inter *net*

Le Nouveau Média Interroge Le Droit

Rapport d'un groupe interdépartemental sur des questions relevant du droit pénal, du droit de la protection des données et du droit d'auteur suscitées par Internet

Office fédéral de la Justice, Berne, mai 1996

Table des matières

I. Objectif et origine

Le présent rapport offre une vue d'ensemble des questions que soulève le réseau mondial de données Internet sous l'angle du droit pénal, du droit de la protection des données et du droit d'auteur. Des recommandations y sont formulées à l'attention des fournisseurs d'accès à Internet (access providers). Ces recommandations ont pour but de contribuer à empêcher l'utilisation abusive et illicite de réseaux de données, et sont destinées à soutenir les efforts déployés par la branche pour élaborer un code de conduite à l'attention des fournisseurs d'accès[1].

Par lettre du 13 juillet 1995, la Direction générale des PTT, département Télécom, a demandé à l'Office fédéral de la justice de coordonner l'élaboration d'éventuelles recommandations dans la perspective d'une entrée sur le marché des fournisseurs d'Internet de UBN (Unisource Business Networks, filiale d' Unisource Holding à laquelle participent les Télécom PTT). Compte tenu des expériences faites avec l'arrêt du Tribunal fédéral, dit „du 156" (ATF 121 IV 109), les Télécom PTT ont à coeur d'éclaircir la question de la *punissabilité à laquelle pourrait les exposer leur qualité de fournisseurs d'Internet* et des mesures qu'ils devraient adopter pour écarter un tel risque.

Dans sa question ordinaire du 24 mars 1995, le conseiller national Bischof a mis l'accent sur la *protection de la jeunesse contre la violence dans les jeux vidéo et informatiques*. Le 31 mai 1995, le Conseil fédéral a notamment souligné dans sa réponse que le Département fédéral de justice et police engagerait le dialogue avec les organisations privées des branches concernées afin de les encourager à renforcer l'efficacité des contrôles qu'elles s'imposent librement. Dans la mesure où de tels jeux font de plus en plus l'objet d'une exploitation sur réseaux également, il s'imposait de traiter l'aspect particulier d'Internet soulevé par la question ordinaire Bischof dans le contexte de la demande formulée par les Télécom PTT.

---

[1] Un groupe de travail privé, dirigé par EU-Net et baptisé "Internet et droit", se propose notamment d'élaborer un code de conduite pour fournisseurs. Des représentants de l'OFCOM et du Préposé fédéral à la protection des données participent également à ce groupe de travail en qualité d'observateurs.

Les questions posées ne représentent évidemment qu'une minuscule parcelle des problèmes juridiques que soulève le développement extrêmement rapide d'Internet. Il va de soi que l'extension globale de ce média, ses possibilités techniques, le nombre de ses utilisateurs, estimé à quelque 40 millions dans le monde, de même que l'absence d'exploitant identifiable et responsable recèlent également d'importants risques d'abus, dont les médias font de plus en plus souvent état ces derniers temps.

Dans ces conditions, il a paru judicieux d'aborder cette problématique de manière plus large, en associant d'autres offices intéressés. A cet effet, la séance qui s'est déroulée le 6 septembre 1995 dans les locaux de l'Office fédéral de la justice réunissait des représentants de l'Office fédéral de la communication, des PTT, de l'Office fédéral de l'informatique, du Préposé fédéral à la protection des données, du Secrétariat général du DFJP (organisation de projets BASIS), de l'Institut fédéral de la propriété intellectuelle ainsi que du Ministère public de la Confédération. Cette séance a donné naissance à un groupe de travail interdépartemental[2], qui a étudié la question au cours de trois autres séances. Dans ce contexte, il a aussi tenu compte du postulat du 23 janvier 1996[3], concernant la „pornographie enfantine sur Internet" et déposé par la Commission des affaires juridiques du Conseil national, qui demande un rapport sur les *moyens d'empêcher la diffusion de pornographie enfantine par le biais de réseaux internationaux de données* (Internet).

Les questions juridiques liées à Internet sont extraordinairement complexes et diverses. De plus, ce média se distingue par un essor technique fulgurant dont il n'est guère possible de prévoir l'évolution aujourd'hui. De ce fait, le présent rapport ne saurait dépasser le stade d'un bilan provisoire et les recommandations qui en découlent doivent être comprises en tant qu'instrument provisoire et incomplet pour lutter contre les abus d'Internet.

---

[2] Sa composition variable était la suivante:
Office fédéral de la justice: Peter Müller, sous-directeur (présidence), Chantal Favre, Ernst Gnägi
SG DFJP (BASIS): Martin Keller, Bernard Werz
Office fédéral de la police: Peter Blaser
Ministère public de la Confédération: Roland Hauenstein
Institut fédéral de la propriété intellectuelle: Andreas Stebler, Pascal Koster
Préposé fédéral à la protection des données: Katrin Atia-Off
Office fédéral de la communication: Ursina Wey, René Dönni
DG PTT: Albert Känzig, Andreas Locher, Peter Martin, Hans-Ulrich Hauser, Marie-Claire Cominoli
Office fédéral de l'informatique: Herbert Roth, Claudio Frigerio

[3] Par décision du 4 mars 1996, le Conseil fédéral s'est déclaré disposé à accepter le postulat.

II. Aspects du droit pénal

1. Catégories d'infractions concernées

En théorie, les auteurs d'infractions peuvent abuser de multiples façons des réseaux informatiques comme Internet ou des réseaux d'importants services connectés en ligne pour parvenir à leurs fins. Le large éventail des infractions dont la commission implique le recours à des réseaux permet toutefois d'opérer une distinction grossière entre deux catégories principales: il s'agit, d'une part, des infractions spécifiquement dirigées contre le réseau et les systèmes de traitement de données raccordés à celui-ci, et d'autre part, des infractions pour lesquelles des réseaux servent de support de communication.

La première catégorie englobe essentiellement les *délits informatiques*, dont la définition pénale est entrée en vigueur le 1er janvier 1995. Il est ainsi parfaitement imaginable que le recours à Internet ou à un autre réseau puisse également donner lieu à une soustraction de données (art. 143 CP), à un accès indu à un système informatique (art. 143bis CP), à une détérioration de données (art. 144bis CP), à une utilisation frauduleuse d'un ordinateur (art. 147 CP) ou à une obtention frauduleuse d'une prestation au sens de l'article 150, 4e alinéa, CP. Toutefois, dans la mesure où ces dispositions pénales ne sont en vigueur que depuis une année, il n'existe pas encore de jurisprudence relative à des affaires spécifiquement liées à Internet permettant d'apprécier l'efficacité de ces normes à l'égard des délits informatiques commis sur des réseaux. Le groupe de travail estime qu'il n'y a pour l'instant pas lieu de compléter la législation applicable dans ce domaine.

Les infractions de la seconde catégorie sont en premier lieu des *délits d'opinion*. On songera en particulier aux dispositions relatives à la *représentation de la violence* (art. 135 CP), à la *pornographie* (art. 197 CP) et à la *discrimination raciale* (art. 261bis CP)[4]: d'une part, les infractions commises sur Internet et recensées en Suisse et à l'étranger relèvent dans une très large mesure de ces trois dispositions. D'autre part, en tant que média planétaire permettant la diffusion de l'écriture, de l'image et du son, Internet se prête extrêmement bien à

[4] D'autres exemples de délits d'opinion se trouvent parmi les délits contre l'honneur (art. 173 ss CP), les violations de secrets (p.ex. art. 320 et 321 CP), la provocation publique au crime ou à la violence (art. 259 CP), diverses formes de détérioration de données au sens de l'article 144bis, ch. 2, CP, telle la fourniture d'indications en vue de la fabrication de virus informatiques, etc.

la commission de délits d'opinion. De plus, la question de la coresponsabilité pénale du fournisseur revêt une portée pratique accrue dans ces infractions. En effet, par le seul fait de publier, de communiquer ou de diffuser des informations dont la teneur est illicite, les personnes qui participent à de tels actes en connaissance de cause remplissent relativement vite les éléments constitutifs de l'intention punissable.

C'est pourquoi il s'impose d'étudier la question de la punissabilité en général, et de celle du fournisseur, en particulier, sur la base des trois formes d'infractions précitées lorsqu'elles sont commises sur Internet (ci-après II. 2.). Avant d'évoquer les mesures de prévention (II. 4.) ainsi que les moyens techniques de prévention (II. 5.), puis de développer des recommandations de droit pénal spécifiquement destinées aux fournisseurs d'accès (II. 6.), il convient de faire une brève digression (II. 3.) sur deux autres secteurs d'infractions ainsi que sur des modifications qui seront introduites incessamment dans le domaine du droit pénal et de la procédure pénale des médias[5].

2. Représentation de la violence, pornographie et discrimination raciale

a) Questions générales de la punissabilité dans le cadre d'Internet

Ainsi que déjà souligné, les principales infractions liées à Internet et à d'autres services connectés en ligne trouvent leur définition pénale aux articles 135 (Représentation de la violence), 197 (Pornographie) et 261bis (Discrimination raciale). Les éléments constitutifs de ces infractions ne requièrent aucune explication particulière: le caractère violent, pornographique ou raciste d'une représentation au sens du code pénal se détermine en fonction des principes généraux; le fait que de telles représentations soient diffusées par le biais d'un organe de presse, d'un film ou d'un réseau ne joue aucun rôle à cet égard. Il en va de même de la définition de la pornographie dite „douce" au sens de l'article 197, chiffre 1 CP. Nous reviendrons cependant plus loin sur les effets spécifiques de cette disposition pénale sur Internet (protection de la jeunesse).

Lorsqu'une représentation, diffusée et captée sur un réseau, remplit les éléments constitutifs objectifs de l'une des trois infractions susmentionnées, il convient d'admettre de prime abord que le *destinataire*, dont l'activité personnelle se borne à regarder la représentation en question, ne se rend pas punissable en vertu du

[5] Pour les infractions concernant les droits d'auteur cf. ci-dessous IV.

droit en vigueur puisque la simple possession/consommation de représentations violentes, racistes ou pornographiques ne constitue pas une infraction. On pourrait toutefois se demander si la possession/consommation de l'utilisateur ne remplit pas les éléments constitutifs de l'importation et de la prise en dépôt au sens des articles 135 et 197, chiffre 3 CP. On pourrait par exemple arguer du fait que l'enregistrement (durable) de scènes de violence et de pornographie „dure" entre dans la notion de prise en dépôt. De même pourrait-on estimer qu'en transférant sur son PC ce type de données en provenance de l'étranger, l'utilisateur remplit les éléments constitutifs de l'importation. Une interprétation aussi extensive serait néanmoins contraire à la volonté du législateur, qui a clairement précisé que la simple possession/consommation de représentations de la violence et de pornographie „dure" ne devait pas tomber de lege lata sous le coup du droit pénal. En d'autres termes, si le comportement de l'usager se limite à la simple consommation de ces représentations et qu'il n'y a aucune intention de les rediffuser, il demeure difficile de soumettre ce comportement au droit pénal en vigueur.

A l'avenir, la situation pourrait cependant changer en ce qui concerne la pornographie impliquant des enfants: le 23 janvier 1996, la commission des affaires juridiques du Conseil national a transmis l'initiative parlementaire von Felten, qui préconise l'interdiction de la possession de matériel pédopornographie. Mais pour qu'une telle disposition pénale soit également applicable aux réseaux de communication, encore faudrait-il placer l'enregistrement électronique sur le même pied que la possession physique. Se poserait alors le problème de la délimitation entre possession et simple consommation. Si cette dernière - considérée en tant que perception intellectuelle consciente de scènes incriminées - devait, elle aussi, devenir un acte punissable, il conviendrait de se demander si l'étendue des mesures de surveillance que présuppose l'application efficace d'une telle norme pénale ne serait pas problématique sous l'angle de la proportionnalité, des ressources engagées et des droits fondamentaux.

La diffusion globale d'Internet a pour corollaire que les représentations incriminées sont en grande partie introduites dans le réseau depuis l'étranger. Dans ce cas, force est de se demander si les conditions d'application du droit pénal suisse quant au lieu disposent d'un élément de référence. En ce qui concerne les trois infractions envisagées, il y a controverse quant à savoir s'il s'agit de délits fondés sur le résultat ou de délits d'action, puisque, dans tous les

cas, un résultat au sens d'une prise de connaissance n'est pas nécessaire pour que l'élément objectif de l'infraction soit rempli.

Si l'on considère le résultat comme la simple possibilité de la prise de connaissance en Suisse, les conditions d'application du droit pénal suisse quant au lieu peuvent se fonder sur l'article 7 CP (principe dit de l'ubiquité). En revanche, si l'on considère ces infractions comme de purs délits d'action, il faut que l'acte ait été commis, du moins en partie, en Suisse pour que le droit pénal suisse soit applicable. On pourrait, à cet égard, estimer que l'entrée des données incriminées se limite à l'endroit où l'auteur introduit lesdites données dans le réseau. Si cet endroit se situe à l'étranger, le droit suisse ne serait pas applicable.

En l'occurrence, les actes qui déterminent les infractions concernées consistent toutefois à *rendre accessible* ou à *diffuser* publiquement. L'introduction des données dans le réseau équivaut à déclencher un processus causal qui ne se limite pas à l'endroit où se trouve l'auteur. Tous les points de connexion qui, par le biais d'un fournisseur, donnent aux utilisateurs la possibilité d'accéder aux données, constituent également des lieux de commission. Ainsi, l'infraction étant, en partie du moins, commise en Suisse, le droit suisse est également applicable en vertu de l'article 3, chiffre 1, 1er alinéa, CP.

En pratique cependant, la poursuite de l'auteur d'une telle infraction - lorsque l'auteur se trouve à l'étranger - ne sera évidemment pas chose facile. Pour aboutir, une procédure suisse devra recourir à l'entraide judiciaire (demande d'extradition, demande de transfert de la poursuite pénale). Hormis nombre d'autres obstacles, il se peut notamment que l'acte réprimé par le droit suisse ne constitue pas une infraction au sens du droit de l'Etat requis. Une telle situation est précisément envisageable en ce qui concerne les délits d'opinion qui nous intéressent ici. Or, à défaut de la double incrimination, les efforts visant à traduire en justice l'auteur étranger sont d'emblée voués à l'échec.

b) De la punissabilité du fournisseur d'accès

Les personnes qui participent à la commission des infractions dont il est question ici, sont non seulement celles qui introduisent les données incriminées dans Internet, mais aussi celles qui, en qualité de complices au sens de l'article 25 CP, prêtent assistance pour diffuser ces données ou les rendre accessibles. Objectivement considérée, la complicité présuppose une forme quelconque de

concours causal dans l'infraction, à défaut duquel l'infraction n'aurait pu être commise ou l'aurait été différemment. Sur le plan subjectif, la complicité implique que son auteur sache ou présume qu'il prête son concours à une forme d'infraction déterminée et qu'il le veuille ou en accepte le risque, l'intention incluant également la prévision du déroulement des événements. Cela dit, le complice ne doit pas nécessairement connaître tous les détails de l'infraction; il suffit qu'il en perçoive les caractéristiques essentielles. En revanche, l'intention totalement indéfinie et généralement présente d'accepter que son propre comportement aide un tiers à commettre des infractions peut ne pas suffire (cf. ATF 117 IV 188, avec renvois).

