La surveillance policière et judiciaire des communications par Internet

Laurent Moreillon
Professeur de droit pénal à l'Université de Lausanne

Sandra Blank
Lic.iur., assistante de recherche à l'Université de Lausanne

I. Introduction

La surveillance policière et judiciaire des messages électroniques est un domaine nouveau et en plein essor. L'idée est de donner aux autorités de poursuite des moyens inédits d'interception permettant la récolte d'indices et de preuves dans la poursuite d'infractions. Le domaine d'investigation ne cesse de s'étendre: criminalité informatique (art. 143 ss CP), escroquerie commise sur Internet (art. 146 CP), blanchiment d'argent (art. 305bis CP), criminalité économique (organisation criminelle, actes de corruption au sens des art. 260bis et 322ter ss CP) financement du terrorisme (art. 260^{quinquies} CP), etc.

Les conditions de la surveillance doivent cependant être réglementées. Dans un Etat de droit, certains mécanismes de prévention policière ne peuvent être acceptés. Ainsi, l'enquêteur ne peut en principe utiliser la technique du cheval de Troie pour confondre un suspect. Plus particulièrement, il ne saurait, à l'aide d'un logiciel spécifique, s'infiltrer discrètement dans la machine d'un tiers pour y lire les informations et les transmettre à l'autorité de poursuite[1]. En droit de procédure pénale suisse, les codes, fédéral ou cantonaux (PPF ou CPP), n'autorisent pas de tels procédés. Faute de base légale expresse, l'introduction clandestine d'un corps étranger dans une machine à distance, dont le contenu informatique a été spécialement protégé, n'est pas admissible[2]. Il y va de l'application des art. 143 et 143bis CP. On pourrait certes envisager l'exception tirée de l'art. 32 CP (devoir de fonction ou de profession). Encore faudrait-il que l'acte soit ordonné par la loi ou qu'il soit accompli selon les formes légales par le fonctionnaire de police ou le magistrat. En effet, selon la jurisprudence, le devoir de fonction doit avoir son fondement dans l'ordre légal, en principe dans une loi ou une ordonnance, fédérale ou cantonale, de droit privé ou de droit administratif[3]. De même, son étendue dépend du contexte juridique et en particulier du droit cantonal[4]. Enfin, à supposer que l'acte soit expressément autorisé par la loi ou qu'à défaut, il s'inscrive dans la clause générale de police, il doit rester proportionné au but visé[5]. On envisage mal l'application de cette disposition, sauf dans des situations exceptionnelles (surveillance d'activités terroristes, à la suite de soupçons concrets et sérieux).

On pourrait également imaginer d'autres formes d'intrusion policière. Ainsi, celle de *«l'espion clavier logique»*[6], ou *Keylogger*. Ce système permet d'enregistrer à couvert

1 Exemple fourni par JEAN TRECCANI, Interceptions électroniques, in Plus de sécurité, moins de liberté, les techniques d'investigation et de preuve en question, Zurich et Coire 2003, p. 217 ss, spécialement 225 s.
2 TRECCANI (n. 1), p. 226 s.
3 ATF 95 IV 5, JdT 1968 IV 38
4 ATF 115 IV 162, JdT 1991 IV 66
5 ATF 107 IV 84, JdT 1982 IV 157
6 Exemple donné par TRECCANI (n. 1), p. 234 s.

***Zusammenfassung**: Die neuen Kommunikationstechnologien haben zu einer Zunahme der Internetkriminalität geführt (Geldwäscherei, Betrug, Finanzierung des Terrorismus, Datenkriminalität). Die internationale Dimension der Problematik zeigt die Lücken der nationalen Verfahrensregeln in Bezug auf die Herausgabe und Siegelung der inkriminierten Daten. Die Verfolgung dieser Art von Kriminalität verlangt eine internationale, effiziente und gegenseitige Rechtshilfe. Einerseits müssen die Staaten ihre nationalen Gesetze harmonisieren. Auf der anderen Seite gilt es die Konvention über die Cyberkriminalität, welche die Grundlagen einer Kooperation der Justizbehörden im speziellen Bereich der neuen Technologien aufstellt, zu ratifizieren. Der Bereich der Cyberkriminalität hat sich wegen dem Kampf gegen den Terrorismus ausgeweitet.*

***Résumé**: Les nouvelles technologies de la communication ont engendré une augmentation des infractions commises sur Internet (blanchiment, escroquerie, financement du terrorisme, ainsi que les infractions électroniques). Leur caractère transfrontalier met en évidence les lacunes des règles de procédures nationales s'agissant de l'interception et de la conservation des données litigieuses. Le respect des garanties de procédure ne permet pas n'importe quelle intervention policière. Dépister l'infraction dans le cadre de ce type de criminalité suppose la mise en œuvre d'une entraide judiciaire internationale efficace. En premier lieu, il appartient aux Etats d'harmoniser leurs législations nationales. En second lieu, de ratifier la Convention contre la cybercriminalité, qui met en place les bases d'une coopération judiciaire spécifique aux nouvelles technologies. Le domaine est varié, à l'image de la lutte contre le terrorisme.*

toutes les frappes de clavier. L'information est alors stockée avant d'être copiée et lue par l'intrus. Cette installation suppose un accès direct à la machine à surveiller. Il y aura en principe infraction à l'art. 143bis CP, à moins que l'intrus n'ait profité de l'inattention de l'ayant-droit ou des failles de son système pour s'introduire dans son bureau et placer l'appareil. Tout au plus peut-on y voir une infraction à la LPD s'agissant de données informatiques copiées[7] ou à l'art. 179novies CP, s'il y a eu soustraction d'un fichier de données personnelles sensibles.

On pourrait enfin concevoir l'espion clavier/matériel. Dans cette hypothèse, l'espion, installé à nouveau sur le clavier, adresse simultanément l'information par émetteur en temps réel à l'observateur[8]. Y a-t-il infraction à l'art.143bis CP? Il n'y a à proprement parler pas d'introduction dans la machine car, en général, l'espion est placé entre le clavier et l'unité centrale informatique. L'appareil se borne ainsi à enregistrer les frappes sur le clavier. Mais l'on pourrait rétorquer que la notion de système informatique englobe tous les éléments actifs et mobiliers de la structure pour permettre l'information[9].

On voit à quel point il est indispensable de réglementer de telles questions aussi délicates. Avant de dégager les quelques réponses données par le droit suisse, il convient d'examiner quelques solutions de droit étranger, qu'il s'agisse du droit du Conseil de l'Europe, du droit américain ou du droit anglo-saxon.

II. Droit étranger

1. Conseil de l'Europe

Le texte principal est la Convention sur la cybercriminalité (STE 185), ratifiée par cinq Etats membres à l'heure actuelle[10], texte qui entre en vigueur pour eux le 1er juillet 2004. La Suisse l'a également signé le 23 novembre 2001. Elle ne l'a cependant pas encore ratifié[11]. Cette convention institue le principe de l'entraide facilitée la plus large possible (art. 23). Elle permet d'autre part l'information spontanée (art. 26) et se veut un complément sur ce point de l'art. 11 du deuxième protocole additionnel à la convention de 1959 du 8 novembre 2001[12], signé par la Suisse le 15 février 2002, mais non encore ratifié.

Dans le domaine de la surveillance électronique, plusieurs dispositions topiques règlent la matière.

A. Conservation rapide de données informatiques stockées

L'idée, exprimée à l'art. 16 de la Convention sur la cybercriminalité, est que chaque Etat adopte les mesures législatives nécessaires pour permettre à ses autorités compétentes la conservation rapide de données électroniques spécifiques, y compris les données relatives au trafic. Les mesures s'appliquent ici aux données *stockées*, soit à celles qui ont déjà été collectées et archivées par le détenteur de données, tel le fournisseur de services[13]. Elles ne s'apparentent pas à la collecte en *temps réel*. Cela présuppose que les données informatiques existent déjà et/ou qu'elles sont en cours de stockage.

