfering with such data, software and supporting information in a variety of manners.

Portugal

At present, only the general rules of the Portuguese Data Protection Act (Law 67/98, of 26th October 1998) and of the Telecommunications Act (Law 69/98, of 28th October) apply to the protection of Internet users' data. Portugal has no specific rules referring to the data protection of the users' of the Internet, namely on the retention of traffic data. Directive 2002/58/CE concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications) has not yet been transposed, therefore, the processing of personal data involving Internet users is still submitted to the general rules on data protection.

The Telecommunications Act made no special reference to electronic communications, although the Portuguese Data Protection Authority (Comissão Nacional de Protecção de Dados)[89] tended to consider its provisions were applicable to electronic communications as well.

Until present, retention of any telecommunication users' data is possible only for transmission of the communication and billing purposes, according to article 6 of the Telecommunications Act. As personal data are collected for telecommunication transmission and billing purposes, the general rule applies: data should be kept for no longer than necessary for the purposes for which they were collected or for which they were further processed (article 5. 1.e of the Data Protection Act).

The Parliament may soon discuss some law projects ruling the users' of Internet personal data processing[90]. One of these projects intends to transpose the European Directive 2002/58/CE (Project 208/IX).The other, related to digital evidence, proposes to rule on the retention of traffic data (Project 217/IX).

Both projects make reference to personal data retention in what concerns electronic communications. None of them has any special rule with respect to the technological devices used by holders of intellectual property rights on material accessible via the Internet.
The Portuguese Data Protection Authority has the power to issue opinions on new legislation concerning personal data and within the exercise of that opining capacity it has taken position referring to the above mentioned Projects of Law 208/IX and 217/IX.[91].

These opinions contained severe critics on many aspects, namely on the traffic data retention periods proposed. Opinions have recalled that Council of Europe's Convention on Cybercrime – and some initial versions of the European Directive on Electronic Communications - did not impose traffic data retention for security purposes[92]. They have also considered that this new legislation is reversing the true intention of this European Directive provision that was meant to be of exceptional use.

Project of Law 208/IX, presented by the Socialist Party, suggests a period of traffic data retention that should last for a minimum of 6 month, and Project of Law 217/IX, of the Popular Party, proposes a

[89] www.cnpd.pt.
[90] Project 208/IX presented by socialist party may be found at:
http://www.assembleiadarepublica.pt/legis/inic_legis/20030122.09.1.0208.1.08.
And Project 217/IX presented by the Popular Party:
http://www.assembleiadarepublica.pt/legis/inic_legis/20030130.09.1.0217.1.04.
[91] These opinions have been published on the Internet: Opinion 10/2003, about the Project of Law 217/IX:
http://www.cnpd.pt/actos/par/2003/par010-03.htm
Opinion 12/2003, about the Project of Law 208/IX: http://www.cnpd.pt/actos/par/2003/par012-03.htm.
[92] This reference is made on the Opinion about Project of Law 217/IX. It also remembered that Article 29 Data Protection Working Party had issued some opinion considering that there should be no systematic traffic data retention, and that it should always respect proporcionality and necessity (see, namely, opinion 4/2001, about Cybercrime Convention, defending that there should be no traffic data retention).

minimum retention period of 1 year. None of these projects establishes any maximum period for traffic data retention, which amounts to a clear violation of the principle of proportionality.

The Project on Digital Evidence (217/IX) was also criticised because it diverged from Council of Europe Cybercrime Convention by intending to admit traffic data retention not only for criminal investigation, but also for preventive effects (Project 208/IX has a similar provision); it imposed an obligation of identification upon every user of the Internet, in every circumstance – their data would be kept by the service provider for an unknown period of time - in a clear violation of the "right to be let alone". On the other hand, the traffic retention period proposed on this Law Projects was considered as being excessive.

Espagne

Législation applicable

La Loi organique n°15/1999, du 13 décembre 1999, relative à la protection des données à caractère personnel (BOE nº 298, de 14 décembre 1999), ne règle pas spécifiquement la question abordée par cet avis, mais elle contient les principes et les garanties de la protection des données. Elle établit l'Autorité indépendante de contrôle (*Agencia de Protección de Datos*).