Dans son arrêt "du 156" (ATF 121 IV 109 ss), le Tribunal fédéral a constaté que le responsable des PTT de l'introduction du télékiosque se rendait coupable de complicité de pornographie au sens de l'article 197, chiffre 1, CP, dès lors qu'il fournissait les prestations nécessaires à l'exploitation du télékiosque tout en sachant qu'il servait à diffuser des enregistrements pornographiques accessibles à des jeunes de moins de 16 ans. A cet égard, le fait que le ministère public ait précédemment attiré l'attention du responsable sur l'utilisation illicite du télékiosque et sur le risque de condamnation pénale qu'il courait en persistant à fournir ces prestations, a joué un rôle capital.

Cette jurisprudence peut être transposée - mutatis mutandis - sur les fournisseurs d'accès à Internet (access providers) et sur les exploitants d'autres réseaux connectés en ligne[6]: La mise à disposition de l'infrastructure implique un comportement actif du fournisseur, dans la même mesure que l'installation du télékiosque par les PTT (cf. ATF 121 IV 120). Le fait que, contrairement aux PTT dans l'exploitation du télékiosque, le fournisseur d'accès ne détienne aucun monopole, est sans importance pour l'élément constitutif de la complicité que représente la contribution causale apportée à l'acte incriminé: le fournisseur poursuivi ne saurait se disculper en objectant que la représentation incriminée était également accessible par l'entremise d'autres fournisseurs.

Pour déterminer la punissabilité pour complicité dans le présent contexte, il y a lieu de répondre à la question essentielle de savoir si le dol éventuel peut être retenu contre le fournisseur d'accès; le dol éventuel consistant en l'occurrence à

[6] Lorsque ci-dessous il sera question de la punissabilité du fournisseur d'accès, il conviendra de tenir compte du fait que des personnes morales ne sont pas punissables en tant que telles. A l'intérieur d'une entreprise, la responsabilité pénale ne peut être imputée qu'aux personnes physiques qui participent aux actes punissables.

favoriser l'accès à des données dont le contenu remplit les éléments constitutifs de formes d'infractions déterminées, ou à favoriser leur diffusion publique. Comme relevé précédemment, une intention générale ne suffit toutefois pas à cet effet. Pour le fournisseur, cela signifie concrètement qu'aucune responsabilité pénale ne découle de sa connaissance générale du fait que, parmi les innombrables informations circulant sur Internet figurent également des données pénalement répréhensibles, auxquelles sa prestation contribue à donner accès.

Le fournisseur n'a pas non plus l'obligation légale de vérifier systématiquement le contenu intégral du réseau pour constater si celui-ci contient des informations pénalement répréhensibles: dans le secteur des communications personnelles individuelles entre usagers (p.ex. via E-Mail), une telle opération se heurte d'emblée au secret des télécommunications. Le fournisseur est en revanche parfaitement habilité à contrôler le contenu de données accessibles au public. Mais, dans ce cas également, un contrôle systématique est totalement irréaliste si l'on songe que le seul trafic d'informations au sein des quelque 17'000 groupes de discussion d'Internet représente un volume de textes estimé entre un et deux gygabyte, soit l'équivalent de plusieurs milliers de livres.

De l'autre côté, des indications spécifiques sur le contenu concret de réseaux, que le fournisseur obtient par ses propres moyens ou que lui fournissent des tiers, sont susceptibles d'établir un niveau de connaissance suffisant pour fonder la complicité intentionnelle. Dans ce cas, le fournisseur risque d'engager sa responsabilité pénale s'il ne prend pas immédiatement les mesures utiles sur le plan technique - par exemple le blocage des groupes d'informations concernés - pour empêcher la rediffusion des données incriminées à ses clients. Le fournisseur, qui obtient ces indications spécifiques de tiers, n'est pas seulement tenu de prendre ces mesures lorsqu'un jugement pénal exécutoire a été rendu (cf. aussi ATF 121 IV 123).

En vertu de l'arrêt „du 156" rendu par le Tribunal fédéral, la référence au contenu concret de réseaux que formule clairement une autorité de poursuite pénale est en tout cas de nature à fonder l'intention du fournisseur donc à inciter ce dernier à prendre les mesures qui s'imposent. Lorsque les indications émanent de particuliers, les circonstances du cas d'espèce sont déterminantes. En tout état de cause, un reproche vague formulé de façon générale par un client ne saurait suffire à conclure à un dol éventuel de la part du fournisseur. En revanche si le client formule des indications concrètes et détaillées, le fournisseur est pour le

moins tenu d'entreprendre lui-même des investigations, le cas échéant avec le concours de l'autorité de poursuite pénale ou de tiers techniquement qualifiés, s'il entend écarter tout risque de punissabilité.

3. Digression: Infractions liées aux explosifs, blanchissage d'argent, modifications imminentes du droit pénal et de la procédure pénale des médias

a) Infractions liées aux explosifs

Il a été constaté à diverses reprises que certains groupes d'informations diffusés par Internet contenaient des instructions détaillées pour fabriquer des explosifs ou des bombes à l'attention des amateurs de ce genre d'objets. A cet égard, on peut se demander si la diffusion de telles „recettes" relève du droit pénal.

Dans ce contexte, l'article 226, 3e alinéa, du code pénal, qui réprime la communication des indications nécessaires à la fabrication d'explosifs (ou de gaz toxiques), revêt une importance primordiale. Cette disposition implique toutefois que l'auteur sache ou doive présumer que le destinataire des informations se propose de faire un emploi délictueux des explosifs (ou des gaz toxiques). Si l'auteur se borne à transcrire les instructions sur une page d'information d'Internet accessible à un nombre indéterminé d'utilisateurs, il ne remplit pas nécessairement les éléments constitutifs du dol (éventuel). Il en va naturellement autrement si l'auteur adresse sciemment et de façon ciblée les instructions à des personnes qui se proposent d'en faire un usage délictueux.

Celui qui diffuse en même temps que le "mode d'emploi" un appel visant à déterminer concrètement le destinataire à commettre une infraction ou l'incitant au crime ou à la violence, se rend coupable d'une (tentative) d'incitation à une infraction (liée aux explosifs) ou de provocation publique au crime ou à la violence (art. 259 CP).

b) Blanchissage d'argent

Le développement fulgurant d'Internet conduit également à s'interroger sur l'applicabilité à ce secteur des normes pénales concernant le blanchissage d'argent. Les transactions financières peuvent s'opérer non seulement par le biais de réseaux fermés, mais aussi sur Internet. Elles n'ont toutefois pas pris une

notable ampleur jusqu'à présent sur des réseaux ouverts, car il n'existe pas encore de système assez sûr pour protéger par exemple les numéros de cartes de crédit contre un accès indu. Mais cette situation pourrait se modifier dans un avenir proche.

Il serait également possible de commettre via Internet des actes de dissimulation réprimés par l'article 305bis CP (*blanchissage d'argent*); le transfert de valeurs patrimoniales d'origine délictueuse d'un compte auprès de la banque X à un autre compte auprès de la banque Y n'en est qu'un exemple. L'applicabilité de l'article 305bis CP aux transactions opérées par le biais d'Internet n'est pas remise en question. Cependant, les réseaux universels précisément offrent la possibilité d'effectuer rapidement et dans le monde entier d'innombrables transactions, dont la reconstitution devrait poser d'énormes problèmes aux autorités de poursuite pénale.

Dans une telle situation, le devoir de vigilance impliquant *l'identification de l'ayant droit économique*, que l'article 305ter, 1er alinéa CP, impose aux personnes professionnellement actives dans le secteur financier, revêt une importance primordiale. Aujourd'hui déjà, des intermédiaires financiers proposent sur Internet l'ouverture de comptes, notamment. Il va de soi qu'un financier au sens de l'article 305ter, 1er alinéa CP est également soumis au devoir d'identification lorsqu'il accepte, garde en dépôt ou aide à placer ou à transférer des valeurs patrimoniales par le biais d'un réseau. Conformément à cette disposition pénale, il est tenu de vérifier l'identité de l'ayant droit économique avec la vigilance que requièrent les circonstances. Dès lors qu'une vérification fiable de l'identité du cocontractant ne saurait être garantie dans le cadre des communications sur Internet, le financier qui ne remplirait le devoir d'identification que lui impose l'article 305ter, 1er alinéa, CP, que par un échange de correspondance sur Internet, violerait son devoir de vigilance. Il est en effet tenu de vérifier l'identité du cocontractant et de l'ayant droit économique par des moyens adéquats en dehors du réseau. A cet égard, la Convention relative à l'obligation de diligence des banques (CDB 92), notamment les chiffres 9 s. et 19 concernant les relations d'affaires nouées par correspondance, peut tenir lieu de directive.

L'acuité des problèmes que pose le blanchissage d'argent pourrait sensiblement augmenter si le développement de nouvelles techniques de paiement (*cyberpayments*) devait s'imposer sur une large échelle. Le Groupe d'Action Financière (GAFI), organisation qui dirige la lutte internationale contre le

blanchissage d'argent, a récemment examiné ces questions de plus près. Bien qu'aucune affaire de blanchissage d'argent n'ait encore été découverte à ce jour sur Internet, le GAFI considère que le risque potentiel est très élevé.

Les techniques de paiement dont il est question en l'occurrence sont, d'une part, les „smart cards" ou cartes de crédit rechargeables, munies d'une puce et, d'autre part, l'exécution de paiements sur réseaux, la monnaie pouvant être enregistrée et transférée sous forme électronique. Certes, le recours aux „cyberpayments" demeure encore timide pour l'instant. En Angleterre, par exemple, le champ d'utilisation des „smart cards", d'usage courant, est restreint; elles sont en outre munies d'une limite de 500 livres. La circulation sur réseaux de la monnaie virtuelle se heurte, pour l'instant encore, au problème du développement d'un système à l'épreuve des piratages. Il est néanmoins possible qu'à l'avenir un nouveau trafic de paiements électronique entre particuliers puisse se développer, qui en cas d'expansion pourrait massivement réduire le recours aux intermédiaires financiers traditionnels. Une telle évolution serait parfaitement susceptible de réduire à néant les éléments essentiels de chaque dispositif de prévention du blanchissage d'argent (p.ex. devoirs d'identification, de documentation et de communication). Aujourd'hui, même un pays comme les USA n'a encore aucune idée des mesures qu'il conviendrait de prendre pour remédier à ce genre d'évolution.

c) Effets de la future révision du droit pénal et de la procédure pénale des médias

Le droit en vigueur, à l'article 27 CP, prévoit déjà des dispositions restreignant la responsabilité en cas de délit d'opinion. Ainsi, la disposition mentionnée prévoit notamment que lors d'un délit de presse le rédacteur en est le seul responsable. Ces prescriptions spécifiques au droit de la presse ne s'appliquent cependant pas aux transmissions électroniques de textes et ne sont donc pas à prendre en considération dans le contexte qui nous préoccupe.

La situation pourrait être modifiée par la future révision du droit des médias : Il est prévu notamment d'étendre le champ d'application de l'article 27 CP à tous les médias, y compris les contenus publiquement accessibles sur Internet. Le principe de la responsabilité exclusive de l'auteur vaudrait également sous l'empire du nouveau droit. Ce qui aurait pour conséquences que serait exclue la punissabilité de toutes les autres personnes qui participent nécessairement à la publication, tel que le fournisseur d'accès à Internet. Ceci à condition que l'auteur publie le

contenu sciemment et volontairement et qu'il puisse être découvert et traduit en justice en Suisse. Comme il a été déjà précisé, (cf. II. 2a in fine), cette condition devrait souvent faire défaut en ce qui concerne les auteurs étrangers publiant sur Internet[7].

A l'intérieur d'une entreprise de médias, le rédacteur responsable, ou à défaut de celui-ci - ce qui semble être le cas souvent pour ce qui est des contenus publiés sur Internet - la personne dont la publication relève de son domaine de responsabilité serait punissable à titre subsidiaire. Ces personnes ne répondraient de l'infraction que si elles ne se sont pas, intentionnellement ou par négligence, opposées à la publication. En pareil cas elles on tomberaient sous le coup d'une autre disposition à savoir la contravention prévue à l'article 322bis du projet CP.

L'entreprise se contentant de transmettre des informations (p. ex. un fournisseur de service Internet) peut aussi en principe être tenue pour responsable au sens de l'article 27 du projet CP si la responsabilité ne peut être imputée à d'autres personnes. Au vu de la distance qui la sépare de l'auteur de l'information et, en particulier, de l'énorme quantité de données à transmettre, son devoir de diligence ne peut néanmoins être assujetti à des exigences élevées. Elles ne devraient donc tomber sous le coup de la norme pénale de l'article 322bis du projet CP que très exceptionnellement.

4. Mesures de prévention envisageables

Comme relevé précédemment, la mondialisation d'Internet place la justice pénale des divers Etats devant de grandes difficultés, lorsqu'il s'agit de poursuivre et de punir les auteurs d'infractions. En ce qui concerne les délits d'opinion notamment, qui revêtent une grande portée pratique, il est certes également possible de poursuivre le founisseur pour complicité lorsque l'auteur principal de l'infraction se trouve à l'étranger. Cela ne doit toutefois pas déboucher sur une extension excessive de la responsabilité pénale du fournisseur. En l'occurrence, cette responsabilité doit au contraire se fonder sur les critères applicables de façon générale.

Dans une telle situation, la prévention revêt une importance capitale. Le principe selon lequel des problèmes globaux requièrent des solutions globales impliquerait certes une démarche concertée sur le plan international pour empêcher la

[7] Actuellement l'application de l'article 27 CP à des publications de presse étrangères est d'ailleurs controversée.

commission d'infractions sur les réseaux mondiaux. Force est toutefois de constater qu'on est encore loin d'une solution globale efficace, sous forme d'instruments internationaux contraignants, par exemple. Dans ces conditions, les Etats se doivent de rechercher des solutions sur un plan interne d'abord, les fournisseurs d'accès à des réseaux étant à cet égard au centre des préoccupations. Deux ébauches de solution s'offrent en principe dans ce contexte: un *dispositif étatique de surveillance et de contrôle* ainsi qu'un *système d'autodiscipline développé au sein de la branche concernée*. Dans le premier cas, la solution envisagée consisterait à imposer aux fournisseurs d'accès l'obligation d'obtenir une autorisation et à les assujettir, dans le cadre du droit de surveillance, à un contrôle ainsi qu'à un devoir de vigilance et de communication. En d'autres termes, pour combattre la criminalité sur les réseaux d'information, l'Etat soumettrait les fournisseurs d'accès à un régime analogue à celui qui s'applique aujourd'hui déjà aux instituts financiers dans le domaine du blanchissage d'argent[8].

Le groupe de travail considère toutefois qu'un dispositif étatique de surveillance ne trouve sa raison d'être qu'à partir du moment où le danger d'une multiplication d'abus pénalement répréhensibles est établi et lorsque la branche n'a ni la volonté ni les moyens de lutter adéquatement contre de tels abus. Ces prémices ne sont pour l'instant pas remplies. En s'efforçant notamment de se doter d'un code de conduite, la branche en question, qui est encore en plein essor, entend contribuer à empêcher la commission d'infractions sur les réseaux. De tels efforts sont susceptibles d'aboutir bien plus rapidement que l'élaboration d'un dispositif étatique de contrôle. Dans ces conditions, le groupe de travail estime judicieux de soutenir le développement d'un système d'autodiscipline en formulant des recommandations.