L'art. 16 ch. 2 permet aux Etats membres d'adapter leur droit national et d'introduire le système de l'*injonction judiciaire*. Il s'agit en effet d'assurer la conservation des données stockées. Concrètement, le juge national notifiera son ordonnance au fournisseur de services. Le magistrat pourrait certes recourir à la technique traditionnelle de la *perquisition*. Toutefois, en présence d'opérateurs de taille, la technique de l'injonction apparaît bien plus efficace. La mesure, ordonnée à titre provisionnel, portera en principe sur une durée d'au moins 90 jours. Elle pourra être renouvelée. Quant au secret (privé, professionnel, d'affaires), il sera sauvegardé, car les données ne seront pas spontanément portées à la

7 Sur ces questions, TRECCANI (n. 1), p. 234 s.
8 Exemple donné par TRECCANI (n. 1), p. 235 s.
9 TRECCANI (n. 1), p. 235 s.
10 Ratification par l'Albanie le 20 juin 2002, la Croatie le 17 octobre 2002, l'Estonie le 12 mai 2003, la Hongrie le 4 décembre 2003, la Lituanie le 18 mars 2004.
11 La ratification n'est, pour le moment, pas à l'ordre du jour du DFJP.
12 STE 182.
13 Voir sur ces questions: rapport explicatif Convention cybercriminalité, ad art. 16-17, n° 149.

connaissance des autorités pénales de poursuites. Une fois conservées, elles ne pourront être communiquées au juge pénal qu'après injonction de les lui divulguer[14].

L'investigation policière ou judiciaire portera sur tout type de données informatiques stockées, à l'image des dossiers commerciaux, médicaux ou personnels[15]. L'idée est de s'assurer la conservation de toutes données qui, au sein de l'entreprise suspectée, seraient susceptibles de disparaître. Il est donc nécessaire de les faire sécuriser par un opérateur. Concrètement, les données stockées pourront demeurer chez l'intéressé, mais sécurisées ou gelées, ou, à défaut, être stockées ailleurs et sous son contrôle[16].

L'enquêteur, tout comme le provider, sont soumis à une stricte obligation de confidentialité. La règle découle de l'article 16 ch. 3. L'idée est que le suspect ne doit pas avoir connaissance des données gelées ou copiées. Il y a donc à la charge de l'opérateur une double obligation, à savoir la conservation des données (sécurisation des données) et la confidentialité des actes d'instruction (secret de l'opération)[17].

Enfin, les mesures d'investigation ne sont licites qu'à condition qu'elles s'inscrivent dans le cadre d'une procédure de nature pénale respectant les droits fondamentaux des parties. La règle est posée à l'article 16 ch. 4 de la Convention, qui renvoie aux articles 14 et 15 du même document.

B. Conservation et divulgation partielle rapide de données relatives au trafic

La matière est réglée à l'art. 17 de la Convention. Cette disposition prévoit la divulgation rapide de certaines données relatives au trafic, aux fins d'identification des autres fournisseurs de services ayant participé à la transmission de communications suspectes. L'obtention de données relatives au trafic concernant des communications antérieures peut s'avérer essentielle pour déterminer la source ou la destination de ces communications. Ces informations sont capitales pour identifier les personnes qui, par exemple, on distribué de la pornographie infantile, ont diffusé de fausses déclarations dans le cadre d'actes d'escroquerie, ont propagé des virus informatiques ou encore ont tenté d'accéder à des systèmes informatiques[18].

Ces données ne sont disponibles que très peu de temps, la législation nationale pouvant parfois interdire un stockage de longue durée. D'où la nécessité de garantir leur conservation[19]. S'il existe plusieurs fournisseurs qui ont participé à la transmission d'une communication, chacun de ceux-ci pourrait ne posséder qu'une seule partie des données, soit une seule pièce du puzzle. Il importe que chaque partie de stockage puisse être examinée, afin d'identifier les sources ou la destination[20].

Bien souvent, l'autorité ne connaît pas le nombre de fournisseurs concernés. L'article 17 de la Convention impose aux fournisseurs, qui reçoivent l'injonction de conservation, de divulguer rapidement aux autorités compétentes une quantité suffisante de données relatives au trafic pour permettre l'identification de tous les autres fournisseurs de services ainsi que la voie par laquelle la communication a été transmise[21].

C. Injonction de produire

Selon l'art. 18 de la Convention, chaque Etat doit prendre les mesures nécessaires pour contraindre une personne présente sur son territoire, à fournir des données informatiques stockées, comme de contraindre un fournisseur de services sur son territoire de communiquer des données qu'il possède sur un de ses abonnés.

L'art. 18 ch. 1 lettre a précise que les données informatiques doivent être «*en possession*» ou «*sous contrôle*». Les notions demeurent vagues. La possession fait référence à la *détention* de matériel. L'expression «*sous son contrôle*» vise des situations dans lesquelles l'intéressé ne possède rien maté-

14 Rapport explicatif, remarque ad art. 16 et 17, n° 156.
15 Rapport explicatif, commentaire ad art. 16, n° 161.
16 Rapport explicatif, commentaire ad art. 16, n° 162.
17 Rapport explicatif, commentaire ad art. 16, n° 163.
18 Rapport explicatif, commentaire ad art. 17, n° 166.
19 Ibidem.
20 Rapport explicatif, remarque ad art. 17, n° 167.
21 Rapport explicatif, remarque ad. art. 17, n° 169.

riellement, mais contrôle librement ses données depuis le territoire qui a ordonné la production. Ainsi, si l'intéressé peut disposer, à distance, d'un stockage en ligne, il pourrait être tenu de donner suite à l'injonction, même si les données figurent physiquement à l'étranger. Plus délicate est cependant la question lorsque, pour y accéder, il faudrait encore, par une liaison du réseau, chercher à identifier l'information. Ici, la «*maîtrise*» de contrôle est plus délicate[22]. Sa portée dépendra du droit de procédure national de l'Etat sur lequel les investigations sont menées. S'agissant du suspect, on peut se demander si une telle injonction n'est pas contraire à l'article 6 CEDH qui prohibe l'auto-incrimination.

L'art. 18 ch. 3 règle la question des *données relatives aux abonnés*. Il faut entendre toute information, sous forme de données informatiques, ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de services, et permettant d'établir le type de service de communication utilisé, l'identité, l'adresse postale ou géographique, le numéro de téléphone de l'abonné et tout autre numéro d'accès, ainsi que les données concernant la facturation et le paiement; enfin toute information permettant d'identifier l'endroit où se trouvent les équipements de communication[23].

D. La perquisition et la saisie de données informatiques

L'art. 19 vise à moderniser et à harmoniser les législations internes concernant la perquisition et la saisie de données informatiques stockées aux fins de recueillir des preuves dans le cadre d'une enquête pénale[24]. L'art. 19 ch. 2 habilite les autorités chargées d'une enquête à étendre l'opération entreprise pour perquisitionner ou accéder par un moyen similaire à un autre système informatique ou une partie de celui-ci lorsqu'elles peuvent penser que les données recherchées sont stockées sur un autre système informatique.

Quant à l'art. 19 ch. 3, il permet la saisie de matériel et de tous les supports de stockage informatique. Ainsi, si la donnée stockée n'est pas copiable, le juge pourra saisir le support lui-même. Le juge peut également rendre les données inaccessibles, soit par codage, soit par blocage. De cette manière, la personne suspectée est privée temporairement de l'accès ou de l'usage, mais en retrouve pleine disposition à l'issue de l'enquête[25].

Enfin, l'art. 19 ch. 4 de la Convention instaure d'autres mesures coercitives pour faciliter la perquisition et la saisie des données stockées: en particulier, les enquêteurs peuvent obliger l'administrateur de la donnée informatique à apporter l'aide nécessaire pour permettre la perquisition et la saisie. Dans certains cas, il s'agira d'un simple mot de passe à découvrir[26].

E. Collecte en temps réel

A l'opposé, les art. 20 et 21 de la Convention prévoient la collecte en *temps réel* de données relatives au trafic et l'interception en temps réel de données relatives au contenu. Il s'agit à proprement parler d'interception de communications directes, en relation avec des réseaux de télécommunication classiques: câble, fibre optique, téléphonie mobile, inter-connexion hertzienne, réseau satellitaire etc. Ces dispositions s'appliquent à des communications spécifiques transmises au moyen d'un système informatique, la communication pouvant être transmise par le biais d'un réseau de télécommunication avant d'être reçue par un autre système informatique[27].