La Loi n° 34/2002 du 11 juillet 2002 des services de la société d'information et du commerce électronique contient certaines dispositions relatives à la rétention des données de trafic (article 12). Seules les données nécessaires à l'établissement et à la facturation de la communication peuvent être conservées pendant une durée maximale de 12 mois. Il y est également précisé qu'en aucun cas l'obligation de rétention de telles données ne peut porter atteinte au principe de la confidentialité des (télé)communications.

Le Royal décret-loi 14/1999 du 17 septembre 1999 relatif à la signature électronique (BOE du 18 septembre 1999) crée dans le chef des prestataires de services de certification reconnus, l'obligation de conservation, notamment par la voie informatique, de toute information et documentation relative à cette certification pendant une durée de 15 ans.

Le Royal décret 994/1999 du 11 juin 1999 portant approbation du règlement des Mesures de Sûretés des Fichiers automatisés, prévoit des mécanismes de protection quant à l'accès à ces données (article 5) et dispose que les fichiers temporaires doivent être effacés dès que la finalité pour laquelle ils ont été créés a été rencontrée.

On mentionnera encore la Résolution du 8 juillet 2002 du Secrétariat d'Etat au Budget et Frais relativement au contrôle de l'accès aux bases de données de ce Secrétariat d'Etat et la mise en place d'un système télématique de communication entre la Commission nationale du Marché des Valeurs et ses utilisateurs, lequel vise à garantir l'authenticité, la confidentialité et l'intégrité des informations et à réglementer leur disponibilité et leur conservation (BOE du 27 mars 1998).

L'article 197 du Code pénal sanctionne, pour sa part, l'utilisation ou la modification non autorisée de données à caractère personnel placées dans des fichiers ou supports informatiques, électroniques ou télématiques. La peine encourue est plus sévère lorsque l'auteur de l'infraction est le responsable du fichier ou lorsque le traitement est effectué dans un but lucratif.

Au niveau de la Communauté autonome de Madrid, on mentionnera la Loi 13/1995 du 21 avril 1995 relative à l'informatique appliquée au traitement des données à caractère personnel.

Avis des autorités indépendantes de contrôle

L'Agencia de Proteccion de datos, soit l'autorité indépendante nationale en matière de protection des données à caractère personnel, a formulé quelques recommandations en la matière :

Outre celles, générales, émise en 1997, *l'Agencia de Proteccion de datos* s'est penchée sur la question du respect par le secteur du commerce électronique, des prescriptions de la Loi Organique 15/1999 relative à la protection des données à caractère personnel. L'*Agencia* a procédé à l'examen de nombreux sites Internet proposant un service d'achat « on line ». Elle a dû constater que seuls 54% des sites visités utilisaient le protocole FTTPS (SSL) pour établir un canal de transmission sûr pour l'envoi de données à caractère personnel. L'absence de garantie de protection suffisante était plus flagrante encore lors d'accession à une page web par hyperlien. L'*Agencia* a donc adopté une série de recommandations spécifiques relatives à l'information de l'internaute en cas de collecte de données, au consentement des utilisateurs d'Internet, aux finalités autorisées de traitements etc. Les données de santé ont fait l'objet d'une attention spécifique.

Plus récemment, l'*Agencia* a fait savoir qu'elle n'était pas favorable à la transmission des données relatives aux passagers des lignes aériennes vers les Etats Unis aux autorités américaines. Elle conseille aux compagnies aériennes de recueillir le consentement exprès des passagers sur tout transfert de telles données aux services de douanes américaines.

La Communauté autonome de Madrid dispose également de son *Agencia de Proteccion de datos* propre. Cette dernière a également rendu un rapport sur la protection des données des utilisateurs d'Internet. La Catalogne vient de mettre sur pied un organe comparable lequel n'a pas encore débuté ses travaux.

Autres avis concernant la protection des utilisateurs d'Internet

Afin de garantir l'utilisation adéquate des moyens techniques et informatiques du Ministère de la Justice et des Communautés autonomes titulaires de compétences en ce domaine, le *Consejo General del Poder judicial* (Conseil général de la Magistrature) a édicté *l'Instruccion 2/2003* laquelle contient un Code de conduite à l'attention des utilisateurs des moyens informatiques au sein de l'administration de la Justice.