5. Moyens techniques de prévention

Pour formuler des recommandations, il convient d'abord d'examiner les possibilités techniques dont dispose aujourd'hui le fournisseur pour détecter et bloquer plus facilement dans son secteur les contenus pénalement répréhensibles diffusés sur un réseau. On mentionnera d'une part les paquets de logiciels spéciaux, tels Surfwatch, Internetfilter, Cybersitter, Cyber Patrol, Netnanny, Webtrack et bien d'autres encore, installables sur un PC ou sur un serveur et qui, en partie, peuvent être aussi mis en oeuvre à l'échelon du fournisseur. Ces

[8] A ce sujet, cf. en particulier l'article 305ter, 1er al., CP ainsi que l'avant-projet de loi fédérale relative à la lutte contre le blanchissage d'argent dans le secteur financier, de janvier 1994.

logiciels contiennent, sous forme de tableaux, les adresses des fournisseurs de données, qui mettent à disposition des supports de textes, d'images, de films et de sons dont le contenu n'est pas destiné à des jeunes. Ils offrent en outre la possibilité de bloquer totalement l'accès à des formats de fichiers déterminés. Seul un mot de passe permet de traverser les filtres ainsi installés. D'autre part, il existe des produits, dont la fonction de filtre s'exerce non pas selon des adresses mais selon des mots ou des supports d'images susceptibles de contenir des représentations pornographiques.

Les produits de la deuxième catégorie ne semble guère avoir fait leurs preuves jusqu'à présent. Des programmes conçus, par exemple, pour rechercher de grandes surfaces de peau dans une image ou dans un film peuvent également déboucher sur le blocage des contenus anodins d'un réseau, telles des images utilisées en médecine. Un fournisseur américain a vécu une telle mésaventure lorsqu'il a éliminé tous les textes dans lesquels figurait le mot "breast" (sein). Le blocage a été levé suite aux protestations formulées par des patientes atteintes d'un cancer du sein qui avaient échangé des expériences et des informations par le biais du service connecté en ligne. Les chances de développer un logiciel intelligent et capable de faire réellement la différence entre les séquences de textes, d'images, de films et de sons pénalement répréhensibles et celles qui ne le sont pas semblent pour le moins minimes. De plus, ces produits se limitent jusqu'à présent, et pour autant qu'on puisse en juger, au seul secteur des infractions liées à la pornographie.

En revanche, l'emploi à titre complémentaire des programmes de logiciels, mentionnés en tête du présent chapitre, qui contiennent également des listes noires de fournisseurs de données, semble plus prometteur. Moyennant un investissement proportionnel, il est ainsi parfaitement possible de recenser une part importante des contenus de réseaux illicites. L'utilité de tels programmes implique toutefois une quantité de données aussi vaste et précise que possible, et présuppose en outre une mise à jour constante. Indépendamment de ces conditions, l'emploi de ces programmes peut présenter l'inconvénient d'un éventuel blocage intégral de groupes d'informations, dont seuls certains éléments devraient être concernés. De plus les longues opérations de filtrage sont susceptibles de ralentir l'ensemble des procédures d'accès. Enfin, ces programmes sont pour une grande part adaptés au marché américain et par conséquent à la situation juridique qui y prévaut.

6. Recommandations

a. Recommandation 1: Blocage de l'accès à des contenus illicites

Le groupe de travail est conscient de la multiplicité des moyens dont disposent les usagers et les fournisseurs de données pour éluder le blocage des contenus de réseaux imposé par un fournisseur d'accès. L'usager pourrait par exemple accéder aux données concernées en passant par un fournisseur étranger qui n'aurait pas instauré de blocage. Par ailleurs, on pourrait imaginer qu'un fournisseur de données, au courant du blocage instauré, offre ses contenus sous une nouvelle rubrique (groupe d'informations) et qu'il en informe directement les intéressés potentiels par le biais du courrier électronique (mail).

Cette situation ne saurait toutefois inciter le fournisseur d'accès à estimer que le blocage de contenus de réseaux criminels est inutile et, partant, superflu. Ce d'autant moins que le fournisseur d'accès est tenu d'agir dès qu'il dispose d'informations suffisantes s'il veut exclure sa propre responsabilité pénale. En outre, bien qu'il ne soit pas totalement efficace, le blocage rend l'accès nettement plus difficile et contribue ainsi à limiter la diffusion et l'accessibilité de contenus de réseaux pénalement répréhensibles.

Recommandation 1

> **Lorsque le fournisseur d'accès dispose d'indices concrets fondés sur ses propres recherches ou sur celles de tiers permettant de présumer l'éventuel caractère illicite de contenus de réseaux déterminés, il procédera ou fera procéder immédiatement à des investigations afin de déterminer si un blocage s'impose. Lorsque le fournisseur d'accès apprend, de façon certaine, l'existence de contenus de réseaux illicites, notamment réprimés par le droit pénal, il prendra immédiatement les mesures raisonnablement exigibles et techniquement réalisables afin de bloquer l'accès à ces contenus de réseaux.**

La première phrase de la présente recommandation se réfère en particulier aux indices fournis par des tiers privés. Dans de tels cas, le fournisseur d'accès se forgera le plus souvent sa propre opinion sur le contenu litigieux avant

l'instauration d'un éventuel blocage[9]. Selon le type d'infraction en cause, il sera sans autre en mesure de déterminer lui-même si un blocage s'impose. Tel sera notamment le cas en présence de pornographie dite „dure", dont la définition formulée à l'article 197, chiffre 3 CP, en particulier celle de la pornographie impliquant des enfants, est aisément accessible au profane. D'autres formes d'infractions peuvent en revanche nécessiter l'avis d'un spécialiste; ce service pourrait être repris dans le cadre d'un système d'autodiscipline.

b. Recommandation 2: Service central

Pour prévenir efficacement la diffusion de contenus criminels sur Internet, il convient en premier lieu de développer le flux des informations à destination des fournisseurs d'accès et entre eux. Un système d'autodiscipline efficient doit garantir aux fournisseurs la mise à disposition d'informations aussi complètes, actuelles et précises que possible sur les contenus de réseaux illicites.

Recommandation 2

Il est recommandé à la branche d'instituer un service central chargé de recevoir et d'exploiter les indications communiquées par les fournisseurs d'accès, les clients de ceux-ci et les tiers au sujet de contenus de réseaux illicites. Ce service, conçu en tant que plaque tournante de services et d'informations, devrait transmettre aux fournisseurs d'accès raccordés à ce service des renseignements actualisés sur les contenus de réseaux qu'il convient de bloquer et offrir aux membres de la branche un appui sur les plans scientifique et technique.

Cet appui peut notamment consister à conseiller les fournisseurs d'accès lors de l'appréciation de contenus de réseaux déterminés sous l'angle du droit pénal. Le service central serait en outre qualifié pour émettre, le cas échéant, des recommandations relatives à l'emploi de programmes de logiciels auxiliaires (cf. à cet égard II.5, ci-dessus) et tenir lieu d'interlocuteur central pour les autorités de poursuite pénale.

c. Recommandation 3: Accès au réseau

[9] A condition que les données lui soient accessibles; s'il s'agit de communications personnelles individuelles entre usagers, le secret des télécommunications s'oppose à ce que le fournisseur procède à un contrôle du contenu de ces communications, cf. ci-dessus II. 2.b).

Parmi les infractions examinées en relation avec Internet, la pornographie dite „douce“, au sens de l’article 197, chiffre 1, CP, constitue un cas particulier, dans la mesure où elle est frappée d’une interdiction relative et non absolue. En matière de pornographie „douce“, n’est en effet punissable notamment que celui qui la rend accessible à des personnes de moins de 16 ans. Pour le fournisseur d’accès, le blocage intégral de tels contenus de réseaux constitue une mesure certes suffisante, mais non absolument nécessaire. Il peut également éviter le risque de punissabilité en garantissant de manière suffisante, par l’adoption de mesures techniques dans sa sphère d’influence, que la pornographie „douce“ demeure inaccessible à des jeunes. Dans ces conditions, le fait de rendre accessible à des jeunes de moins de 16 ans des représentations de pornographie douce demeure de la seule responsabilité de l'usager.

Recommandation 3

Il est recommandé au fournisseur d’accès de ne conclure en principe des contrats d’abonnement qu’avec des personnes physiques majeures et capables de discernement. De plus, l’abonné ne doit pouvoir accéder au réseau que moyennant une procédure d’identification et un mot de passe (pin-code).

d. Recommandation 4: Réserve dans le contrat d'abonnement

Il va de soi que les clients ou les partenaires contractuels du fournisseur d’accès sont également susceptibles d’utiliser des réseaux de manière abusive. Le fournisseur d’accès a, là encore, la possibilité d’adopter des mesures complémentaires:

Recommandation 4

Dans le contrat d’abonnement, le fournisseur d’accès se réservera le droit de bloquer le raccordement provisoirement en cas de soupçons et de résilier unilatéralement le contrat si le client diffuse des contenus illicites ou en permet la consultation depuis son raccordement.

e. Recommandation 5: Invitation à annoncer toute utilisation illicite du réseau

La recommandation 2 souligne déjà l'importance d'un afflux d'indications aussi large que possible vers les fournisseurs d'accès au sujet des contenus de réseaux illicites a déjà été soulignée dans le cadre de la recommandation 2. Il est évident que les usagers, notamment, sont fréquemment en mesure de livrer des renseignements utiles à cet égard.

Recommandation 5

> **Le client sera expressément invité, dans le contrat d'abonnement, à annoncer immédiatement au fournisseur d'accès et/ou au service central (cf. recommandation 2) les contenus de réseaux illicites ou toute autre utilisation illicite d'Internet dont il a connaissance.**

f. Recommandation 6: Formes de représentations de la violence et de pornographie dure

Il convient de revenir ici sur le problème évoqué dans l'introduction, à savoir les jeux électroniques comprenant des scènes de violence (question ordinaire Bischof). Dans la mesure où de tels jeux contiennent des scènes qui représentent avec insistance des actes de cruauté envers des êtres humains ou des animaux et qui, de ce fait, portent gravement atteinte aux principes élémentaires de la dignité humaine, ils remplissent les éléments constitutifs de l'infraction définie à l'article 135 CP (Représentation de la violence). Outre des jeux anodins, les réseaux peuvent permettre l'exploitation de jeux qui violent l'interdiction de représenter de la violence, que ce soit sous forme d'offre au moyen d'un catalogue (l'infraction consistant à offrir et à promouvoir), ou de possibilité de charger des programmes incriminés ou de participer à des jeux enregistrés d'une autre manière (l'infraction consistant à mettre en circulation, à montrer, à rendre accessible ou à mettre à disposition). Les considérations et les recommandations qui précèdent sont donc également applicables aux jeux et aux offres remplissant les éléments constitutifs de l'infraction susmentionnée.

Recommandation 6

Le fournisseur d'accès doit être conscient du fait que la représentation de la violence, sanctionnée par l'article 135 CP, ne se résume pas seulement à des séquences de films ou à des photographies, mais qu'elle peut aussi prendre la forme d'autres objets ou représentations, tels que des jeux électroniques, et que la promotion et l'offre de représentations de la violence sont également des actes punissables. Il en va de même en ce qui concerne les représentations de pornographie dure au sens de l'article 197, chiffre 3 CP.

III. Aspects du droit de la protection des données

Le groupe de travail a invité le Préposé fédéral à la protection des données (PFPD) à présenter, par écrit, les questions que soulève Internet sur le plan du droit de la protection des données. La position du PFPD, dont il sera question ici, fait l'objet de l'annexe 1 au présent rapport. Elle rappelle les principes généraux du droit de la protection des données (p. 1 ss) et, sur cette base, expose les risques que présente Internet en général pour la protection des données (p. 5 s.), les risques que présentent les services spécifiques d'Internet pour la protection des données (p. 6 ss) et les problèmes qui concernent les fournisseurs d'accès en particulier (p. 8 s.). Sur ce dernier point, le groupe de travail formule des recommandations qui reflètent, d'une part, la position du fournisseur d'accès en tant que participant au flux général des données sur des réseaux et, d'autre part, ses propres possibilités de traitement spécifique des données dans le cadre de son activité.

1. Recommandation 7: Information sur les risques en matière de protection des données

Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées (art. 7, 1er al., LPD). Outre les personnes qui expédient des données personnelles ou en permettent la consultation sur un réseau, l'obligation de garantir une protection appropriée des données incombe à celui qui met à disposition le réseau de communication des données et, partant, au fournisseur d'accès également. Il convient néanmoins de ne pas assujettir à des exigences excessives son devoir de garantir la confidentialité, la disponibilité et la conformité des données (cf. p. 9

s. de l'avis du PFPD). L'information des clients sur les mesures techniques destinées à assurer leur protection et sur les risques que présente l'utilisation du réseau du point de vue du droit de la protection des données occupe le premier plan.

Recommandation 7

Le fournisseur d'accès informera ses clients de manière suffisante sur les risques que peuvent présenter l'utilisation du réseau de même que le recours à des services sous l'angle du droit de la protection des données, et lui fournira des indications concernant les mesures et les produits destinés à garantir la confidentialité, la conformité et la disponibilité des données personnelles (p.ex. des techniques de chiffrage et de cryptage).

2. Recommandation 8 (Traitement de données personnelles) et Recommandation 9 (Profils de la personnalité et publication de données personnelles)

Dans le déroulement de ses affaires (notamment pour établir la facturation), le fournisseur d'accès doit forcément traiter des données personnelles relatives à ses clients, p.ex. nom, adresse, numéro de téléphone, voire fréquence et modalités d'utilisation. Or, de telles données pourraient être utilisées à des fins étrangères au but dans lequel elles avaient été recueillies, c'est-à-dire communiquées à des tiers ou exploitées dans l'élaboration de profils de la personnalité (cf. à cet égard l'avis du PFPD).

Recommandation 8

Le fournisseur d'accès ne traitera que les données personnelles relatives à ses clients dont il a besoin pour fournir sa prestation. Des mesures organisationnelles et techniques garantiront l'accès des données traitées exclusivement au personnel qui en a besoin dans l'accomplissement de ses tâches. Les données ne seront pas utilisées dans un but autre que celui qui aura été indiqué lors de leur collecte, qui ressort des circonstances ou qui est prévu dans la loi. Elles ne seront rendues accessibles à des tiers

qu'avec l'accord du client ou que sur la base d'une obligation de communication qualifiée.

Recommandation 9

Le fournisseur d'accès n'établira aucun profil de la personnalité au sujet de ses clients, ni ne rendra leur nom, leur adresse ou leur numéro de téléphone accessible sur un réseau, à moins que la personne concernée n'y ait consenti, ou qu'il n'existe une justification légale ou un intérêt public ou privé prépondérant.