L'autorité de poursuite nationale pourrait-elle obliger le fournisseur de services à se doter de l'équipement technique lui permettant de collecter en temps réel les données relatives au trafic et d'enregistrer des informations sensibles? Selon l'art. 20 ch. 1er, l'acquéreur ou le provider n'a pas le devoir de mettre au point de nouveaux équipements, d'engager un expert ou de prêter coopération et assistance en toute circonstance. Toutefois, si le matériel du provider le permet, ce dernier doit prêter main forte. Ainsi, s'il possède notamment un logi-

22 Rapport explicatif, remarque ad art. 18, n° 173.
23 Rapport explicatif, ad art. 18, remarque n° 178.
24 Rapport explicatif, ad art. 19, remarque n° 184.
25 Rapport explicatif, ad art. 19, remarque n° 198.
26 Rapport explicatif, ad art. 19, remarque n° 202.
27 Rapport explicatif, ad art. 20-21, remarque n° 206.

ciel, même désactivé, il doit, sur requête du juge, le remettre sous tension pour prêter assistance[28].

L'art. 21 (interception de données relatives à leur contenu) donne la faculté au juge de déterminer si le contenu de la communication a un caractère illégal (menaces, actes d'intimidation, complots, actes terroristes, allégations frauduleuses, etc.). La mesure permet également d'apporter la preuve d'infractions passées ou futures (meurtres, délits économiques, trafic de stupéfiants, etc.).

2. Droit des pays anglo-saxons

A. Droit américain

En matière de surveillance des télécommunications, les règles figurent essentiellement dans deux textes principaux, le *USA Patriot Act*[29] et le *Homeland Security Act*[30]. Ce dernier a pour but de réorganiser les institutions et les méthodes de lutte contre les intérêts nationaux. Il a permis de créer un «*Department of Homeland Security*» qui est chargé de coordonner les actions.

Avant les attentats du 11 septembre et l'entrée en vigueur de ces deux lois, la surveillance était principalement régie par deux actes: Le *Federal Wiretap Act* de 1968[31], qui régit les conditions de la surveillance dans le cadre des infractions «classiques» commises sur le territoire américain, ainsi que le *Foreign Intelligence Surveillance Act* de 1978[32], qui instaure un régime particulier de la surveillance pour les investigations menées par les services secrets à l'encontre de mouvements étrangers.

Suite aux attentats du 11 septembre 2001, le gouvernement américain s'est doté de moyens encore plus efficaces pour lutter contre le terrorisme. Le Congrès a donc adopté plusieurs actes, notamment le *USA Patriot Act*, entré en vigueur le 26 octobre 2001. La loi modifie plusieurs autres législations, notamment les lois régissant le *Wiretap/stored communications*, les *Pen registers/trap and trace laws et le Foreign Intelligence Surveillance Act* de 1978. Elle permet ainsi la mise sur écoute de tout appareil de communication utilisé par toute personne, en rapport de près ou de loin avec un présumé acte terroriste; l'assignation (*Subpoena*) aux fins d'obtenir des déclarations concernant des données relatives au trafic, de la part notamment des providers.

La section 215 du *USA Patriot Act* facilite l'accès du gouvernement à des enregistrements stockés par des tiers concernant toute activité privée en relation avec le terrorisme ou toute autre activité clandestine. Cette disposition étend en conséquence les pouvoirs du FBI et lui permet d'exiger de n'importe quel tiers, y compris des médecins, des libraires, des bibliothécaires, des universités et des providers, tous renseignements dont ils disposent sur leurs clients: nom, adresse, localisation de l'appareil, heure, durée des appels, mode de paiement, numéro de carte de crédit etc. (section 210 en relation avec la section 215).

La section 225[33] du *Homeland and Security Act 2002*[34] complète le *USA Patriot Act 2001* en prévoyant que les providers pourront communiquer volontairement aux autorités le contenu des e-mails ou des messages instantanés des internautes lorsqu'ils jugent qu'il y a urgence. C'est à ces derniers d'apprécier le caractère d'urgence. Leur responsabilité ne sera pas engagée même s'ils divulguent des données personnelles en violant le secret des correspondances.

Pratiquement, à la suite des attentats du 11 septembre 2001, le droit américain confère des pouvoirs quasi illimités aux autorités de poursuite en cas de graves soupçons.

La section 215 du *USA Patriot Act 2001* n'est-elle pas en contradiction avec les 1er et 4ème amendements de la Constitution américaine, qui garantissent la liberté d'opinion et d'expression ainsi que l'inviolabilité des communications? Le gouvernement américain justifie la violation au motif que la loi autorise le Président à «utiliser la for-

28 Rapport explicatif, ad art. 20, remarque n° 221.
29 *USA Patriot Act*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, HR.3162.
30 *Homeland Security Act 2002*, H.R.5005.
31 *Federal Wiretap Act*, 18 U.S.C, 2516.
32 *Foreign Intelligence Surveillance Act*, Pub. L. No. 95- 511, 92 Stat. 1783.
33 Appelée aussi *Cyber Security Enhancement Act 2002*.
34 *Homeland Security Act 2002*, H.R.5005.

ce nécessaire et appropriée contre les Etats, organisations ou personnes qu'il considère avoir autorisé, commis ou aidé des attaques terroristes ou qui ont abrité de telles organisations ou personnes[35]».

La section 218 autorise le FBI à procéder à des recherches concrètes ou à une mise sous surveillance d'un citoyen américain pour détecter des preuves de la commission d'un crime, sans avoir à prouver une «cause probable», passée actuelle ou future, d'actes punissables. Ce type de surveillance pourrait semble-t-il servir à recueillir des preuves dans le cadre d'infractions «classiques» commises sur le territoire américain[36].

La section 214 permet de collecter des données d'origine stockées. Avant l'entrée en vigueur du *USA Patriot Act 2001*, le mandat émis pour la surveillance des données relatives au trafic était valable uniquement dans la juridiction du juge qui l'avait accordé. La loi prévoit dorénavant que le mandat est valable sur tout le territoire américain quel que soit le lieu d'émission.

La section 217 autorise les autorités fédérales américaines à intercepter des communications si le détenteur, surveillant ou gérant des informations contenues dans l'ordinateur donne son accord. En cas d'urgence, et s'il y a risque d'atteinte à la vie ou à l'intégrité corporelle, ou s'il s'agit d'atteintes à la sécurité nationale, les autorités peuvent procéder à la mise sous écoute sans la moindre injonction d'un tribunal. Cette mesure peut être prise par la FISA (*Foreign Intelligence Surveillance service*). Concrètement, un risque de détournement ou d'attentat suffit.[37]

B. Droit anglais

Le Royaume-Uni ne disposait pas de législation suffisante en matière de surveillance. A plusieurs reprises, des mesures d'interception ont été contestées devant la Cour européenne des droits de l'homme pour violation de la vie privée (art. 8 CEDH)[38]. Une première loi est entrée en vigueur en 1985: *Interception of communication Act 1985*. Elle n'a pourtant pas suffi à pallier aux lacunes existantes en matière de surveillance.

En 1998, l'Angleterre a adopté le *Human Rights Act 1998*, ce qui lui a permis d'intégrer enfin dans son système les dispositions de la CEDH. Elle s'est en outre conformée à la Directive de l'Union européenne concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[39]. Ces dispositions n'ont cependant pas suffit à régler le mécanisme de la surveillance informatique.

La Grande-Bretagne a donc adopté le RIPA, *Regulation of Investigatory powers Act 2000*, qui règle l'accès aux données de communication par les autorités publiques.[40] En principe, toute personne qui intercepte volontairement et sans autorisation légale une communication en cours de transmission sur un réseau de télécommunication public commet une infraction (Section 1(1)). Il en va de même de celui qui intervient sur une communication privée (Section 1(2)). La loi contient deux exceptions (Section 6).