Sweden

A new Act on electronic communications (*Lag om elektronisk kommunikation* (SFS 2003:389)) entered into force on 25 July 2003. This important legislative reform took place in order to make the domestic regulations in the relevant area of law compatible with the five EU Directives.[93] All the Directives implemented deal with the issue of electronic communications. Provisions regarding the processing of personal data are laid down in Directive 2002/58/EC (Directive on privacy and electronic communications). This Directive particularises and complements Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Directive 95/46/EC is incorporated into Swedish law through the Personal Data Act (Personuppgiftslagen (SFS 1998:204)). The purpose of this legislation is to protect individuals against the violation of their personal integrity by processing of personal data.[94] If another statute, for example

[93] Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), Directive 2002/20/EC on the authorisation of electronic communications networks and services (Authorisation Directive), Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive), Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[94] Personal Data Act Section 1.

the new Act on electronic communications, contains provisions that may be found to deviate from the Personal Data Act, the provisions of the latter shall apply.[95]

Personal data may, according to the main rule in Section 10 of the Personal Data Act, only be processed if the registered person has given his/her consent to the processing. However, there are some exceptions and personal data may, for example, be processed if necessary in order to perform a work task in conjunction with the exercise of official authority.[96]

According to Article 5.1 of Directive 2002/58/EC, Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned. According to the Government Bill, which deals with the new act, Article 5 of the Directive is of fundamental importance for the protection of privacy in the electronic communications sector.[97] The Article is implemented through Chapter 6 Section 17 of the Act on electronic communications. According to the Directive the prohibition of storage of communications and the related traffic data by persons other than the users or without their consent shall not prevent technical storage which is necessary for the conveyance of a communication.[98] This exemption is implemented in the new act.[99]

The storage of traffic data is also dealt with in Article 6 of the Directive and in Chapter 6 Sections 5 to 8 in the Act on electronic communications. The principal rule entails that traffic data relating to subscribers and users, processed and stored by the provider of a public communications network or publicly available electronic communications service, shall be erased or made anonymous when it is no longer required for the transmission of a communication. There are several exemptions from the prohibition of storing and processing traffic data. Both the Directive and the Swedish act contain provisions which permit the processing of traffic data when, for example, it is necessary for the purposes of subscriber billing and interconnection payments.[100]

The Act on electronic communications contains provisions concerning the security of processed data.[101] The provider of a publicly available electronic communications service and the provider of the public communications network shall take appropriate measures to safeguard the security of processed data. According to the Government Bill which deals with the new act the security of processed data comprises the security of personal data.[102]

The Data Inspection Board (Datainspektionen) is the supervisory authority in Sweden as regards the processing of personal data and it has commented upon the Act on electronic communications.[103] The Data Inspection Board has underlined that Article 4 of Directive 2002/58/EC, concerning security, is to be appraised in the light of Directive 95/46/EC.[104] The Data Inspection Board is, therefore, of the opinion that Chapter 6 Section 3 of the Act on electronic communications, which regulates the security, should contain a reference to the relevant provisions of the Personal Data Act.

[95] Personal Data Act Section 2 and Act on electronic communications Chapter 6 Section 2.
[96] Personal Data Act Section 10 para. e.
[97] Prop. 2002/03:110 Lag om elektronisk kommunikation pp. 252-255.
[98] Directive 2002/58/EC Article 5.1 and para. 22 of the preamble.
[99] Act on electronic communications Chapter 6 Section 17 para. 2.
[100] Directive 2002/58/EC Article 6.2 and Act on electronic communications Chapter 6 Section 6.
[101] Directive 2002/58/EC Article 4 and Act on electronic communications Chapter 6 Sections 3-4.
[102] Government Bill, Prop. 2002/03:110 Lag om elektronisk kommunikation pp. 250-252.
[103] Opinion on the proposal on a new Act on electronic communications, (Yttrande över förslag till ny lagstiftning om elektronisk kommunikation (SOU 2002:60)).
[104] Directive 2002/58/EC para. 20 of the preamble.