IV. Aspects du droit d'auteur

Les autoroutes de l'information telles qu'Internet suscitent également des questions relevant du domaine des droits d'auteur. Dans le document annexé à ce rapport (annexe 2) l'Institut de la propriété intellectuelle donne un aperçu de ces questions et en particulier de ce qu'il faut comprendre par oeuvre protégée par le droit d'auteur (ch. 3 de l'annexe). Cet exposé informe également sur les droits voisins protégés par la Loi sur le droit d'auteur (LDA). Sont protégés les artistes exerçant leur art qui proposent leur oeuvre ainsi que les producteurs de supports de sons ou d'images et les producteurs d'émissions pour leurs services (ch. 4 de l'annexe). Compte tenu du fait que la protection du droit d'auteur et des services est limitée quant au fond et au temps (ch. 7 de l'annexe), il est néanmoins évident que des contenus protégés (tels que des films, de la musique, des photos, des textes etc.) sont, par le biais d'Internet, rendus perceptibles, reproduits, propagés, modifiés ou utilisés d'une autre manière.

Il convient donc - également sur les autoroutes de l'information - de respecter les droits qui appartiennent aux auteurs ou à leurs successeurs en droit resp. aux ayants droits découlant des droits voisins (ch. 9 de l'annexe). C'est ainsi que l'auteur a le droit exclusif de décider si et le cas échéant quand et comment son oeuvre peut être utilisée. Parmi ces droits il faut mentionner en particulier le droit de publication (c'est-à-dire le droit de rendre une première fois son oeuvre accessible à un grand nombre de personnes), le droit de la rendre perceptible (p.ex. en l'introduisant dans un réseau de données), le droit de la reproduire (p.ex. l'enregistrement de son oeuvre sur le disque dur d'un ordinateur) ainsi que le droit

de la propager et de la modifier. L'auteur peut donc interdire que son oeuvre soit publiée, vue et entendue, reproduite ou même modifiée.

Etant donné que sur Internet, en relation avec l'utilisation d'oeuvres protégées par le droit d'auteur ainsi que de services protégés par les droits voisins, il est possible d'agir de plusieurs façons et de manière illicite, le danger de violer ces droits augmente. Tous les participants (fournisseurs d'informations, fournisseurs d'accès, demandeurs d'informations) doivent être conscients que les droits d'auteur et les droits voisins doivent être respectés aussi sur les autoroutes de l'information.

En effet, celui qui, sans l'autorisation de l'ayant droit et sans pouvoir s'appuyer sur une exception de protection (ch. 10 de l'annexe) utilise des droits d'auteur ou des droits voisins, peut être poursuivi civilement ou pénalement (art. 61 ss LDA). Le *droit civil*, met à la disposition de l'auteur ou de l'ayant droit un arsenal considérable de mesures de protection (actions en constatation et en exécution d'une prestation, mesures provisionnelles et publication du jugement). Outre l'interdiction d'utilisation, il est aussi possible, une fois que l'utilisation a déjà eu lieu, d'agir en réparation du dommage. Sur plainte adéquate, les violations de droits commises intentionnellement peuvent également être poursuivies *pénalement*. Les dispositions pénales prévoient des peines d'emprisonnement pour un an au plus ou l'amende pouvant s'élever à 40'000 francs. Celui qui agit par métier à l'encontre des dispositions de la loi sur les droits d'auteur est poursuivi d'office. Il est passible d'une peine d'emprisonnement de 3 ans au plus et d'une amende de 10'000 francs au maximum.

Le *fournisseur d'informations* (p.ex. une banque de données), qui propose sur un réseau des oeuvres protégées par le droit d'auteur ou par des droits voisins, doit en premier lieu disposer de ces droits, étant donné que le "uploading" (c'est-à-dire l'enregistrement de l'information indispensable à sa consultation) ainsi que l'offre de ces informations nécessitent toujours des actes relevant du droit d'auteur ou des droits voisins (p.ex. reproduire, faire voir ou entendre).

Dans ce contexte se pose la question de savoir dans quelle mesure le *fournisseur d'accès* peut être tenu pour responsable d'utilisations illicites. Il est du devoir du fournisseur d'accès de mettre à disposition des usagers, qui n'ont pas de propre raccordement direct aux autoroutes de l'information, les moyens de s'y raccorder. Le fournisseur d'accès n'est ainsi en principe pas un utilisateur d'oeuvres

protégées par le droit d'auteur, mais il sert plutôt d'intermédiaire pour les contenus qui se trouvent sur Internet, qu'ils soient protégés ou non.

Lorsque l'intermédiaire ne procure aux demandeurs d'informations que l'accès à l'autoroute de l'information, il convient de répondre en premier lieu à la question de savoir s'il procède à une utilisation indépendante de l'oeuvre au sens de l'article 10 LDA et s'il commet donc simultanément une violation du droit. Tel pourrait être le cas par exemple lorsque le fournisseur d'accès fait un enregistrement intermédiaire sur le soi-disant "Proxy-Server". Il s'agit en l'occurrence d'une reproduction généralement automatique et de courte durée. Etant donné que cette reproduction est techniquement indispensable et qu'elle s'efface automatiquement dans un bref délai, il y a controverse sur le point de savoir s'il s'agit effectivement d'une reproduction relevant du droit d'auteur au sens de l'article 10, 2e alinéa, lettre a LDA.

Il convient cependant de signaler que la loi sur le droit d'auteur ne prévoit pas d'exception de ce type et qu'une violation du droit d'auteur ne peut pas être exclue. Il est par ailleurs évident que sans l'intervention de l'intermédiaire, les signes transportés sur Internet seraient inutilisables pour l'usager; quant à l'oeuvre qui en découle, c'est l'intermédiaire qui la fait "voir ou entendre en un lieu autre que celui où elle est présentée" (art. 10, 2e al., let. c LDA). La question de savoir si la diffusion de l'oeuvre ou sa rediffusion (art, 10, 2e al., let. d et e LDA) dans le cadre d'Internet sont des actes relevant du droit d'auteur, n'est pas encore résolue. Il ne peut donc pas être exclu que les infractions en question soient - ne serait-ce qu'indirectement - imputées au fournisseur d'accès. Ce raisonnement est à la base d'un arrêt du Tribunal fédéral (ATF 107 II 82 ss) qui concerne toutefois l'ancienne loi sur les droits d'auteur. Dans ce cas le Tribunal fédéral a laissée ouverte la question de savoir si les PTT ont violé les droits d'auteurs en exploitant leur réseau d'ondes dirigées; en même temps il a constaté que celui qui n'est que complice de la violation du droit est solidairement responsable de l'infraction en vertu de l'article 50, 1er alinéa CO. Le Tribunal fédéral a estimé que les PTT remplissaient cette condition et a reconnu une responsabilité solidaire.

1. Recommandation 10: Blocage de l'accès en de violation des droits d'auteur

En principe le fournisseur d'accès ne doit pas être traité autrement que celui qui, dans son magasin de CD, vend des disques Compact non licenciés. Ceci vaut en particulier pour la question de la participation à l'infraction. Vu que la LDA ne prévoit pas de règles particulières dans ce domaine, ce sont les dispositions du Code pénal sur la complicité qui seront applicables; les explications relatives à la punissabilité du fournisseur d'accès sont valables (cf. ci-dessus II. 2. b). On peut ajouter que selon l'ATF 121 IV 109 ss la punissabilité dépend de la possibilité et des moyens de contrôle présumés. Ce contrôle est particulièrement difficile à pratiquer sur Internet compte tenu de l'immense flot d'informations, de l'aspect international ainsi que de l'organisation non hiérarchique du réseau.

D'autre part, le fournisseur d'accès, même s'il pouvait procéder lui-même au contrôle nécessaire, ne serait, dans la plupart des cas, pas en mesure de constater des violations du droit d'auteur ou de droits voisins, étant donné qu'il ne peut guère savoir avec certitude si le fournisseur d'informations a les licences requises ou si les ayants droit ont autorisé la diffusion (p.ex. il faut bien admettre que les oeuvres ou les services qui ont été introduits sur Internet puissent être consultés sur ce réseau). Afin de pouvoir poursuivre le fournisseur d'accès pour complicité, il faut qu'il existe certains indices évidents (p.ex. un jugement entré en force, des informations des autorités chargées de la poursuite pénale etc.) qui laissent à supposer une violation du droit en question. Lorsqu'on sera en présence de tels indices concrets, il sera aussi permis d'exiger du fournisseur d'accès qu'il prenne les mesures nécessaires en vue d'éviter d'autres violations du droit.

Si le fournisseur d'accès voulait s'exclure de toute responsabilité pénale ou civile, il devrait lui-même se voir concéder une licence l'autorisant à voir ou entendre des oeuvres assujetties au droit d'auteur ou aux droits voisins. Ceci semble être plutôt théorique et guère praticable, étant donné qu'il est très difficile de savoir quelles sont les informations protégées transmises ou enregistrées par le fournisseur d'accès. De ce point de vue, il serait indispensable de prévoir une signalisation électronique et individualisée des informations qui sont à disposition et qui peuvent être consultées sur une autoroute de l'information. Un tel système n'étant pas encore prêt, le fournisseur d'accès doit être conscient du fait que par sa position d'intermédiaire, il encourt un certain risque, qui ne peut être exclu totalement compte tenu de la situation juridique actuelle.

Recommandation 10

La recommandation 1 sera également suivie, lorsque le fournisseur d'accès a connaissance de certains contenus de réseaux qui vont à l'encontre de droits d'auteur ou de droits voisins.

2. Recommandation 11: Clause relative aux droits d'auteurs dans le contrat d'abonnement

Le client (demandeur d'informations) du fournisseur d'accès peut utiliser de façon illicite des oeuvres ou des présentations rendues perceptibles de manière juridiquement irréprochable, par exemple en les enregistrant, modifiant ou retransmettant de façon illicite. Etant donné que ces actes sont du seul fait de l'usager, il n'est guère possible de les imputer au fournisseur d'accès faute de conditions subjectives nécessaires à la complicité. Il serait toutefois utile que le fournisseur d'accès indique à son client au moment de conclure le contrat d'abonnement, que celui qui, sur Internet, viole intentionnellement des droits d'auteur ou des droits voisins en est pénalement responsable, donc punissable.

Recommandation 11

Le fournisseur d'accès devrait dans le contrat d'abonnement signaler le devoir de respecter les droits d'auteur et les droits voisins et se réserver le droit de bloquer provisoirement le raccordement en cas de soupçon de violation de ce devoir et de résilier unilatéralement le contrat d'abonnement en cas de violations effectives.

V. Rappel des 11 Recommandations

1	Blocage de l'accès à des contenus illicites	Lorsque le fournisseur d'accès dispose d'indices concrets fondés sur ses propres recherches ou sur celles de tiers permettant de présumer l'éventuel caractère illicite de contenus de réseaux déterminés, il procédera ou fera procéder immédiatement à des investigations afin de déterminer si un blocage s'impose. Lorsque le fournisseur d'accès apprend, de façon certaine, l'existence de contenus de réseaux illicites, notamment réprimés par le droit pénal, il prendra immédiatement les mesures raisonnablement exigibles et techniquement réalisables afin de bloquer l'accès à ces contenus de réseaux.
2	Service central	Il est recommandé à la branche d'instituer un service central chargé de recevoir et d'exploiter les indications communiquées par les fournisseurs d'accès, les clients de ceux-ci et les tiers au sujet de contenus de réseaux illicites. Ce service, conçu en tant que plaque tournante de services et d'informations, devrait transmettre aux fournisseurs d'accès raccordés à ce service des renseignements actualisés sur les contenus de réseaux qu'il convient de bloquer et offrir aux membres de la branche un appui sur les plans scientifique et technique.
3	Accès au réseau	Il est recommandé au fournisseur d'accès de ne conclure en principe des contrats d'abonnement qu'avec des personnes physiques majeures et capables de discernement. De plus, l'abonné ne doit pouvoir accéder au réseau que moyennant une procédure d'identification et un mot de passe (pin-code).

4	Réserve dans le contrat d'abonnement	Dans le contrat d'abonnement, le fournisseur d'accès se réservera le droit de bloquer le raccordement provisoirement en cas de soupçons et de résilier unilatéralement le contrat si le client diffuse des contenus illicites ou en permet la consultation depuis son raccordement.
5	Invitation à annoncer toute utilisation illicite du réseau	Le client sera expressément invité, dans le contrat d'abonnement, à annoncer immédiatement au fournisseur d'accès et/ou au service central (cf. recommandation 2) les contenus de réseaux illicites ou toute autre utilisation illicite d'Internet dont il a connaissance.
6	Formes de représentations de la violence et de pornographie dure	Le fournisseur d'accès doit être conscient du fait que la représentation de la violence, sanctionnée par l'article 135 CP, ne se résume pas seulement à des séquences de films ou à des photographies, mais qu'elle peut aussi prendre la forme d'autres objets ou représentations, tels que des jeux électroniques, et que la promotion et l'offre de représentations de la violence sont également des actes punissables. Il en va de même en ce qui concerne les représentations de pornographie dure au sens de l'article 197, chiffre 3 CP.
7	Information sur les risques en matière de protection des données	Le fournisseur d'accès informera ses clients de manière suffisante sur les risques que peuvent présenter l'utilisation du réseau de même que le recours à des services sous l'angle du droit de la protection des données, et lui fournira des indications concernant les mesures et les produits destinés à garantir la confidentialité, la conformité et la disponibilité des données personnelles (p.ex. des techniques de chiffrage et de cryptage).

8	Traitement de données personnelles	Le fournisseur d'accès ne traitera que les données personnelles relatives à ses clients dont il a besoin pour fournir sa prestation. Des mesures organisationnelles et techniques garantiront l'accès des données traitées exclusivement au personnel qui en a besoin dans l'accomplissement de ses tâches. Les données ne seront pas utilisées dans un but autre que celui qui aura été indiqué lors de leur collecte, qui ressort des circonstances ou qui est prévu dans la loi. Elles ne seront rendues accessibles à des tiers qu'avec l'accord du client ou que sur la base d'une obligation de communication qualifiée.
9	Profils de la personnalité et publication de données personnelles	Le fournisseur d'accès n'établira aucun profil de la personnalité au sujet de ses clients, ni ne rendra leur nom, leur adresse ou leur numéro de téléphone accessible sur un réseau, à moins que la personne concernée n'y ait consenti, ou qu'il n'existe une justification légale ou un intérêt public ou privé prépondérant.
10	Blocage de l'accès en cas de violation des droits d'auteur	La recommandation 1 sera également suivie, lorsque le fournisseur d'accès a connaissance de certains contenus de réseaux qui vont à l'encontre de droits d'auteur ou de droits voisins.
11	Clause relative aux droits d'auteur dans le contrat d'abonnement	Le fournisseur d'accès signalera, dans le contrat d'abonnement, le devoir de respecter les droits d'auteur et les droits voisins et se réserver le droit de bloquer provisoirement le raccordement en cas de soupçon de violation de ce devoir et de résilier unilatéralement le contrat d'abonnement en cas de violations effectives.

Stellungnahme des Eidg. Datenschutzbeauftragten (EDSB) zu datenschutzrechtlichen Fragen, die sich im Zusammenhang mit Internet stellen

1. Vorbemerkung

Anlässlich einer von der Hauptabteilung Strafrecht, Beschwerden und Grundstückserwerb des Bundesamtes für Justiz (BJ) initiierten Sitzung vom 6. September 1995 wurden Rechtsprobleme im Zusammenhang mit Internet diskutiert. Der Eidgenössische Datenschutzbeauftragte wurde dabei eingeladen, die datenschutzrechtlichen Fragen, die sich im Zusammenhang mit Internet ergeben, schriftlich darzulegen.