L'interception n'est pas interdite (Section 1(3)) si elle est commise ou permise par une personne qui, de par sa fonction a le droit de contrôler ou d'accéder au système de télécommunication privé (Section 1(2) RIPA). De même, le comportement est licite lorsque la surveillance est autorisée légalement, soit lorsque les deux parties y ont consenti (Section 3(1)), lorsque l'autorité judiciaire a ordonné l'interception (Section 3(2)), ou qu'elle s'inscrit dans le cadre de mesures d'entraide judiciaire pénale avec l'étranger (Section 4(1)). Une surveillance

35 Arrêt de la Cour fédérale de Richmond du 8 janvier 2003, non encore publié, mais cité par ANTOINE J. BULLIER, Une Cour d'appel fédérale soutient le point de vue de l'exécutif américain dans une affaire concernant un ancien détenu de Guantanamo, Droit pénal-Editions du Juris-Classeur, juin 2003, p.6 ss.

36 American Civil Liberties Union, Surveillance under the *USA Patriot Act*, http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12263&=206.

37 Sur ces questions, section 201 *Federal Wiretap Act*, 18 USC, 2510-2522.

38 Malone v. UK (1984) 7 E.H.R.R. 14 et Halford v. UK (1997) 24 E.H.R.R. 523.

39 Directive 97/66/CE, L 24/1 30.1.98.

40 YAMAN AKDENIZ, NICK TAYLOR, CLIVE WALKER, Regulation of Investigatory Powers Act 2002 (1): BigBrother.gov.uk: State surveillance in the age of information and rights, Crim.L.R. (2001), p. 73ss. PETER MIRFIELD, Regulation of Investigatory Powers Act 2000 (2): Evenditial Aspects, Crim.L.R. (2001), p. 91ss.

ne pourra toutefois être mise en place que dans la mesure où un comportement suspect a été commis sur le territoire anglais. Cela suppose que la communication puisse être interceptée sur un système de transmission de données localisées sur ce territoire. A défaut, le droit anglais s'applique dans la mesure où le message était délivré à un correspondant situé sur le territoire anglais (Section 2 (4)).

De plus, selon le *Regulation of Investigatory Powers Order (Maintenance of Interception Capability) 2002*, entré en vigueur le premier août 2002[41]; les opérateurs britanniques ont l'obligation d'intercepter les communications électroniques et de les stocker (e-mails, télécopies/fax, informations concernant les sites web visités). Pratiquement, dès que le fournisseur d'accès reçoit une injonction, il disposera d'un délai de 24 heures pour initier la surveillance de la personne suspectée. Il devra en outre veiller à communiquer l'information en temps réel.

Il est toutefois facile de contourner une telle surveillance. En effet, les fournisseurs d'accès disposant de moins de 10'000 abonnés n'ont pas l'obligation de conserver de telles données. Il en va de même des intermédiaires de télécommunication travaillant avec des institutions financières, telles que les banques, les sociétés d'assurance et les établissements de placement. Pour échapper à toute surveillance, il suffit donc à l'abonné de choisir un de ces deux types de réseaux «protégés»[42].

III. La surveillance des communications électroniques en droit suisse

1. Introduction

En Suisse, comme à l'étranger, le juge pénal est de plus en plus amené à ordonner des mesures de surveillance pour *dépister* l'infraction. Bien souvent, la criminalité est *transfrontière*. Sur ce point, la coopération judiciaire transfrontalière ne se limite pas à l'application de la loi fédérale sur l'entraide internationale en matière pénale[43], ou au concordat suisse intercantonal d'entraide judiciaire[44]. D'autres lois trouvent application. Tel est le cas de la loi fédérale sur la surveillance de la correspondance par poste et télécommunications[45]. Plusieurs questions demeurent en suspens.

- Quelle est la loi de procédure applicable (droit cantonal, droit fédéral)?
- S'agissant de délits informatiques, sur quoi peut porter la surveillance informatique?

2. Loi fédérale sur la surveillance de la correspondance par poste et télécommunications

Depuis le 1er janvier 2002 est en vigueur en Suisse la loi fédérale sur la surveillance de la correspondance par poste et télécommunications (ci-après LSCPT)[46]. Cette loi s'applique aussi bien à la surveillance de la correspondance par poste que par télécommunications (art. 1er al. 1 LSCPT). Elle s'applique indifféremment à toute procédure, qu'il s'agisse d'une enquête fédérale, cantonale ou d'une demande de coopération judiciaire au sens de l'art. 18 a EIMP.

La loi s'applique à toute organisation étatique, à tout organisme soumis à concession ou à obligation d'annoncer qui fournit des services postaux ou de télécommunications, ainsi qu'à tout fournisseur d'accès Internet. Elle remplace les dispositions correspondantes des lois cantonales de procédure et harmonise les conditions de surveillance dans ce domaine. Il en découle que le droit cantonal est subsidiaire dès le 1er janvier 2002, dans la mesure où il ne sert plus qu'à désigner l'autorité habilitée à autoriser la surveillance.

La loi est complétée par une ordonnance du 30 octobre 2001 sur la surveillance de la correspondance par poste et télécommunications (ci-après OSCPT)[47]. Ce texte définit les types de surveillance qui peuvent être ordonnés, les modalités de l'exécution et les obligations des fournisseurs de services. Elle précise les dispositions spécifiques relatives à la surveillance dans les domaines de la téléphonie mobile et d'Internet. Ac-

41 Statutory Instrument 2002 No. 1931.
42 DAVID ORMEROD et SIMON MCKAY, Telephone intercepts and their admissibility, Crim.L.R (2004), p. 15ss.
43 RS 351.1.
44 RS 351.71
45 RS 780.1.
46 RS 780.1.
47 RS 780.11.

tuellement, la surveillance des accès Internet se limite aux fonctions du seul courrier électronique[48].

Les conditions de la surveillance sont posées à l'art. 3 de la loi. Quatre éléments de base doivent être remplis:

- il doit exister de graves soupçons reposant sur des faits déterminés;
- la gravité de l'acte justifie la surveillance;
- les mesures d'investigation sont demeurées jusqu'à présent lettre morte ou seraient excessivement difficiles;
- la surveillance ne peut s'exercer que dans le cadre d'infractions strictement énumérées (art. 3 al. 2 LSCPT).

La loi permet ainsi la surveillance et l'interception de communications dans la plupart des crimes et délits contre l'intégrité corporelle, contre le patrimoine, contre la liberté, contre l'intégrité sexuelle, contre le faux dans les titres ou contre la sécurité publique. La loi ajoute encore quelques infractions au code pénal militaire, à la loi fédérale sur le matériel de guerre[49], sur l'énergie atomique[50] ou sur la protection de l'environnement[51].

La LSCPT a été récemment modifiée[52]. L'art. 3 al. 2 LSCPT étend les mesures au financement du terrorisme (art. 260^{quinquies}), à la loi sur les épizooties, aux inondations, aux installations électriques, à la propagation de maladies de l'homme, à la contamination de l'eau potable ainsi qu'à d'autres menaces alarmant la population, à la provocation publique au crime, à la mise en danger de la sécurité au moyen d'armes, au génocide, enfin, à la corruption[53].

On peut se demander s'il était judicieux que le législateur établisse une liste exhaustive d'infractions justifiant la surveillance. D'une part, avec le développement de la criminalité, en particulier électronique, la liste devra constamment être adaptée. D'autre part, une liste aussi précise, qui limite l'investigation à des délits graves, pourrait amener l'autorité de poursuite à qualifier systématiquement de graves les faits reprochés à la personne suspectée pour justifier la mesure. D'un autre côté, si la loi se limitait à poser des conditions vagues de surveillance, l'on assisterait à une pléthore d'investigations pour des faits qui pourraient s'avérer futiles par la suite, avec des conséquences lourdes et dommageables pour la sphère privée du prévenu.
En l'état, la LSCPT permet déjà la surveillance et la communication d'informations détenues par un tiers (abonné). L'art. 4 LSCPT permet ce type de mesures lorsque la personne suspectée utilise le raccordement d'un tiers ou lorsqu'elle utilise une cabine téléphonique publique (art. 4 al. 1er et 2 LSCPT). Si le tiers abonné est un mandataire tenu au secret professionnel (avocat, notaire, médecin), la loi autorise la surveillance (art. 4 al. 3) dans la mesure où cette personne fait l'objet de graves soupçons et que la personne suspectée utilise l'adresse de ce tiers soumis au secret. En pareil cas, l'autorité de saisie procédera au tri des données, sous la surveillance d'une autorité judiciaire qui n'est pas saisie du dossier d'enquête[54].