The Netherlands

The leading Dutch case of the moment is *Teleatlas*, which was decided, in summary proceedings, by the *Rechtbank* [Regional Court] of Utrecht in July 2002 (LJN nr. AE5537). Teleatlas, a software producer, believed that Internet users where illegally copying its software and selling them at sites such as *eBay*. Wishing to bring proceedings against the Internet user 'X' who offered Teleatlas software for sale without authorisation, Teleatlas requested the Internet service provider Planet to provide it with the name, address and telephone number of 'X', who was a subscriber to Planet. Planet refused, arguing *inter alia* that the *Wet bescherming persoonsgegevens (WBP)* [Data Protection Act] did not allow the release of these data.

When Teleatlas brought proceedings against Planet, the Regional Court observed that Article 8, sub f, WBP only allows the release of data if (a) this is necessitated by the legitimate interests of a third party, and (b) the fundamental rights and freedoms of the person concerned, and notably his right to protection of private life, do not prevail. In answering the question whether in a specific case the release of data is permissible, an important question is if other – less intrusive – means are available to achieve the aim pursued.

Turning to the facts of the instant case, the Regional Court noted that Teleatlas had not really pursued alternative ways to identify 'X', despite a number of alternatives suggested by Planet. For instance, Planet had offered to block X's access to Internet, but this offer had not been accepted. On these grounds the court dismissed the action brought by Teleatlas.

The *College bescherming persoonsgegevens (CBP)* [Data Protection Authority] is the independent supervisory authority that monitors the application of the legislation concerning the processing of personal data. Although the CBP has not delivered any recent opinions that are directly relevant to our topic, it did advise, in 2002, the Minister of Justice to amend the *Wetsvoorstel Kansspelen Internet* [draft Gambling (Internet) Act], so as to enhance the protection of the privacy of those taking part in games through Internet.

United kingdom

There is no general regulation addressed specifically to the protection of personal data of the users of the Internet but such data, insofar as it is collected or retained by someone in the United Kingdom or on equipment located there, is governed by the Data Protection Act 1998 which regulates the collection and retention of such data. This legislation confers through section 28 a general exemption on the application of this legislation in respect of personal data where this is required for the purpose of safeguarding national security and the need for such an exemption is something that can be conclusively determined by a Minister of the Crown.

There is provision the Regulation of Investigatory Powers Act 2000, s 22 enabling access to be obtained to communications data where necessary: in the interests of national security; for the purpose of preventing crime or of preventing disorder; in the interests of the economic well-being of the United Kingdom; in the interests of public safety; for the purpose of protecting public health; for the purpose of assessing or collecting any tax; duty, levy or other imposition, contribution or charge payable to a government department; for the purpose, in an emergency, of preventing death or injury, or of mitigating any injury or damage to a person's physical or mental health; or for any purpose specified by an order made by the Secretary of State. Communications data includes data comprised in or attached to a communication, information about the use made by a person of the communications service and any other information held or obtained in relation to to persons to whom the service is provided (s 21(4)).

Furthermore under the Anti-terrorism, Crime and Security Act 2001 there is provision for the adoption of codes of practice about, or the conclusion of agreements on, the retention of communication data by

communications providers for the purpose of safeguarding national security or the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security (s 102). In addition there is power, after reviewing the operation of provisions in the code of practice or agreements, to make an order giving directions with regard to the retention of data, whether directed to communication providers generally, those of a specific description or particular ones. The duty under such directions shall be enforceable by civil proceedings for an injunction. An order may be made for an initial period of two years but may be extended with parliamentary approval. No order has so far been made but a code has been adopted (http://www.homeoffice.gov.uk/docs/retention_of_communications_data.pdf). The need for a communications service provider to retain data routinely for the prevention of terrorism for any longer than the data would normally be retained for its own business purposes has been doubted by the Information Commissioner (http://www.dataprotection.gov.uk/dpr/dpdoc.nsf (Anti-terrorism Crime and Security Act 2001 – Part 11 Retention of Communications Data). In his view, if there is a need, retention should be on the basis of a statutory duty, providing a greater degree of certainty than is possible with a voluntary agreement. Although the Commissioner considered the code to be a workable document which correctly set out the data protection considerations for communication service providers, he was concerned about the code referring to the possibility of the national security exemption under the Data Protection Act 1998, s 28 being invoked as it was not clear what this could add to the code's provision on the retention of data needed for national security purposes. He considered that the retention period of twelve months provided for in the code was a cause of less concern than earlier proposals. He also expressed concern about the need to control access to the relevant data where this was not for national security purposes.