2. Einleitung

Das Internet kann als die erste Stufe der "Global Information Infrastructure" (GII) betrachtet werden. Bis vor wenigen Jahren waren die Nutzer des weltweiten Computernetzes zum grossen Teil Wissenschafter in Behörden, Universitäten und Forschungsstätten, die in einem kollegialen Vertrauensverhläitnis (sozusagen unter Insidern) Daten austauschten.

Durch den nach wie vor anhaltenden enormen Boom des Internet, hat sich der Nutzerkreis stark ausgeweitet. Vor allem durch die einfachen Abfragemöglichkeiten des World Wide Web (WWW) wird das Netz auch für Firmen und Private attraktiv. Die Benutzer haben sehr unterschiedliche Aufgaben, Möglichkeiten und Motivationen sich der Internet-Dienste zu bedienen. Da das frührere gegenseitige Vertrauen unter den Netzteilnehmern und damit eine weitgehende Selbstregulierung abnimmt, treten immer mehr Vorfälle auf, die Fragen der Legalität in verschiedenen Bereichen aufwerfen. Im Internet werden neben andern Informationen auch Personendaten bearbeitet; daher stellen sich auch datenschutzrechtliche Fragen.

3. Allgemeine datenschutzrechtliche Grundsätze

Seit dem 1. Juli 1993 ist das *Bundesgesetz über den Datenschutz vom 19. Juni 1992* (DSG) in Kraft. Der Datenschutz ergibt sich aus dem Persönlichkeitsrecht und dem verfassungsmässigen, aber ungeschriebenen Grundrecht der persönlichen Freiheit. Es geht beim Datenschutz somit um den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden (Art. 1 DSG).

Datenschutz kommt zum Tragen, wenn *Personendaten bearbeitet* werden. Es wird unterschieden zwischen *Personendaten, besonders schützenswerten Personendaten und Persönlichkeitsprofilen.*

3.1. Daten

Personendaten

sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG), wie Name, Adresse, Geburtsdatum, Grösse, Haarfarbe, Hobby, Arbeitgeber, Foto etc.

In ihrer Persönlichkeit sind sowohl *natürliche Personen* (Menschen) als auch *juristische Personen* (z.B. Aktiengesellschaften), über die Daten bearbeitet werden, geschützt (Art. 3 lit. b DSG).

Besonders schützenswerte Personendaten sind Daten über:

- die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
- die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
- Massnahmen der sozialen Hilfe,
- administrative oder strafrechtliche Verfolgungen und Sanktionen (Art. 3 lit. c DSG).

Fotos können zu besonders schützenswerten Personendaten werden, wenn sie Angaben etwa über die Rassen- und Religionszugehörigkeit einer bestimmten oder bestimmbaren Person machen.

Ein **Persönlichkeitsprofil** ist eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt (Art. 3 lit. d DSG).

3.2 Bearbeiten und Bekanntgeben

Bearbeiten ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, *Bekanntgeben*, Archivieren,Vernichten (Art. 3 lit. e DSG).

Das *Bekanntgeben* ist das Zugänglichmachen von Personendaten wie z.B. das Einsichtgewähren, Weitergeben, Veröffentlichen (Art. 3 lit. f DSG). Unter das Bekanntgeben fällt auch das *Verschicken via E-Mail* und das *Zurverfügungstellen im Abrufverfahren*

3.3 Anwendbarkeit des DSG

Das DSG gilt für das Bearbeiten von Personendaten sowohl duch *private Personen*, als auch durch *Bundesorgane*.

Private Personen sind in erster Linie natürliche und juristische Personen des Privatrechts, Bürger, Bürgerinnen, Handelsgesellschaften etc., aber auch Personen des öffentlichen Rechts (Bundesorgane), soweit sie privatrechtlich handeln.

Bundesorgane sind Behörden und Dienststellen des Bundes, Departemente, Bundesämter, deren Abteilungen und Sektionen, andere öffentlich-rechtlich organisierte Einrichtungen im Bundesbereich, z.B. Körperschaften, Anstalten und Stiftungen, die bei der Erfüllung öffentlich-rechtlicher Aufgaben Daten für den Bund bearbeiten und auch natürliche oder juristische Personen des Privatrechts, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind (z.B. Krankenkassen).

4. Bearbeiten , Datensicherheit, Bekanntgabe, Auskunftsrecht

4.1 Grundsätze

Rechtmässigkeit

Personendaten dürfen nur rechtmässig beschafft werden (Art. 4 Abs. 1 DSG).

Private Personen dürfen Personendaten nur bearbeiten, sofern die Persönlichkeit der betroffenen Person nicht widerrechtlich verletzt wird (Art. 12 DSG); insbesondere dürfen Personendaten nicht gegen den ausdrücklichen Willen einer Person bearbeiten, es sei denn ein im DSG vorgesehener Rechtfertigungsgrund erlaubt dies (Art. 13 DSG).

Bundesorgane dürfen Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht (Art. 17, 19 DSG)

Zweckgebundenheit

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, gesetzlich vorgesehenoder aus den Umständen ersichtlich ist (Art. 4 Abs. 3 DSG).

Verhältnismässigkeit

Es dürfen nur die Personendaten bearbeitet werden, die für die *Aufgabenerfüllung absolut notwendig* sind (Art. 4 Abs. 2 DSG).

Richtigkeit der Daten

Wer Personendaten bearbeitet, muss sich über deren Richtigkeit vergewissern (Art. 5 Abs. 1 DSG). Jede betroffene Person hat das *Recht auf Berichtigung* unrichtiger Daten (Art. 5 Abs. 2 DSG).

Richtigkeit bedeutet allerdings nicht nur, dass Daten keine Falschaussagen enthalten dürfen, sondern auch, dass sie, soweit in einem bestimmten Sachzusammenhang erforderlich, nachgeführt und vollständig sein müssen.

Beispiele: Ein Personalchef, der einen Arbeitnehmer aufgrund eines veralteten Arztzeugnisses versetzt oder entlässt, verletzt dessen Persönlichkeit. Eine Kreditüberprüfung führt zu falschen Schlüssen, wenn daraus hervorgeht, dass jemandem in einem Scheidungsurteil Unterhaltszahlungen auferlegt worden sind, jedoch der Hinweis fehlt, dass die Unterstützungspflicht des Betreffenden infolge Wiederverheiratung seines früheren Ehegatten entfallen ist.

Erfordernis der Datensicherheit

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 Abs. 1 DSG). Ausführungsbestimmungen dazu finden sich in 8 ff, 20 ff. *Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993* (VDSG).

Wer als Privatperson Personendaten bearbeitet oder ein Datenkommunikationsnetz zur Verfügung stellt, sorgt für die Vertraulichkeit, die Verfügbarkeit und die Richtigkeit der Daten, um einen angemessenen Datenschutz zu gewährleisten.

4.2 Massnahmen zur Gewährleistung der Datensicherheit

Zur Gewährleistung der Datensicherheit sind *allgemeine technische und organisatorische Massnahmen* sind zum Schutz der Systeme gegen die Risiken der unbefugten oder zufälligen Vernichtung, des zufälligen Verlusts, technischer Fehler, der Fälschung, des Diebstahls, der widerrechtlichen Verwendung, des unbefugten Änderns, Kopierens, Zugreifens oder anderer unbefugten Bearbeitungen zu treffen.

Die Massnahmen müssen angemessen sein und insbesondere dem Zweck der Datenbearbeitung, der Art und Umfang der Datenbearbeitung, der Einschätzung der möglichen Risiken für die betroffenen Personen und dem gegenwärtigen Stand der Technik Rechnung tragen.

Besondere Massnahmen zur Zugangskontrolle, Zugriffskontrolle, Benutzerkontrolle, Personendatenträgerkontrolle, Transportkontrolle, Bekanntgabekontrolle, Speicherkontrolle und der Eingabekontrolle müssen insbesondere bei der automatisierten Bearbeitung von Personendaten getroffen werden.

4.3 Bekanntgabe ins Ausland

Die Bekanntgabe von Personendaten darf grundsätzlich nur erfolgen, wenn dadurch die Persönlichkeit der betroffenen Person nicht schwerwiegend verletzt wird. Eine schwerwiegende Verletzung wird angenommen, wenn ein Datenschutz fehlt, der dem schweizerischen geichgestellt ist.

Ein Rechtfertigungsgrund kann in der Einwilligung der betroffenen Person liegen.

Die fehlende gleichwertige Datenschutzgesetzgebung kann durch entsprechende Verträge mit den Empfängern der Daten im Ausland geheilt werden.

4.4 Auskunftsrecht

Die Datensammlungen sind so zu gestalten, dass die betroffenen Personen ihr *Auskunftsrecht* (Art. 8 DSG) wahrnehmen können.

4.5 Verantwortlichkeit für die Gewährleistung des Datenschutzes

Für die Gewährleistung des Datenschutzes ist zum einen die Privatperson oder das Bundesorgan verantwortlich, die/das die Daten selber bearbeitet oder die Daten durch einen Dritten bearbeiten lässt, zum anderen der Datenkommunikationsnetzbe-

treiber, wobei es sich bei dem Datenkommunikationsnetz um ein logisches und/oder ein physikalisches handeln kann.

5. Datenschutz und Internet

5.1 Generelle Datenschutzrisiken im Internet:

Alle, die in irgendeiner Form Personendaten bearbeiten, sind an diese Grundsätze gebunden. Das bedeutet, dass jeder, der über Internet Personendaten z.B. verschickt oder im Abrufverfahren zugänglich macht, die oben ausgeführten Grundsätze zu berücksichtigen hat.

Ebenso gelten diese Grundsätze unabhängig von der Art bzw. der Sensibilität der Personendaten. Die Grundsätze finden somit sowohl auf die Angaben von etwa Qualifizierungen, Spezialitäten, Hobbies, Körpermasse etc. einer bestimmten oder bestimmbaren Person Anwendung, als auch auf die Angabe von Name, Adresse, Telefonnummer und anderer Kommunikationsparameter.

Je sensibler die Personendaten werden, desto höher sind die Anforderungen an den Datenschutz.

Das Bekanntgeben von Personendaten im Internet stellt aufgrund der möglichen nationalen, internationalen und globalen Verfügbarkeit, Verknüpfbarkeit und Nicht-Kontrollierbarkeit, wer was mit den Personendaten macht, aus datenschutzrechtlicher Sicht ein grosses Problem dar.

Über Internet ist eine enorme Menge von Informationen, darunter auch ein grosser Teil Personendaten erreichbar. Es ist zu bedenken, dass durch die Verknüpfung mehrerer Datenbestände, die einzeln unproblematisch sein können, schwer abschätzbare Risiken (z.B. Persönlichkeitsprofile, Kaufprofile, Bewegungsprofile) entstehen können.

Einmal über Internet öffentlich zugängliche Daten stehen einer äusserst grossen Benutzerzahl zur Verfügung. Sie können abgerufen, lokal gespeichert, weiterbearbeitet und an Dritte weitergegeben werden. Eine genaue Kontrolle, wohin die Daten fliessen und auf welche Weise diese ausgewertet werden, ist nicht mehr möglich. Zudem ist es insbesondere wegen der Indexierung, dem Caching im WWW etc. fast unmöglich, Daten wieder zu entfernen.

Bekanntgabe von Personendaten im Internet durch Private:

Werden durch Dritte *(Private)* Personendaten im Internet zum allgemeinen Abruf national, international, global bereitgestellt werden, sollte eine Einwilligung der betroffenen Person in schritflicher Form oder mittels eines vergleichbaren Verfahrens vorliegen, diese umfasst folgende Elemente:

- die Kenntnisnahme von den Gefahren und Möglichkeiten des Netzes (Verfügbarkeit, Verknüpfbarkeit, Vertraulichkeit)
- die Kenntnisnahme der weltweiten Verfügbarkeit
- die Kenntnisnahme davon, dass in Ländern, in denen die Daten verfügbar sind, keine adäquate Datenschutzgesetzgebung besteht
- die Kenntnisnahme, auf welchem Netz die Daten verfügbar sind
- die Kenntnisnahme des Zwecks der Bearbeitung auf dem Netz
- die Kenntnisnahme der gespeicherten Daten
- einen Widerrufsvorbehalt, der auch das Recht auf Korrektur einschliesst

Für die Bekanntgabe von Personendaten im Arbeitsverhältnis gelten strengere Bedingungen über Art. 362, 328b OR.

Bekanntgabe von Personendaten im Internet durch Bundesorgane:

Sollen von *Bundesorganen* Personendaten im Internet national, international oder global zum Abruf zur Verfügung gestellt werden, ist darauf zu achten, dass das Zur-Verfügung-Stellen von Personendaten im Internet eine Bekanntgabe von Personendaten im Abrufverfahren ist. Gemäss Art. 19 Abs. 3 DSG dürfen Bundesorgane Personendaten im Internet nur zum Abruf zur Verfügung stellen, *wenn dies in einer gesetzlichen Grundlage ausdrücklich vorgesehen ist.* Die Möglichkeit der Zulässigkeit von Bekanntgaben aufgrund von Einwilligungen der betroffenen Personen sieht das DSG nur für den Einzelfall der Bekanntgabe vor (Art. 19 Abs. 1 lit. b DSG). Da aber im Abrufverfahren eine Vielzahl von Abfragen von den unterschiedlichsten Stellen zu den unterschiedlichsten Zeiten erfolgen kann, kann nicht mehr von einem Einzelfall im Sinne des Art. 19 Abs. 1 lit. b DSG ausgegangen werden.

Bekanntgabe von Personendaten ins Ausland:

Das Internet kennt als globales Netz keine nationalen Grenzen. Daten werden in Staaten übertragen, die keine oder nur unzureichende Datenschutzbestimmungen kennen. Auch ist der Zugriff auf Datenbestände von solchen Ländern aus möglich. Gemäss Art. 6 Abs. 1 DSG ist die Übermittlung von Daten in andere Länder unzulässig, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde. Das ist grundsätzlich der Fall, wenn in den anderen Ländern keine dem schweizerischen Datenschutz vergleichbare Gesetzgebung besteht.

Import von Personendaten aus dem Ausland:

Werden Personendaten aus dem Ausland importiert, fallen diese unter den Anwendungsbereich des DSG. Werden Daten in andere Länder importiert, fallen sie unter deren Datenschutzgesetzgebungen, was dazu führt, dass ein und dieselben Personendaten in einem Land nur unter sehr strengen datenschutzschrechtlichen Bedin-

gungen bearbeitet werden dürfen, in einem anderen Land keinen Reglementierungen unterworfen sind.

Immer häufiger wächst der Wunsch, firmeninterne Netze mit dem Internet zu verbinden, einerseits um das Informationsangebot zu nutzen, andererseits um einen Teil der Firmeninformationen im Netz zu verbreiten. Eine wirksame Massnahme zur Abschottung vertrauenswürdiger Netze vor unsicheren Netzen ist die Verwendung von Zwischenrechnern (sog. Firewalls), solange das Internet keine eigenen wirksamen Mittel zur Authentifizierung und/oder Chiffrierung bereitstellt.