La loi précise également le type de surveillance (art. 5). Notamment, elle permet de surveiller le contenu de la communication, ainsi que les données indiquant quand et avec quelle personne et au moyen de quel raccordement la personne suspectée a été en communication. La surveillance peut également porter sur le trafic, la fréquence ainsi que la facturation des communications sur une période rétroactive de six mois (art. 5 al. 1 lettre b).

Quant à la surveillance du téléphone et du courrier électronique, la loi distingue, à l'instar des dispositions topiques de la Convention sur la cybercriminalité, le *temps réel* et le *procédé rétroactif*.

La surveillance en *temps réel* (art. 16 lettres a à c OSCPT pour le téléphone et art. 24 lettres a à e OSCPT pour le e-mail) permet la lecture du message, la détermination et

48 Sur ce point, voir l'art. 24 OSCPT qui limite expressément la surveillance aux e-mails.
49 RS 514.52.
50 RS 732.0.
51 Voir les infractions énumérées à l'art. 3 ch. 2 LSCPT.
52 FF 2003, p. 2532, p. 2535.
53 Sur ces questions FF 2003, p. 2532 et 2535.
54 Sur ces questions, voir THOMAS HANSJAKOB, Les surveillances téléphoniques du point de vue de l'avocat, in Revue de l'Avocat 2003 n° 2, p. 47 ss.

le positionnement de l'appareil par rapport au relais et l'indication du moment durant lequel l'appareil est enclenché. Elle permet d'identifier les numéros d'appelés et d'appelants, le numéro SIM, la date, l'heure, la durée de la communication ainsi que les pièces jointes à un courrier e-mail.

Quant à la *surveillance rétroactive* (art. 7 lettre d) et 24 lettre f OSCPT), elle permet uniquement d'indiquer les numéros d'appelés et d'appelants, les numéros SIM, la position du détenteur de l'appareil et, s'agissant du courrier e-mail, le type de connexion, les données utilisées pour la procédure d'identification (login) ainsi que les noms des usagers.

En revanche, la loi ne permet pas la surveillance ou l'interception de messages déjà transmis et logés dans l'ordinateur du destinataire. Seule la perquisition (soumise aux dispositions générales du droit cantonal) permet de lire le contenu du message enregistré. A cet égard, le juge saisira à titre de mesure préventive l'ordinateur, le PC et, surtout, le disque dur de l'intéressé afin d'y lire a posteriori les inscriptions litigieuses.
La loi contient également des obligations à l'égard du fournisseur d'accès Internet. Celles-ci résultent notamment de l'art. 26 OSCPT. Chaque fournisseur d'accès Internet doit être en mesure d'exécuter le type de surveillance ordonné et de transmettre les informations, sur réquisition, à l'autorité pénale de poursuite compétente, en bref de conserver pendant une durée de six mois toute information[55].

IV. Compatibilité du droit suisse avec le droit international

En matière d'entraide judiciaire pénale, la Suisse a signé, notamment, la Convention européenne d'entraide judiciaire du 20 avril 1959 (CEEJ, STE n° 030)[56]. Cette convention est complétée par deux protocoles additionnels, le premier, du 17 mars 1978 (STE n° 099)[57] ainsi que le second du 8 novembre 2001 (STE n° 182)[58].

Les dispositions de la LSCPT sont-elles compatibles avec celles de la Convention sur la cybercriminalité? D'une façon générale, la réponse est affirmative, même si l'on doit déplorer qu'un stockage d'une durée maximale de six mois est insuffisant lorsqu'il s'agit de lutter contre de graves formes de criminalité informatique, à l'image du blanchiment d'argent ou de la corruption. Il faut rappeler d'autre part que l'OSCPT limite curieusement la surveillance aux seuls courriers e-mail. A cet égard, la Suisse ne paraît guère à jour, s'agissant de la surveillance de sites consultés. Cette situation est d'autant plus regrettable que la loi permet une surveillance bien plus large et qu'elle n'exclut pas la surveillance et le contrôle des sites Internet visités. A cet égard, le mécanisme de la perquisition et de la saisie prévu par le droit cantonal ne correspond guère aux dispositions topiques de la Convention sur la cybercriminalité. Souvent, l'auteur présumé de l'infraction aura fait disparaître physiquement l'ordinateur et, par voie de conséquence, le disque dur, rendant sans objet les mesures d'investigation.

La Convention sur la cybercriminalité prévoit en outre l'entraide concernant l'accès aux données stockées (art. 31), l'accès transfrontière des données stockées lorsqu'elles sont disponibles au public (art. 32), l'entrée dans la collecte en temps réel de données relatives au trafic (art. 33) ainsi que l'entraide en matière d'interception de données relatives au contenu (art. 34). Sur ce point, les dispositions de procédure (lois cantonales, lois fédérale sur l'entraide judiciaire en matière pénale et loi fédérale sur la procédure pénale) devront être adaptées en conséquence.

La Convention sur la cybercriminalité permet en particulier à un Etat requérant, alors même que l'entraide serait refusée dans l'Etat de commission de l'infraction, de prendre contact directement avec le détenteur de l'information stockée à l'étranger (art. 32)[59]. La convention permet ainsi à un Etat étranger de contourner les règles

55 Art. 5 al. 2 et 15 al. 3 LSCPT.
56 RS 0.351.1.
57 RS 0.351.21.
58 La Suisse est sur le point de ratifier ce protocole, voir FF 2003, p. 2878 ss.

usuelles de l'entraide judiciaire. En particulier, l'Etat requérant n'aura plus besoin de démontrer que les télécommunications suspectes se rapportent à des faits de nature pénale, qu'ils satisfont à la condition de la double incrimination, que l'entraide n'est pas exclue ou que les mesures requises ne violent pas les réserves émises par l'Etat requis (délits politiques, fiscaux, espionnage militaire, etc.). Sur ce point, la convention portera une atteinte sévère au principe de la souveraineté des Etats. La Suisse devra nécessairement modifier radicalement sa législation ou émettre des réserves sur ce point.

La Convention sur la cybercriminalité prévoit enfin la mise en place de réseaux de contacts fonctionnant en permanence (réseau 24/7, art. 35). Chaque partie désignera un office capable de donner à toute partie requérante et en tout temps des informations portant sur l'apport de conseils techniques, la conservation de données, l'apport d'informations à caractère juridique, la localisation et le recueil de preuves. En droit suisse, l'article 8 OSCPT prévoit la mise en place d'un centre de traitement de données informatiques. Ce service, qui n'est actuellement pas encore en fonction, est appelé à donner des renseignements 24 heures sur 24 heures aux autorités de poursuite pénale concernées. En particulier, il devrait recevoir et enregistrer des données sensibles, et les mettre à disposition des personnes chargées d'enquêtes pénales.

V. Conclusion

La LSCPT a permis à la Suisse d'anticiper les besoins en matière de surveillance pénale dans le domaine des nouvelles technologies. Toutefois, le chemin est loin d'être achevé. La ratification de la Convention sur la cybercriminalité nécessitera une modification en profondeur du droit suisse. Les récents attentats de Madrid pourraient inciter le législateur à modifier rapidement le droit de procédure fédéral, sans attendre l'entrée en vigueur le la convention. ■

59 Voir le texte de l'art. 32 Convention sur la cybercriminalité: «Une partie peut, sans l'autorisation d'une autre partie: a) accéder à des données informatiques stockées accessibles au public (sources ouvertes) quelle que soit la localisation géographique de ces données ou b) accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique».

Das Urheberrecht und Open Source Software

Mike J. Widmer
Dr. iur., Project Manager, Zürich

I. Einleitung

Was heute unter anderem Autos von Software unterscheidet ist, dass man die regelmässig anfallenden Servicearbeiten bei Fahrzeugen selber oder durch beliebige Dritte durchführen lassen kann, während diese bei handelsüblicher Software nur durch den Hersteller getätigt werden können. Anders als bei Fahrzeugen ist es nämlich bei Software einerseits technisch schwierig, einen Blick unter die Kühlerhaube zu werfen und andererseits rechtlich verboten[1], dies zu tun. Da der für Servicearbeiten benötigte Quellcode eines Computerprogramms beim Erwerb handelsüblicher Software nicht mitgeliefert wird, sieht man sich einem Auto mit verschlossener Kühlerhaube gegenüber. Diese im Fahrzeugmarkt wohl untolerierbare Situation hat sich aus diversen Gründen aber bei Computerprogrammen etabliert. Seit einiger Zeit nimmt die breite Öffentlichkeit allerdings mit zunehmendem Interesse zur Kenntnis, dass bereits seit gut zwei Jahrzehnten eine andere, nicht geschlossene Kategorie von Computerprogrammen besteht. Solche offenen Computerprogramme, welche heute in vielen Anwendungsbereichen echte Alternativen zu den herkömmlichen geschlossenen Systemen darstellen[2], werden mit dem Sammelbegriff «Open Source Software» bezeichnet.

Bei Open Source Software ist jedoch nicht nur der zur Verfügung gestellte und somit offene Quellcode ein Charakteristikum, sondern auch die rechtliche Komponente in der Gestalt der diversen Open Source Softwarelizenzen. Sie sind es, welche die Offenheit des Quellcodes erst garantieren und die Entwicklung von Open Source Software insgesamt ermöglichen, da sie dem Lizenznehmer im Gegensatz zu herkömmlichen Softwarelizenzen eine umfassende Verwendung des Computerprogramms und insbesondere des Quellcodes erlauben. Das rechtliche Fundament in Form von Open Source Softwarelizenzen stellt somit das zentrale Element jeder Open Source Software dar und ermöglicht erst die Entwicklung von Open Source Software. Diese mit einem Basar[3] verglichene Entwicklungsmethode setzt nämlich typischerweise voraus, dass eine Vielzahl von Personen Zugang zum Quellcode haben und in einem stetigen, kollaborativen Prozess die Software verbessern bzw. bearbeiten, vervielfältigen und verbreiten können.

II. Grundlagen

1. Open Source Software

Um das Phänomen Open Source Software aus rechtlicher Sicht betrachten zu können, ist es von Bedeutung, eine klare Begriffsbestimmung[4] vornehmen zu können. Dies wird einerseits dadurch erleichtert, dass der Begriff «Open Source Software» eine Wort-

***Résumé:** Dans beaucoup de domaines, le «open source» s'est révélé être une réelle solution de rechange face aux systèmes informatiques traditionnels. En tant que tel, il bénéficie de la protection du droit d'auteur, au même titre que d'autres programmes d'ordinateur. De par l'extrême difficulté à définir l'auteur d'un software «open source», une telle qualification ne dépend d'aucun ordre, ni d'aucune combinaison ou fréquence. Outre le risque qu'une modification future du droit des inventions porte sur les inventions en matière de software, il n'est pas exclu que les règles du droit d'auteur aient indirectement un effet négatif sur le développement du software «open source», en favorisant les mesures techniques de protection («digital rights management systems»). Il ne reste plus qu'à espérer que l'imminente révision du droit d'auteur tiendra aussi compte des préoccupations liées au software «open source».*

1 Ausnahmsweise und nur in beschränktem Masse lässt das Gesetz einen Blick in den Quellcode zu (vgl. Art. 21 URG).
2 So verwendet z.B. das Bundesgericht das Officepaket StarOffice, welches als Open Source Software unter dem Namen OpenOffice bekannt ist. Weiter finden sich insbesondere im Bereich des Internets diverse Open Source Computerprogramme, welche eine weitere Verbreitung als vergleichbare herkömmliche Computerprogramme aufweisen (BIND, Sendmail, Apache, PHP usw.).
3 Vgl. dazu RAYMOND E., The Cathedral and the Bazaar, 2000, http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/.
4 Eine ausführliche begriffliche Herleitung findet sich bei WIDMER M., Open Source Software - Urheberrechtliche Aspekte freier Software, Schriften zum Immaterialgüterrecht Bd. 72, Bern 2003, S. 4 ff.

***Zusammenfassung**: Open Source Software hat sich in vielen Bereichen zu einer echten Alternative gegenüber herkömmlichen Computersystemen entwickelt. Freie bzw. Open Source Software geniesst unter den gleichen Bedingungen wie andere Computerprogramme den Urheberrechtsschutz. Die Urheberschaft bei Open Source Software tritt in beliebiger Reihenfolge, Kombination und Häufigkeit auf, weshalb eine präzise Bestimmung der Urheber äusserst schwierig ausfallen kann. Neben der steten Gefahr, welche von einer möglichen Neuregelung im Patentrecht zugunsten von Softwarepatenten ausgeht, könnten sich auch die urheberrechtlichen Regelungen zugunsten technischer Schutzmassnahmen (Digital Rights Management) indirekt negativ auf die Entwicklung von Open Source Software auswirken. Es bleibt deshalb zu hoffen, dass in der anstehenden Revision des Urheberrechtsgesetztes auch die Bedenken der Open Source Softwaregemeinde gehört werden.*

schöpfung aus dem Jahre 1998 ist, um die Philosophie der bereits 1984 begründeten sog. «free Software» besser vermarkten zu können, und andererseits dadurch, dass eine sog. Open Source Definition besteht.

Betrachtet man Open Source Software als einen Zweig der sog. «free Software», wird man zur Begriffsbestimmung unweigerlich die Free Software Definition[5] konsultieren. Diese von RICHARD STALLMANN, Begründer und geistiger Vater der freien Softwarebewegung, erstellte Definition beantwortet die Frage, wann Software als «frei» bezeichnet werden darf. Mit «frei» wird dabei nicht etwa auf kommerzielle Aspekte abgestellt, sondern auf die vier Freiheiten, welche die Free Software Definition ausmachen. Diese beschreiben jeweils konkrete Nutzungshandlungen (gebrauchen, ändern, vervielfältigen, bearbeiten), welche der Benutzer freier Software vornehmen darf. Freie Software darf somit durchaus kommerziell verbreitet werden, solange dem Empfänger des Computerprogramms die vier Freiheiten zugestanden werden.

Die Definition von freier Software bildete indirekt die Vorlage für die eigentlich massgebende Definition von Open Source Software, die 1998 erarbeitete Open Source Definition[6]. Diese aus zehn Punkten bestehende Definition hält zu Beginn fest, dass es sich nur dann um Open Source Software handelt, wenn neben dem Zugang zum Quellcode auch die Lizenzbestimmungen, welche die Nutzung des Computerprogramms regeln, die Kriterien der Open Source Definition erfüllen. Neben den bereits in der Free Software Definition statuierten Nutzungsrechten finden sich in der Open Source Definition unter anderem auch Bestimmungen, welche die Integrität des Quellcodes, Diskriminierungsverbote und Erläuterungen zur gemeinsamen Verbreitung von Open Source Software und herkömmlicher Software betreffen.

Bei Open Source Software handelt es sich somit definitionsgemäss um Computerprogramme, welche unter Open Source Lizenzen verbreitet werden. Open Source Lizenzen wiederum sind Lizenzen, welche die Kriterien der Open Source Definition erfüllen und somit insbesondere die freie Verbreitung und Modifikation der Software gestatten und den Zugriff auf den Quellcode sichern.

2. Weitere Formen von Software

Neben freier Software bzw. Open Source Software existieren noch diverse weitere Formen von Computerprogrammen, welche zum Teil sprachlich dem Begriff «Open Source» nahe stehen aber alle in zentralen Punkten von der Free Software Definition oder der Open Source Definition abweichen.

Proprietäre Software bezeichnet Computerprogramme, welche unter restriktiven Lizenzbestimmungen verbreitet werden und bei welchen der Quellcode nicht zur Verfügung steht. Sie stellen genau das Gegenteil von Open Source Software dar und werden deshalb auch als «Closed Source Software» bezeichnet. Obwohl sie oft gegen ein Entgelt verbreitet werden, ist dies kein zwingendes Merkmal von proprietärer Software.