Aus diesen Ausführungen folgt, dass international die Harmonisierung der Datenschutzgesetzgebungen, insbesondere im Bereich des Internet sowie die Einführung einer zentralen Kontrolle anzustreben ist.

5.2 Datenschutzrisiken bei speziellen Internet-Diensten

Im folgenden werden anhand einzelner Internet-Dienste mögliche Datenschutz-Risiken dargestellt und Lösungsansätze aufgezeigt. Die Aufzählung der Dienste und möglichen Gefahren erhebt keinen Anspruch auf Vollständigkeit:

5.2.1 E-Mail

Electronic Mail (E-Mail) ermöglicht die weltweite Kommunikation zwischen verschiedenen Partnern im Netz. Es handelt sich um den meistgenutzten Internet-Dienst. Die Vertraulichkeit der übertragenen Daten kann nicht als gegeben betrachtet werden: Wer unverschlüsselte Nachrichten verschickt, muss damit rechnen, dass diese von Dritten gelesen werden können. Ebenso hat der Empfänger einer E-Mail keine Garantie, dass der Absender auch derjenige ist, für den er sich ausgibt. Eine Fälschung seiner Kennungen ist technisch möglich. Weiter kann nicht ausgeschlossen werden, dass die übertragene Nachricht auf ihrem Weg unbefugt und unbemerkt verändert oder unterdrückt wird, dass die Übertragung zeitlich verzögert oder bei Transaktionen die Reihefolge vertauscht wird.

Kommunikationspartner können jedoch selbst gewisse Massnahmen ergreifen, die Vertraulichkeit, Verbindlichkeit und Integrität zu gewähren. (kryptographischen Verfahren)

Auch wenn die versandten Nachrichten vertraulich übertragen werden, ist das Risiko vorhanden, dass Kommunikationsprofile erstellt werden d.h. dass systematisch erhoben wird, wer mit wem Nachrichten ausgetauscht hat.

Die E-Mail-Adresse kann gegebenenfalls Angaben über den Adressaten entalten: Beispielsweise: Name, Vorname, Staat, Art der Organisation (privat, staatliche Behörde, non-profit-organisation, Universität etc.), Abteilung, Provider etc.

5.2.2 Newsgroups

Newsgroups sind elektronische Diskussionsforen. Die Beiträge, die in diese Foren (im Internet existieren mehrere tausend zu den unterschiedlichsten Themen) geschrieben werden, sind öffentlich. Alle interessierten Internet-Benutzer können die gewünschten Newsgroups anwählen und die Artikel lesen und sich an den Diskussionen beteiligen. Auch dies knn wie bei E-Mail ge- oder verfälscht werden.

Die Artikel können abgespeichert und nach Belieben (z.B. nach bestimmten Stichwörtern) ausgewertet werden. Die Auswertung kann mit Mitteln und in einem Masse erfolgen, denen sich die Benutzer nicht oder nur begrenzt bewusst sind.

Es existieren im Internet öffentlich zugängliche Datenbanken, bei denen nach Stichwörtern sowie nach Sender/Empfänger von Newsgroup-Artikeln gesucht werden kann. So ist es möglich, die Artikel, die ein bestimmter Internet-User im Laufe der Zeit in die diversen Newsgroups geschrieben hat, aufzulisten und auszuwerten. Dabei kann ein umfassendes Bild der Persönlichkeit entstehen, wie dies beim Lesen einzelner Artikel meist nicht der Fall ist. Zudem können Newsgroup-Artikel Personendaten über Dritte enthalten. Da diese Daten weltweit abgerufen und gespeichert werden, ist es den Betroffenen praktisch unmöglich, die Bearbeitung zu kontrollieren.

5.2.3 File Transfer Protocol (FTP) und Telnet:

FTP ist ein Dienst, der es erlaubt, Dateien von und nach Internet-Servern zu transferieren. Zum einen stellt sich das Problem der Vertraulichkeit der Dateien (siehe E-Mail) zum andern dasjenige des Kommunikationsverhaltens.

Mit dem Telnet-Dienst kann sich ein Internet-Benutzer von seinem Terminal aus auf einem entfernten Rechner im Netz arbeiten.

Sowohl bei FTP und Telnet besteht das Risiko des Abflusses von Personendaten in Länder mit qualitativ geringeren Datenschutzbestimmungen als im Ursprungsland.

Es bestehen die Gefahren des Mithörens der Benutzername/Passwort-Kombination und der Benutzerdaten.

5.2.4 World Wide Web

Über das äusserst populäre World Wide Web (WWW) können Internet-Informationen über eine bequeme Benutzeroberfläche (Hypertextsystem) abgerufen werden. Anhand der besuchten Server und abgerufenen Informationen kann unter Umständen ein Bild der Persönlichkeit offenbar werden. (siehe Abschnitt: Internet-Provider)

Die zum grossen Teil öffentlichen Informationen im WWW können, wie die Newsgroup-Artikel, Personendaten von Dritten enhalten. Per Abrufverfahren ist der Zugriff auf Datenbestände aller Art möglich.

Bei einigen Servern werden mittels elekronischer Fragebogen Daten erfasst, bei denen eine Missbrauchsgefahr nicht ausgeschlossen werden kann. Hier liegt es am Netz-Benutzer zu entscheiden, welche seiner Personendaten er wo preisgeben will.

Ein Betreiber eines Internet-Servers erhält Angaben über diejenigen Netz-Benutzer, die seine Seiten besuchen. Er "sieht" die IP-Adresse sowie allenfalls weitere Angaben über den verwendeten WWW-Browser etc. Die IP-Adresse identifiziert den Benutzer nicht unbedingt eindeutig. Falls er sich über eine Wählleitung beim Provider einwählt, werden die IP-Adressen meist dynamisch zugewiesen, d.h. es wird eine IP-

Adresse vergeben, die momentan gerade nicht genutzt wird. Dem Provider seinerseits ist jedoch bekannt, zu welcher Zeit jeder seiner Kunden mit welcher IP-Adresse im Netz war, da sich diese mit User-ID und Passwort authentifizieren.

Hat der Abfragende seinen Browser für E-Mail-Zwecke so konfiguriert, dass beim E-Mail auch seine Klartext-Adresse mitgeliefert wird, hat das zur Folge, dass die Klartext-Adresse auch bei Abfrage der WWW-Seite, jedoch ohne Kenntnis des Abfragenden, mitgeliefert wird.

Zudem kann dank WWW-Indices, die automatisch gepflegt werden, das Internet (WWW usenet, ftp) fast flächendeckend durchsucht und das Ergebnis weiterverarbeitet werden.

5.3. Internet-Provider

Der Internet-Provider (Provider) bietet seinen Kunden den Zugang zum Internet. Er bietet die technischen Vorraussetzungen, um Internetdienste zu nutzen.

Zudem bieten Provider auch oben angeführte Dienste an.

5.3.1 Bearbeitung von Personendaten durch den Provider

Zum einen bearbeitet der Provider, um das Geschäft mit seinen Kunden abwickeln zu können, Personendaten, wie Name, Adresse, Telefonnummer, Art der technischen Ausrüstung etc. Diesbezüglich finden die Bestimmungen des DSG auf ihn Anwendung.

Der Provider darf ausschliesslich diejenigen Personendaten seiner Kunden bearbeiten, die er zur Erfüllung seiner Dienstleistung benötigt. Diese variieren je nach Abrechnungsmodus. Die einen Provider erheben lediglich eine Pauschalgebühr, andere erheben auch Zeit und/oder Volumengebühren.

Die bearbeiteten Daten sind durch technische und organisatorische Massnahmen ausschliesslich dem Personal zugänglich zu machen, das sie zur Erfüllung ihrer Aufgabe benötigen. Die Daten dürfen zu keinem andern Zweck verwendet werden als demjenigen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist.

Die Daten dürfen Dritten nur zugänglich gemacht werden, sofern der Kunde einverstanden ist bzw. eine gesetzliche Pflicht zur Bekanntgabe besteht. Sofern die Kommunikationsdaten als sogenannte Randdaten unter das Fernmeldegeheimnis gem. Art. 15 FMG fallen, geht dieses als lex specialis dem DSG vorgeht.

Darüber hinaus ist es dem Provider technisch möglich, das *Kommunikationsverhalten* seiner Kunden weitgehend zu erfassen. Er kann feststellen, zu welchen Zeiten ein Benutzer im Netz aktiv ist, welche Dienste er nutzt, mit welchen andern Internetbenutzern er elektronisch in Kontakt tritt sowie welche Informationen er von welchen Servern abruft. In diesem Zusammenhang ist die Entstehung von Persönlichkeitsprofilen - d.h. Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Art. 3 lit. d DSG) - möglich. Das Erstellen derartiger Kommunikationsprofile ist, sofern nicht durch Einwilligung der betroffenen Person, durch ein Gesetz oder ein überwiegendes öffentliches oder privates Interesse gerechtfertigt, unzulässig.

Einzelne Provider stellen ihre Kundenlisten mit geschäftlicher bzw. privater Telefonnummer weltweit der gesamten Netzgemeinde zum Abruf zur Verfügung. Dies ist nur zulässig, sofern die betroffene Person eingewilligt hat, durch ein überwiegendes öffentliches oder privates Interesse oder durch Gesetz gerechtfertigt ist.

Die Provider sollen die Kunden auf die getroffenen technischen und organisatorischen Massnahmen hinweisen, damit diese die Risiken möglichst gut einschätzen können und ihr Verhalten anpassen können.

5.3.2 Verantwortlichkeit des Providers

Grundsätzlich hat die Person, die Personendaten über ein Netz verschickt, in einem Netz Personendaten zum Abruf zur Verfügung stellt oder abruft, die Bearbeitungsgrundsätze des DSG, insbesondere den der Datensicherheit gem. Art. 7 DSG i.V.m. Art. 8 ff. Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 zu beachten. Das heisst, dass diese Person für die Erfüllung dieser Bedingungen verantwortlich ist. Verschickt sie Personendaten über ein Kommunikationsnetz, das ein Dritter zur Verfügung stellt, so hat sie dafür zu sorgen und ist dafür verantwortlich, dass die Anforderungen an die Datensicherheit auch beim Transport über die Leitungen gewährleistet sind.

Neben der Person, die z.B. die Personendaten über die Leitungen verschickt, ist auch der Dritte, der das Datenkommunikationsnetz zur Verfügung stellt, soweit es in seinen Möglichkeiten liegt, dafür verantwortlich, dass die in Art. 8 VDSG aufgezählten Anforderungen erfüllt sind (vgl. hierzu auch Punkt 6.1 der Empfehlung Nr. R (95) 4 des Europarates betreffend den Datenschutz im Bereich der Telekommunikationsdienste, insbesondere der Telefondienste). Dies bedeutet, dass grundsätzlich für die Vertraulichkeit, Verfügbarkeit und Richtigkeit sowohl derjenige verantwortlich ist, der die Personendaten verschickt, als auch derjenige, der das Datenkommunikationsnetz bzw. die Leitungen zur Verfügung stellt. Der Provider ist als jemand anzusehen, der ein Datenkommunikationsnetz zur Verfügung stellt. An die Möglichkeiten, die ein Provider hat, die Vertraulichkeit, Verfügbarkeit und Richtigkeit der Daten zu gewährleisten, sind jedoch nicht allzu grosse Anforderungen zu stellen. So soll der Provider seinen Kunden über die datenschutzrechtlichen Risiken, die sich aus dem Benutzen des Netzes sowie der Inanspruchnahme von Diensten ergeben können, ausreichend informieren sowie ihn auf Massnahmen und Produkte zur Gewährleistung der Vertraulichkeit, Richtigkeit und Verfügbarkeit von Personendaten hinweisen.

Datenautobahnen aus der Sicht des Urheberrechts und der verwandten Schutzrechte

1. Vorbemerkungen

Die Informationsgesellschaft und ihre neuen Kommunikationsmittel wie Datenautobahnen oder auch Multimedia stellen bezüglich des Urheberrechtsschutzes eine Reihe rechtlicher Fragen. Eine davon ist sicherlich diejenige, ob der gegenwärtige Schutz ausreicht, um die Verwendung von Werken der Literatur und Kunst sowie von nachbarrechtlich geschützten Leistungen (vgl. hinten Ziff. 4) in diesem neuen Umfeld zu kontrollieren. Offen ist aber auch noch, wie sich diese Rechte anwenden und durchsetzen lassen, ohne dass dabei der Informations- und Dokumentationsfluss allzusehr eingeschränkt wird.

Da die Datenautobahnen ein grenzüberschreitendes Phänomen darstellen, stellen sich sowohl auf nationaler wie auf internationaler Ebene ähnliche Fragen und daher sind auch gegenwärtig die verschiedensten Gremien daran, zu prüfen, ob und allenfalls welche Massnahmen zu ergreifen sind, damit urheberrechtlich geschützte Werke und die durch die verwandten Schutzrechte geschützten Leistungen im Rahmen der neuen technischen Möglichkeiten der erforderliche Schutz gewährt werden kann und gleichzeitig auch die berechtigten Bedürfnisse der Nutzer berücksichtigt werden können. Es sei hier nur kurz auf die aktuellen Bestrebungen der Weltorganisation für geistiges Eigentum (OMPI) hingewiesen, mit einem Zusatzprotokoll zu einer weltweiten Urheberrechtskonvention (Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst; vgl. hinten Ziff. 6) die im Zusammenhang mit den neuen technischen Möglichkeiten aufgetauchten Rechtsfragen aus urheberrechtlicher Sicht in den Griff zu bekommen. Auch in der EU (mit dem Grünbuch über das Urheberrecht und verwandte Schutzrechte in der Informationsgesellschaft), den USA (Intellectual Property and the National Information Highway) oder in Frankreich (Industries culturelles et nouvelles techniques) sowie in weiteren Staaten sind entsprechende Berichte erschienen.

In der Schweiz ist gegenwärtig insbesondere die Schweizerische Vereinigung für Urheber- und Medienrecht (SVUM) daran, ein umfassendes Werk über den 'Information Highway' herauszugeben. Diese Arbeit wird über das Urheberrecht hinausgehen und auch andere Rechtsgebiete (wie Kommunikationsrecht, Datenschutz, Strafrecht, Rechtsstellung des Access Providers, zivilrechtliche Haftung usw.) abdecken und ebenfalls einige interdisziplinäre Beiträge (technische und praktische Seite des Information Highway) enthalten.

Im folgenden geht es darum zu prüfen, inwieweit über Datenautobahnen (wie das Internet) überhaupt urheberrechtlich geschützte Inhalte angeboten werden und welche Probleme aus urheberrechtlicher Sicht sich daraus ergeben können. Da gegenwärtig noch vieles im Fluss ist und man sich in diesem Bereich noch auf unsicherem rechtlichen Boden befindet, erhebt dieses Papier nicht den Anspruch auf Vollständigkeit.

2. Gesetzliche Grundlage

In der Schweiz wird das Urheberrecht durch das Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, URG) vom 9. Oktober 1992 geregelt. Der Schutz dieses Gesetzes gilt nach Artikel 1 URG für

- Urheber von Werken der Literatur und Kunst *(Urheberrecht);*
- ausübende Künstler, Hersteller von Ton- und Tonbildträgern sowie für Sendeunternehmen *(verwandte Schutzrechte)*.