Kommerzielle Software charakterisiert sich dadurch, dass für das Computerprogramm ein Entgelt bezahlt werden muss. Oft wird es als Gegenteil von freier Software verstanden, was jedoch nicht korrekt ist, da freie Software ohne weiteres auch gegen ein Entgelt - wenn auch nicht in Form von Lizenzgebühren - verbreitet werden darf.

Bei Freeware gilt was bei freier Software eben nicht zwingend gelten muss: «free as in free beer»[7]. Computerprogramme, welche als Freeware gelten, können somit vom Benutzer kostenlos gebraucht, vervielfältigt und verbreitet werden[8]. Der Quellcode und mit ihm das Recht, das Computerprogramm weiterzuentwickeln, werden dem Benutzer allerdings nicht eingeräumt.

Shareware unterscheidet sich von den anderen herkömmlichen Kategorien von Computerprogramm nur durch das Vermarktungs- bzw. Vertriebskonzept[9]. Dieses

5 http://www.fsf.org/philosophy/free-sw.html.
6 http://opensource.org/docs/definition_plain.php.
7 «'Free software' is a matter of liberty, not price. To understand the concept, you should think of 'free' as in 'free speech', not as in 'free beer'» (http://www.fsf.org/philosophy/free-sw.html).
8 JOCHEN M., Softwareüberlassungsverträge, 3. A., München 2000, Rz. 289 a.E.
9 FRANK A., Kommerzielle Online-Nutzung von Computerprogrammen, CR 6/2000, S. 345.

beruht darauf, dass dem Benutzer für eine gewisse Zeit meist unentgeltlich die Möglichkeit gegeben wird, die Software zu testen. Danach muss für den weiteren Gebrauch ein Entgelt bezahlt werden. Um eine grösstmögliche Verbreitung der Software zu erreichen, wird dem Benutzer während der Testphase üblicherweise auch das Vervielfältigungs- und Verbreitungsrecht eingeräumt.

Ein Public Domain Computerprogramm charakterisiert sich dadurch, dass jegliche Verwendung der Software gestattet ist, da der Urheber der Software auf die ihm zustehenden Urheberrechte verzichtet und damit die uneingeschränkte Nutzung der Software ermöglicht[10]. Die Verfügbarkeit des Quellcodes ist allerdings kein Kriterium weshalb die Weiterentwicklung von Public Domain Software nicht immer möglich ist.

Mit Shared Source hat die Firma Microsoft Lizenzmodelle[11] entworfen, welche gewissen Personenkreisen bei bestimmten Computerprogrammen eine klar regulierte Einsicht in den Quellcode erlauben und als Reaktion auf die zunehmende Popularität und Konkurrenz von Open Source Software bewertet werden müssen. Allen Shared Source Lizenzmodellen ist gemeinsam, dass sie entgegen dem sprachlichen Verständnis keine echte «gemeinsame Nutzung» des Quellcodes erlauben und schon gar keine freie Weiterentwicklung und Verbreitung ermöglichen.

3. Copyleft

Weder die Free Software Definition noch die Open Source Definition enthalten Regelungen darüber, wie die von ihnen aufgestellten Freiheiten bzw. Kriterien gegenüber beliebigen Dritten, welche das Computerprogramm nicht direkt vom Urheber erhalten, sichergestellt werden. Es ist deshalb gemäss beiden Definitionen durchaus möglich, dass freie Software- bzw. Open Source Softwarelizenzen es dem Lizenznehmer freistellen, ob er das Computerprogramm im Sinne von Open Source weiterverbreitet. Da sich die Nutzungsfreiheiten nicht durch technische Massnahmen mit dem Computerprogramm verbinden lassen, bedarf es einer anderen Methode, um die Freiheiten in der Verbreitungskette für alle Teilnehmer zu sichern. Diese Methode, welcher sich auch die bedeutendste aller Open Source Softwarelizenzen, die GNU General Public License, bedient, wird als Copyleft bezeichnet.

Unter Copyleft versteht STALLMANN und dessen Free Software Foundation «a general method for making a program free software and requiring all modified and extended versions of the program to be free software as well.[12]» Die Umsetzung dieser Methode erfolgt in der GNU GPL in Art. 2 Abs. 1 lit. b in welchem festgehalten wird, dass weiterentwickelte GPL Software oder Software, die GPL Software oder Bestandteile davon enthält, wiederum unter den Bedingungen der GNU GPL lizenziert werden muss[13]. Copyleft hat somit nichts mit einer Abkehr vom Urheberrechtssystem zu tun, sondern setzt ganz im Gegenteil das Bestehen eines urheberrechtlichen Schutzes voraus; denn ohne diesen wäre es dem Urheber nicht möglich, über die Konditionen der weiteren Verwendung seines Werkes zu bestimmen. Mit Copyleft wird somit lediglich das urheberrechtliche Instrumentarium dazu verwendet, um allen Benutzern umfassende Verwendungsbefugnisse zu sichern[14]. Dies mag zu Beginn etwas verwirren, da das Urheberrecht bisher mehrheitlich für die Ausgestaltung proprietärer und entsprechend restriktiver Regelungen verwendet wurde.

III. Urheberrechtliche Aspekte bei Open Source Software

1. Freie Software als Werk?

A. Open Source Software als Werk i.S.v. Art. 2 Abs. 3 URG

Computerprogramme gelten beim Vorliegen der allgemeinen urheberrechtlichen Schutzvoraussetzung nach Art. 2 Abs. 3

10 JOCHEN M., a. a. O. (Fn 8), Rz. 284.
11 http://www.microsoft.com/resources/sharedsource/Licensing/default.mspx.
12 http://www.fsf.org/licenses/licenses.html#WhatIsCopyleft.
13 Vgl. die Kommentierung der GNU GPL bei WIDMER M. (Fn 4), S. 102 ff.
14 «Proprietary software developers use copyright to take away the users' freedom; we use copyright to guarantee their freedom. That's why we reverse the name, changing 'copyright' into 'copyleft'» (http://www.fsf.org/copyleft/copyleft.html).

URG als Werke im Sinne des Urheberrechts. Da Open Source Software nichts anderes darstellt als Computerprogramme, welche unter einer Open Source Softwarelizenz verbreitet werden, gilt dies auch für diese Art von Computerprogrammen[15]. Besonders bei Open Source Software darf die Frage gestellt werden, ob der Quellcode als solcher auch als Computerprogramm gilt. Das URG beantwortet diese Frage nicht. Mit einem Blick über die Landesgrenzen finden sich mit Art. 10 Abs. 1 Trips[16], Art. 4 WCT[17] und Art. 1 Abs. 2 Satz 1 der Computerprogramm-Richtlinie[18] gleich drei Rechtsnormen, welche den Schutz beiden Ausdrucksformen (Objekt- und Quellcode) zukommen lassen. Gemäss der herrschenden Lehre gilt denn auch in der Schweiz der Quellcode als Computerprogramm[19].

B. Open Source Software als Werk zweiter Hand i.S.v. Art. 3 URG

Art. 3 Abs. 1 URG definiert ein Werk zweiter Hand als eine geistige Schöpfung mit individuellem Charakter, das unter Verwendung eines bestehenden Werkes derart geschaffen wird, dass das vorbestehende Werk weiterhin in seinem individuellen Charakter erkennbar bleibt. Open Source Software als Entwicklungsmodell verstanden, begünstig somit die dauerhafte Entstehung von Werken zweiter Hand, werden doch dabei Computerprogramme fortlaufend von diversen Personen weiterentwickelt. Es kommt somit ständig zur Begründung von neuen selbständigen Urheberrechten, falls nicht eine sog. freie Benutzung[20] oder eine lediglich kleine Änderung vorliegt. Die Übersetzung des Quellcodes in den Objektcode, das sog. Kompilieren, stellt keine Übersetzung i.S.v. Art. 3 Abs. 2 URG dar. Es wird nämlich lediglich die Form in einer mechanischen und automatisierten Art und Weise durch ein weiteres Computerprogramm, den sog. Kompiler, verändert.