Obwohl das URG ein relativ junges Gesetz ist, sind bei dessen Erlass die neuesten technologischen Herausforderungen wie etwa Datenautobahnen oder Multimedia noch kaum bekannt gewesen und daher auch unberücksichtigt geblieben.

Im weiteren gelten auch die internationalen Abkommen auf dem Gebiet des Urheberrechts und der verwandten Schutzrechte, denen die Schweiz angehört (vgl. hinten Ziff. 6).

3. Urheberrechtsschutz

3.1. Werke der Literatur und Kunst

Urheberrechtsschutz geniessen Werke der Literatur und Kunst (Art. 2 Abs. 2 URG) wie etwa:

- *Texte* jeglicher Art (vom Roman über die wissenschaftliche Abhandlung und den Zeitungsartikel bis hin zum Werbeprospekt);
- *Werke der Musik*;
- *Werke der bildenden Kunst* (wie Malerei, Bildhauerei, Graphik);
- *Werke mit wissenschaftlichem oder technischem Inhalt* wie Zeichnungen, Pläne oder Karten;
- *visuelle oder audiovisuelle Werke* wie Fotografien und Filme;
- *Computerprogramme*.

3.2. Schutzvoraussetzungen

Die obgenannten Werke sind aber nur urheberrechtlich geschützt (Art. 2 Abs. 1 URG), falls sie

- zum Bereich der Literatur und Kunst gehören;
- das Ergebnis einer geistigen Schöpfung sind und
- einen individuellen Charakter haben; d.h. das Merkmal der Individualität bzw. der Originalität erfüllen (gemäss Bundesgericht ist dies der Fall bei *'konkreten Darstellungen, die nicht bloss Gemeingut enthalten, sondern insgesamt als Ergebnis geistigen Schaffens von individuellem Gepräge oder als Ausdruck einer neuen originellen Idee zu werten sind; Individualität oder Originalität gelten denn auch als Wesensmerkmale des urheberrechtlich geschützten Werkes'; BGE 113 II 196).*

Der Urheberrechtsschutz umfasst auch *Entwürfe, Titel und Teile* von Werken, sofern die obigen Schutzvoraussetzungen erfüllt sind. Es kommt somit nicht auf den Aufwand oder die finanziellen Mittel zur Schaffung eines Werkes an. Im Einzelfall obliegt es indessen den ordentlichen Gerichten verbindlich festzustellen, ob die Schutzvoraussetzungen erfüllt sind.

Es ist offensichtlich, dass auf Datenautobahnen urheberrechtlich geschützte Inhalte (wie Filme, Fotos, Texte, Musik usw.) angeboten, weiterverbreitet, gespeichert, verändert und auch anderswie genutzt werden.

3.3. Werke zweiter Hand und Sammelwerke

Ein *Werk zweiter Hand* (Art. 3 URG) liegt vor, falls ein bereits vorhandenes Werk (ursprüngliches Werk) so bearbeitet wird, dass sein *individueller Charakter erkennbar bleibt*. Das Gesetz nennt als Beispiele Übersetzungen oder audiovisuelle Bearbeitungen. Aber auch jede andere Bearbeitung eines schon bestehenden Werkes kann zu einem Werk zweiter Hand führen. Obwohl auch Werke zweiter Hand denselben Schutz wie die ursprünglichen Werke geniessen, bleibt in diesen Fällen das Recht der am ursprünglichen Werk Berechtigten (Urheber bzw. Rechtsinhaber) vorbehalten; Werke zweiter Hand dürfen somit nur mit deren Zustimmung an die Öffentlichkeit gebracht werden. Da es ohne weiteres möglich ist, auf Datenautobahnen eingespeiste Werke herunterzuladen, zu speichern und zu bearbeiten, kommt dieser Bestimmung besondere Bedeutung zu.

Sammlungen (Art. 4 URG) sind geschützt, sofern es sich bezüglich Auswahl oder Anordnung um geistige Schöpfungen mit individuellem Charakter handelt. Der Schutz besteht unabhängig davon, ob die einzelnen Bestandteile urheberrechtlich geschützt sind oder nicht. Damit ist klar, dass auch eine Datenbank als solche urheberrechtlichen Schutz geniessen kann, ohne dass die einzelnen Elemente geschützt sein müssen. Auch diese Bestimmung ist in diesem Zusammenhang

wesentlich, ist es doch eine der wichtigen Funktionen des Internet, den Zugriff auf verschiedenste Datenbanken (Bibliographische Datenbanken, Faktendatenbanken, Volltextdatenbanken, numerische Datenbanken, Textdatenbanken usw.) zu ermöglichen.

3.4. Das Kollektivwerk

Ein Werk kann auch von mehreren Personen gemeinsam geschaffen werden. Dies ist gerade bei Filmen oder auch Computerprogrammen die Regel. Das Gesetz spricht hier von *Miturheberschaft* und gesteht den Beteiligten gemeinsam das Urheberrecht zu (Art. 7 URG). Ein solches Werk darf somit nur mit Zustimmung aller Miturheber verwendet werden, was natürlich die Einholung der entsprechenden Rechte besonders erschwert. Allerdings befinden sich diese Rechte vielfach gebündelt bei einem Rechtsinhaber (z.B. Produzent, Arbeitgeber oder Auftraggeber), der sich die entsprechenden Rechte durch einen Vertrag hat abtreten lassen. Das URG (Art. 17) überlässt im übrigen die ausschliesslichen Verwendungsbefugnisse an einem Computerprogramm von Gesetzes wegen dem Arbeitgeber.

3.5. Nicht geschützte Werke

Nach schweizerischem Recht (Art. 5 URG) geniessen Gesetze, Verordnungen, andere amtliche Erlasse, Entscheidungen, Protokolle und Berichte von Behörden und öffentlichen Verwaltungen, Zahlungsmittel sowie amtliche oder gesetzlich geforderte Sammlungen (wie die Amtliche oder die Systematische Gesetzessammlung des Bundes) und Übersetzungen solcher Werke *keinen Schutz*. Deren Benützung ist somit aus urheberrechtlicher Sicht uneingeschränkt möglich. Frei ist natürlich auch die Benutzung von Werken, bei denen die Schutzfrist abgelaufen ist (vgl. hinten Ziff. 7.1.2).

4. Geschützte Leistungen (verwandte Schutzrechte)

Neben den Urhebern von Werken der Literatur und Kunst schützt das Urheberrechtsgesetz unter dem Titel *verwandte Schutzrechte* auch:

- die *ausübenden Künstler*, d.h. Personen, die ein Werk darbieten oder an der Darbietung eines Werkes mitwirken (Art. 33 URG);
- die *Hersteller von Ton- und Tonbildträgern* (Art. 35 URG) sowie
- die *Sendeunternehmen* (Art. 36 URG).

5. Geltungsbereich

In der Schweiz sind Werke unabhängig von der Staatsbürgerschaft des Urhebers bzw. vom Ort der Veröffentlichung oder der Herausgabe geschützt. Der gleiche Grundsatz gilt für die Berechtigten aus den verwandten Schutzrechten.

6. Internationale Abkommen

Im Bereich der internationalen Beziehungen sind in erster Linie die bereits erwähnte *Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst* (RBUe; über 100 Mitgliedstaaten) und das *Welturheberrechtsabkommen* (WUA; ebenfalls ca. 100 Mitgliedstaaten) zu erwähnen. Beide Abkommen sehen die Inländerbehandlung vor und gewährleisten einen Mindestschutz, wobei allerdings das Schutzniveau unterschiedlich hoch ist Das wichtigste internationale Abkommen für die verwandten Schutzrechte ist das *Abkommen über den Schutz der ausübenden Künstler, der Hersteller von Tonträgern und der Sendeunternehmen* (Rom-Abkommen; ca. 50 Mitgliedstaaten). Die Schweiz gehört allen drei Abkommen an.

7. Entstehung und Ende des Schutzes

7.1. Urheberrecht

7.1.1. Entstehung des Schutzes

Sowohl in der Schweiz als auch in allen übrigen Mitgliedstaaten der Berner Übereinkunft sind zur Erlangung des Urheberrechtsschutzes *keine Formalitäten* zu erfüllen, wie etwa die Hinterlegung oder Registrierung des Werkes oder das Anbringen irgend eines Vermerkes auf den Werkexemplaren bzw. das Erscheinen eines entsprechenden Hinweises auf dem Bildschirm beim Abrufen des Werkes aus einer Datenbank. Der gesetzliche Schutz tritt ohne weiteres mit der Schaffung des Werkes durch eine natürliche Person ein (vgl. hinten Ziff. 8).

Die ausschliesslich dem *Welturheberrechtsabkommen* - nicht aber der Berner Übereinkunft - angehörenden Staaten sind allerdings befugt, den Urheberrechtsschutz von der Anbringung des Kennzeichens © mit dem Namen des Urheberrechtsinhabers und der Jahreszahl der ersten Veröffentlichung an einer gut sichtbaren Stelle jedes Werkexemplares abhängig zu machen. Die Erfüllung weiterer Formalitäten kann aber auch hier nicht gefordert werden. In der Schweiz ist ein solcher Hinweis nicht erforderlich und ein Urheberrecht kann auch ohne ihn geltend gemacht und durchgesetzt werden.

7.1.2. Ende der Schutzdauer

Der Urheberrechtsschutz erlischt in der Schweiz *70 Jahre nach dem Tod* des Urhebers (Art. 29 URG) (Nach der Berner Übereinkunft sind Werke mindestens bis 50 Jahre nach dem Tod des Urhebers geschützt. Somit kann die Einspeisung eines Werkes auf eine Datenautobahn in einem Land mit niedriger Schutzfrist durchaus gesetzeskonform sind, das Kopieren in der Schweiz aber unter den Verbotsanspruch des Urhebers fallen, da das Werk hier aufgrund der Inländerbehandlung noch geschützt ist). *Für Computerprogramme gilt eine Schutzdauer von 50 Jahren*, welche ebenfalls mit dem Tod des Urhebers zu laufen beginnt.

Haben mehrere Personen bei der Schaffung eines Werkes mitgewirkt, so beginnt die Schutzfrist nach dem Tod der zuletzt verstorbenen Person zu laufen (Art. 30 URG); für anonyme oder pseudonyme Werke mit der Veröffentlichung des Werkes (Art. 31). Bei *audiovisuellen Werken* (Filmen) ist für die Berechnung der Schutzdauer der Tod des Regisseurs massgebend (Art. 30 Abs. 3 URG).

7.2. Verwandte Schutzrechte

Der Schutz der verwandten Schutzrechte ist ebenfalls formlos und die Schutzdauer beginnt mit der Darbietung des Werks durch den ausübenden Künstler, mit der Herstellung des Ton- oder Tonbildträgers oder mit der Ausstrahlung der Sendung und dauert ab diesem Zeitpunkt 50 Jahre (Art. 39 URG). Das Rom-Abkommen sieht eine Mindestschutzdauer von 20 Jahren vor.

8. Übertragung des Urheberrechts

Urheber ist die *natürliche Person,* die das Werk geschaffen hat (Art. 6 URG). Diese ist auch originärer Rechtsinhaber. *Juristische Personen* (Unternehmen) können Urheberrechte somit nur vertraglich erwerben.

Die Übertragung eines im Urheberrecht enthaltenen Rechts (vgl. hinten Ziff. 9.1) schliesst die Übertragung anderer Teilrechte nicht in sich, wenn nichts Gegenteiliges vereinbart worden ist. Insbesondere gilt in diesem Falle die Übertragung des Wiedergaberechts nur für die unveränderte Wiedergabe. Die Übertragung der Urheberrechte ist *formfrei* (Art. 16 URG). Selbstverständlich ist es einem Urheber auch möglich, auf seine Rechte zu verzichten. In diesem Fall dürfen die Werke im Rahmen des Verzichts frei gebraucht werden. Ein solcher Verzicht muss allerdings in der Regel ausdrücklich vermerkt sein. Ohne entsprechenden Vermerk ist davon auszugehen, dass der Urheber seine Rechte wahrnehmen will (Zur Frage, ob allenfalls mit der Einspeisung eines Werkes auf eine Datenautobahn durch den Urheber selbst auf die Geltendmachung gewisser Rechte verzichtet wird, vgl. hinten Ziff. 9.1).

Neben der Übertragung von Rechten ist es auch möglich, mittels eines Lizenzvertrages entsprechende Verwendungsbefugnisse einzuräumen.

9. Inhalt des Urheberrechts und der verwandten Schutzrechte

9.1. Urheberrecht

Der Urheber hat zunächst das Recht zu bestimmen, ob, wann und wie sein Werk erstmals veröffentlicht werden soll (Art. 9 Abs. 2 URG). Eine Veröffentlichung liegt vor, wenn das Werk *zum ersten Mal* rechtmässig einer grösseren Anzahl Personen zugänglich gemacht wird. Der Urheber hat somit das alleinige Recht, sein unveröffentlichtes Werk erstmals auf eine Datenautobahn einzuschleusen. Mit der erstmaligen Veröffentlichung gilt dieses Recht als konsumiert.

Von Bedeutung für die Verwendung eines Werkes auf einer Datenautobahn sind aber auch die weiteren Rechte, welche der Urheber an einem Werk hat. Dabei gilt

als Grundsatz (Generalklausel), dass ihm *das ausschliessliche Recht* zusteht, zu bestimmen, ob, wann und wie sein Werk *verwendet* werden darf (Art. 10 Abs. 1 URG) Der Gesetzgeber hat diese offene und nicht abschliessende Formulierung gewählt, damit auch künftige, zur Zeit der Gesetzgebung noch nicht bekannte Nutzungsformen eingeschlossen sind. Damit erfasst aber das geltende URG auch die Nutzung urheberrechtlich geschützter Werke auf den Datenautobahnen.

Zu den besonders erwähnten Verwendungsarten gehören unter anderem:

- *das Vervielfältigungsrecht (Art. 10 Abs. 2 Bst. a URG);* d.h. das Recht, ein Werk durch irgend ein Verfahren zu kopieren (Herstellung von weiteren Werkexemplaren mittels Druck, Ton-, Tonbild- oder Datenträger). Gemeint ist somit zunächst die Wiedergabe auf einem dauerhaften Material. *Aber es bestehen keine Zweifel, dass auch das herunterladen eines Werkes auf die Festplatte eines Computers als Vervielfältigung gilt.* Eine derartige Kopie erlaubt es ebenfalls, ein Werk erneut zu verwenden, weiterzuverbreiten oder gar zu ändern. Wesentlicher Unterschied im Internet ist, dass ein Werk bzw. dessen Inhalt in digitalisierter Form übermittelt wird; dabei entsteht beim Vervielfältigen eines Werkes eine dem Original qualitativ ebenbürtige Kopie. Damit ist aber auch klar, dass das Speichern eines Werkes aus dem Internet auf den eigenen Computer, die Einspeicherung in eine Datenbank oder das Laden von einer elektronischen Bibliothek zum Vervielfältigungsrecht des Urhebers gehören, da hierbei entsprechende neue Werkexemplare entstehen.
- *das Verbreitungsrecht (Art. 10 Abs. 2 Bst. b URG)* ist das Recht des Urhebers, Werkexemplare anzubieten, zu veräussern oder sonstwie in Verkehr zu bringen. Da im Internet grundsätzlich keine körperlichen Werkexemplare entstehen, sondern die Weitergabe regelmässig mit einer Vervielfältigung verbunden ist, spielt das Verbreitungsrecht nur eine untergeordnete Rolle.
- *das Recht ein Werk wahrnehmbar zu machen (Art. 10 Abs. 2 Bst. c URG)*. Der Urheber bzw. der Rechtsinhaber hat das ausschliessliche Recht, sein Werk anderswo (auch mit technischen Mitteln wie Datenautobahn) wahrnehmbar zu machen. Damit hat er aber auch die Möglichkeit das individuelle Anbieten seines Films oder seiner Musik über das Internet zu verbieten. Hat der Berechtigte allerdings sein Werk selbst in das Internet eingespiesen oder wurde es mit seinem Wissen und Willen eingespiesen, besteht eine Vermutung, dass er in diesem Rahmen in die Wahrnehmbarmachung seines Werkes eingewilligt hat (vgl. dazu auch Ziff. 8).
- *das Senderecht (Art. 10 Abs. 2 Bst. d URG);* d.h. das Recht, das Werk durch Radio, Fernsehen oder ähnliche Einrichtungen zu senden. Hier stellt sich die Frage, ob das Übermitteln eines Werkes auf einer Datenautobahn dem 'senden' gleichgesetzt werden kann. Mit dem Begriff Senden ist die

gleichzeitige Übermittlung eines Werkes an eine unbeschränkte und unbestimmte Zahl von Personen gemeint. Im Internet ist zumindest das Erfordernis der Gleichzeitigkeit nicht gegeben, da hier die Werke durch die Nutzer individuell und interaktiv abgerufen werden können. Somit dürfte das *Sende-* wie auch *das Weitersenderecht (Art. 10 Abs. 2 Bst. e URG;* d.h. das Recht, gesendete Werke mit Hilfe von technischen Einrichtungen, deren Träger nicht das ursprüngliche Sendeunternehmen ist, weiterzusenden) im Rahmen der Übertragung über Internet kaum von grossem Interesse sein.

- *das Vermietrecht (Art. 13 URG):* Mit Ausnahme der Computerprogramme ist es zulässig, rechtmässig erworbene Werkexemplare zu vermieten. Derjenige, der Werkexemplare vermietet oder sonstwie gegen Entgelt zur Verfügung stellt, muss dem Urheber hiefür allerdings eine Entschädigung bezahlen. Dagegen hat der Urheber eines *Computerprogrammes* das ausschliessliche Recht, das Programm zu vermieten. Computerprogramme dürfen somit *ohne die ausdrückliche Einwilligung des Rechtsinhabers* nicht gegen Entgelt Dritten zur Verfügung gestellt werden. Das Einspeichern und Zurverfügungstellen eines Werkes auf einer Datenautobahn fällt allerdings in der Regel nicht unter den Tatbestand des Vermietens, da nicht die Übergabe von (Original)-Werkexemplaren erfolgt.

- *das Änderungsrecht sowie das Recht zu bestimmen, ob das Werk zur Schaffung eines Werkes zweiter Hand verwendet oder in ein Sammelwerk aufgenommen werden darf (Art. 11 Abs. 1 URG).* Die Interaktivität des Internets erlaubt dem Benutzer nicht bloss passives konsumieren, sondern auch selektives Auswählen und die Vornahme von Änderungen. Aber auch hier sind ihm durch das Urheberrecht klare Grenzen gesetzt, darf doch ein Werk ohne die Einwilligung des Urhebers weder geändert noch für ein Werk zweiter Hand verwendet werden oder in eine Datenbank aufgenommen werden. Das ausschliessliche Recht des Urhebers auf Wiedergabe bezieht sich sowohl auf die unveränderte als auch auf die veränderte Wiedergabe des Werkes und schliesst insbesondere auch das Bearbeitungsrecht ein. Dies gilt insbesondere auch für das 'Sampeln' verschiedener Werke wie dies etwa bei Multimedia-Produkten häufig vorkommt. Aber selbst wenn eine vertragliche oder gesetzliche Befugnis zur Änderung eines Werkes oder zur Schaffung eines Werkes zweiter Hand vorliegt, kann sich der Urheber gegen jede Entstellung seines Werkes wehren, die sein Persönlichkeitsrecht verletzt (Art. 11 Abs. 2 URG).

9.2 Verwandte Schutzrechte

Ausübende Künstler haben grundsätzlich gegenüber dem Urheberrecht parallele Rechte, d.h. sie haben das Recht, ihre Darbietung wahrnehmbar zu machen. Daneben haben sie aber auch das Sende- und Weitersenderecht, das Aufnahme- und Vervielfältigungsrecht sowie das Verbreitungsrecht *(Art. 33 URG)*. Es gilt allerdings zu beachten, dass sie - im Gegensatz zu den Urhebern - nicht den Schutz einer Generalklausel haben, die ihnen ein allgemeines ausschliessliches Recht einräumt. Bei der Verwendung im Handel erhältlicher Ton- oder Tonbildträger zum Zwecke der Sendung, der Weitersendung, des öffentlichen Empfangs oder der Aufführung haben sie Anspruch auf eine Vergütung *(Art. 35 URG)*.

10. Schutzausnahmen

Die folgenden für die Datenautobahnen relevanten Schutzausnahmen erlauben ausnahmsweise den Gebrauch urheberrechtlich geschützter Werke durch den Informationsnachfrager. Das ausschliessliche Recht des Urhebers wird durch diese Bestimmungen somit eingeschränkt. Der Access Provider kann diese Schutzausnahmen für sich nicht beanspruchen, da er ja nicht eigentlicher Nutzer von urheberrechtlich geschützten Werken, sondern vielmehr ein Vermittler ist.

10.1. Eigengebrauch

Das URG erlaubt die Verwendung *veröffentlichter Werke* zum Eigengebrauch (Art. 19 URG). Darunter fällt beispielsweise nebst der Werkverwendung *im persönlichen Bereich* d.h. unter Verwandten und Freunden (Art. 19 Abs. 1 Bst. a URG) auch *jede Werkverwendung des Lehrers für den Unterricht in der Klasse* (Art. 19 Abs. 1 Bst. b URG) sowie das auszugsweise *Vervielfältigen* von Werken in Betrieben, öffentlichen Verwaltungen, Instituten, Kommissionen und ähnlichen Einrichtungen *für die interne Information oder Dokumentation* (Art. 19 Abs. 1 Bst. c URG).

Während sich die Bst. a und b *auf jegliche Arten der Werkverwendung* beziehen, gilt Bst. c nur für das Vervielfältigen. Das Abrufen eines Werkes oder auch das Weiterleiten über das Internet an einen Freund (unter der Voraussetzung, dass ein Dritter keinen Zugriff hat) sowie die Herstellung digitaler Kopien sind somit im oben erwähnten persönlichen Rahmen erlaubt. Im Rahmen dieser privaten Nutzung ist somit auch das 'downloading' von on line verfügbaren Daten (mit Ausnahme einer allfälligen Vergütung für das Trägermaterial) frei.

In den Fällen der erlaubten Vervielfältigung geschützter Werke nach Bst. b und c steht den Rechtsinhabern ein *Vergütungsanspruch* zu, der ausschliesslich von den zuständigen Verwertungsgesellschaften (vgl. Ziff. 11.1) geltend zu machen ist. Wie dieser Vergütungsanspruch bei der Verwendung von Werken auf der

Datenautobahn wahrzunehmen ist, ist noch nicht gelöst. Im Ausland wurde deshalb gar vorgeschlagen, den Eigengebrauch für digitale Verwendungsarten nicht mehr zuzulassen.

Es ist auch darauf hinzuweisen, dass die vollständige oder weitgehend vollständige Vervielfältigung von im Handel erhältlicher Werkexemplare nur für den privaten Kreis (Verwandte und Freunde) zulässig ist (Art. 19 Abs. 3 URG). Für Schulzwecke oder für die interne Information oder Dokumentation eines Unternehmens dürfen somit nicht ganze Werke aus Datenbanken kopiert werden.

10.2. Computerprogramme

Computerprogramme dürfen auch für den Eigengebrauch nicht kopiert werden (Art. 19 Abs. 4 URG), sondern vom rechtmässigen Benutzer nur insoweit verwendet als dies für den bestimmungsgemässen Gebrauch des Programms, zu dem das Laden, Anzeigen, Übertragen oder Speichern gehören, notwendig ist.

Allerdings erlaubt das URG die *Entschlüsselung des Programmcodes*, sofern dies zur Herstellung der Interoperabilität, d.h. zur Verknüpfung mit einem anderen unabhängig geschaffenen Programm erforderlich ist. Dies aber nur unter der Voraussetzung, dass diese Informationen nicht ohne weiteres zugänglich sind und die normale Auswertung des Programmes nicht beeinträchtigt wird (Art. 21 URG i.V.m. Art. 17 URV).

10.3. Zitatrecht

Es ist erlaubt, *ein veröffentlichtes Werk* in einem eigenen Werk zu zitieren*, wenn das Zitat zur Erläuterung, als Hinweis oder zur Veranschaulichung dient und der Umfang durch diesen Zweck gerechtfertigt ist.* Das Zitat ist als solches zu kennzeichnen und die Quelle ist deutlich anzugeben (Art. 25 URG).

10.4. Berichterstattung über aktuelle Ereignisse

Zum Zwecke der Information dürfen über aktuelle Fragen kurze Ausschnitte aus Presseartikeln sowie aus Radio- und Fernsehberichten vervielfältigt oder weiterverbreitet werden; der Ausschnitt und die Quelle sind anzugeben (Art. 28 URG).

11. Verwaltung der Urheber- und der verwandten Schutzrechte

11.1. Die Regelung der kollektiven Verwertung

Zur gegenwärtigen Situation ist festzuhalten, dass nach Art. 40 Abs. 1 URG nur einzelne Verwertungsbereiche der Bundesaufsicht unterliegen. So können beispielsweise die *Vergütungsansprüche* im Bereich der Massennutzungen (z.B. Kopieren zum Eigengebrauch, Vermieten von Werkexemplaren, Verwendung von Ton- und Tonbildträgern zu Aufführungs- und Sendezwecken) nur von zugelassenen Verwertungsgesellschaften geltend gemacht werden. Bis heute gibt es fünf solcher Gesellschaften in der Schweiz (SUISA für Werke der Musik; SUISSIMAGE für visuelle und audiovisuelle Werke; PROLITTERIS für Werke der Literatur, der Fotografie und der bildenden Kunst; Société suisse des auteurs für wort- und musikdramatische Rechte sowie SWISSPERFORM für die verwandten Schutzrechte. Dagegen ist die persönliche Verwertung ausschliesslicher Rechte durch den Urheber nicht der Bundesaufsicht unterstellt.

Im Hinblick auf die Datenautobahnen lässt sich gegenwärtig noch nicht abschliessend feststellen, welche Nutzungen unter die Bundesaufsicht fallen und welche nicht. Da aber der Urheber die Verwendung seines Werkes auf dem Internet kaum kontrollieren kann, dürfte in vielen Fällen eine zentrale Verwaltung der Rechte sowohl zugunsten der Urheber wie auch der Nutzer sein. Die Verwertungsgesellschaften sind deshalb bemüht, sich bereits jetzt möglichst viele Rechte im Zusammenhang mit diesen neuen Nutzungsformen im Rahmen ihrer Verträge mit den Urhebern abtreten zu lassen. Es liegt allerdings an den Urhebern zu entscheiden, ob sie auch das für Internet und Multimedia wesentliche Bearbeitungsrecht einräumen wollen.

In der Schweiz werden aber nicht nur inländische Werke und Darbietungen genutzt. Deshalb lassen sich die schweizerischen Verwertungsgesellschaften mittels Gegenseitigkeitsverträgen mit ähnlichen Organisationen im Ausland die Befugnis einräumen, die Rechte ausländischer Urheber und Rechtsinhaber in der Schweiz wahrzunehmen. Ziel dieser Verträge ist es, den Nutzern ein möglichst vollständiges und weltweites Repertoire anbieten zu können. Während dieses Ziel von der SUISA in ihrem Bereich (Werke der Musik) nahezu erreicht wird, gibt es bei den restlichen Gesellschaften noch teilweise erhebliche Lücken.

Bereits wurde auch die Einführung einer gesetzlichen Lizenz für Werke in digitalisierter Form vorgeschlagen. Dies würde bedeuten, dass der Rechtsinhaber die Verwendung seines Werkes im Internet nicht mehr verbieten könnte. Allerdings würde ihm ein entsprechender Vergütungsanspruch verbleiben. Dies könnte letztlich zu einem sogenannten 'pay per use'-System führen, was für den Nutzer - im Gegensatz zu Pauschalabgaben - den Vorteil hätte, dass er nur für das bezahlen muss, was er effektiv nutzt.

12. Rechtsschutz

Wer ohne Bewilligung der Berechtigten und ohne dass er sich auf eine Ausnahmeregelung stützen kann, Urheberrechte oder verwandte Schutzrechte nutzt, kann zivil- oder strafrechtlich belangt werden (Art. 61ff. URG). Auf zivilrechtlicher Ebene steht dem Urheber bzw. dem Rechtsinhaber ein umfangreiches zivilrechtliches Schutzinstrumentarium (Feststellungs- und Leistungsklage, vorsorgliche Massnahmen und Veröffentlichung des Urteils) zur Verfügung. Nebst einem Benutzungsverbot kann hier für die bereits erfolgte Nutzung auch Schadenersatz verlangt werden. Strafrechtlich gesehen handelt es sich bei Urheberrechtsverletzungen beziehungsweise bei der Missachtung von verwandten Schutzrechten um Vorsatzdelikte, die grundsätzlich auf Antrag zu verfolgen sind. Die Strafbestimmungen sehen in diesem Fall Gefängnis bis zu einem Jahr oder Busse bis zu 40'000 Franken vor. Bei gewerbsmässigem Vorgehen sind sie von Amtes wegen zu verfolgen (Art. 63 bzw. 69 URG) und es droht eine Gefängnisstrafe bis zu 3 Jahren und eine Busse bis zu 100'000 Franken.

13. Schlussfolgerungen

Es ist wohl kaum zu bestreiten, dass heutzutage über das Internet vielfach geschützte Werke ohne Beachtung der Urheberrechte und der verwandten Schutzrechte genutzt werden. Gründe hierfür mögen sein, dass es einerseits für die Informationsanbieter äusserst schwierig ist, die Rechte für die weltweite On-line-Verbreitung geschützter Werke und Leistungen zu erwerben, andererseits ist es aber auch dem Rechtsinhaber - mindestens solange ihm die hiezu nötigen technischen Hilfsmittel fehlen - nicht möglich, die Verwendung seiner Werke auf dem Internet zu kontrollieren. Es gilt daher, mit geeigneten Massnahmen der Auffassung entgegenzuwirken, dass im Internet angebotene Werke gemeinfrei sind und somit von jedermann ohne entsprechende Einwilligung oder Entschädigung verwendet oder gar verändert werden dürfen.

Dies gilt umsomehr als mit dem geltenden Urheberrechtsgesetz ein geeignetes Instrumentarium zur Verfügung steht, um die Rechte der Urheber und weiterer Rechtsinhaber auch in diesem veränderten Umfeld zu gewährleisten.

3. Mai 1996 / ST