C. Open Source Software als Sammelwerk i.S.v. Art. 4 URG

Sammelwerke finden sich wie bei anderen Computerprogrammen auch bei Open Source Software im Bereich von Datenbanken und Programmpaketen. Beide sind selbständig geschützt, sofern bezüglich Auswahl und Anordnung eine geistige Schöpfung mit individuellem Charakter vorliegt (Art. 4 Abs. 1 URG).

Bei Datenbanken muss eine klare Trennung zwischen den Daten bzw. der Datenbank als solcher und dem zum Betrieb der Datenbank benötigten Computerprogramm gemacht werden. Nur Ersteres lässt sich als Sammelwerk qualifizieren weshalb auch die prominente Open Source Datenbank MySQL nicht als Sammelwerk, sondern als Computerprogramm zu qualifizieren ist.

Die unzähligen Distributionen[21], d.h. Sammlungen von diversen Open Source Computerprogrammen, welche auf ein Trägermedium gespeichert und zum Erwerb angeboten werden, stellen eine Form von Programmpaketen dar. Eine weitere Form von Programmpaketen findet sich bei komplexen Computerprogrammen wie z.B. Office Applikationen, bei welchen eigenständige Computerprogramme zu einer funktionalen Einheit verbunden werden. Auch sie sind bei individueller Auswahl und Anordnung als Sammelwerk geschützt.

D. Open Source Software als nicht geschütztes Werke

Freie bzw. Open Source Software geniesst unter den gleichen Bedingungen wie andere Computerprogramme den Urheberrechtsschutz. Die irrige Meinung, wonach es sich bei freier Software um Computer-

15 Auf die rechtliche Unterscheidung der Begriffe «Software» und «Computerprogramm» sei an dieser Stelle nicht eingegangen.
16 Abkommen über handelsbezogenen Aspekte der Rechte an geistigem Eigentum vom 15. April 1994 (SR 0.632.20).
17 WIPO Copyright Treaty vom 20. Dezember 1996.
18 Richtlinie 91/250/EWG des Rates vom 14. Mai 1991 über den Schutz von Computerprogrammen.
19 THOMANN F., Softwareschutz durch das Urheberrecht, in: Thomann F./Rauber G. (Hg.), Softwareschutz, Bern 1998, S. 11; NEFF E./ARNM., Urheberrechtlicher Schutz der Software, Urheberrecht im EDV-Bereich, in: SIWR II/2, Basel/Genf/München 1998, S. 122; BARRELET D./EGLOFF W., Das neue Urheberrecht, 2. A., Bern 2000, Rz 24 zu Art. 2 URG.
20 Als freie Benutzung erkannte der Einzelrichter am OG AG ein Computerprogramm, bei welchem der übernommene Quellcode nur zu einem Zehntel mit dem ursprünglichen Programm übereinstimmte (Entscheid «BLISS», SMI 1991, S. 79 ff.).
21 Solche Distributionen, welche zum Teil hunderte von einzelnen Programmen aufweisen können, finden sich insbesondere beim Betriebssystems GNU/Linux.

programme handelt, welche vom Internet beliebig bezogen und verwendet werden können, lässt sich womöglich mit dem zweideutigen Begriff «frei» erklären, welcher in diesem Zusammenhang aber eben gerade nicht frei von jeglichen Regelungen meint, sondern die durch die Lizenzbestimmungen gewährten Freiheiten bezeichnet.

2. Wer ist Urheber von Open Source Software?

Open Source Software wird typischerweise von einer Vielzahl meist nur lose organisierter Personen entwickelt. Die einzelnen Beiträge können dabei sowohl in quantitativem als auch qualitativem Umfang stark variieren, denn neben der eigentlichen Entwicklungsarbeit gibt es unzählige weitere Aufgaben wie z.B. die finanzielle Unterstützung des Projektes oder das Testen der Software, welche wahrgenommen werden müssen. Da der Urheber das ausschliessliche Recht hat zu bestimmen, ob, wann und wie sein Werk verwendet wird (Art. 10 Abs. 1 URG), bedarf es zur Weiterentwicklung von Computerprogrammen der Zustimmung des Urhebers. Es ist deshalb insbesondere in Hinblick auf die zunehmende Beteiligung von Unternehmen an der Entwicklung von Open Source Software unerlässlich, den Urheber bestimmen zu können, da ein gutgläubiger Erwerb von Nutzungsrechten ausgeschlossen ist.

A. Beginn der Entwicklung

Urheber eines Werkes ist diejenige natürliche Person, welche es geschaffen hat (Art. 6 URG). Unternehmen, welche Open Source Software entwickeln, gelten somit nicht als Urheber, können aber als Arbeitgeber nach Art. 17 URG Rechtsinhaber der ausschliesslichen Verwendungsbefugnisse sein. Als erschaffen gilt ein Computerprogramm auch dann, wenn es unter Zuhilfenahme von weiteren Computerprogrammen bzw. Programmierhilfen entwickelt wird, da diese bis heute lediglich als Werkzeuge gelten, deren sich der Entwickler bewusst bedient. Falls solche Hilfsprogramme allerdings eigene Codebestandteile in die Software integrieren, muss geprüft werden, ob es sich um einen Fall kollektiver Werkschöpfung handelt.

Betrachtet man die Entwicklung diverser Open Source Softwareprojekte, so stellt man fest, dass am Anfang oft der Code eines Einzelnen steht. Dieser Entwickler lässt sich somit als ursprünglicher Urheber der Software qualifizieren. Falls zu Beginn hingegen bereits mehrere Personen an der Entwicklung teilnehmen, kann es sich um Miturheberschaft (Art. 7 URG) handeln. Dies setzt allerdings voraus, dass die Entwickler einen Entschluss zur Verfolgung eines gemeinsamen Ziels gefasst haben und ihre Arbeit im Hinblick auf das Gesamtziel leisten[22]. Aus diesen Gründen gelten Personen, welche ein Projekt lediglich finanziell oder durch das Testen der Software unterstützen, nicht als Miturheber.

B. Beginn der Basarentwicklung

Das charakteristische Element des basarartigen Entwicklungsmodells ergibt sich typischerweise nach der Veröffentlichung der Software, da die Entwicklergemeinde erst jetzt von einem anstehenden Projekt erfährt und Zugang zu dessen Quellcode erhält. Spätestens zu diesem Zeitpunkt wird auch das Schicksal des zu Beginn von einer einzigen Person geschaffenen Codes durch Dritte beeinflusst. Dies bedeutet allerdings nicht zwingend, dass der ursprüngliche Urheber gänzlich die Kontrolle über die Weiterentwicklung verliert, da es ihm freisteht zu entscheiden, ob und unter welchen Bedingungen er den Code Dritter in die offiziellen Folgeentwicklungen integriert[23]. Die Stellung der nun zum Projekt stossenden Entwickler unterscheidet sich von der Anfangsphase des Projektes primär dadurch, dass nun bereits ein Programm vorhanden ist, an welchem weitergearbeitet werden kann. Eine solche Weiterarbeit an einem bereits bestehenden Werk führt nicht zu einer Miturheberschaft am ursprünglichen Werk, da es dazu an einer koordinierten Zusammenarbeit fehlt. Es handelt sich dann um eine Werkverbindung,

22 REHBINDER M., Schweizerisches Urheberrecht, 3. A., Bern 2000, Rz. 112; VON BÜREN R., Urheber, in: SIWR II/1, S. 139.

23 So entscheidet z.B. Linus Torvalds, der Erfinder des Betriebssystems GNU/Linux, grundsätzlich alleine über die Aufnahme von Weiterentwicklungen in die nächste Version der Software.

falls man nicht eine sog. nachträgliche Miturheberschaft bejahen kann. Dies charakterisiert sich dadurch, dass das ursprüngliche Werk in der klaren Absicht geschaffen wird, es als unselbständigen Teil mit weiteren Elementen zusammenzufügen[24]. Diese Situation lässt sich durchaus auch bei Open Source Softwareprojekten feststellen, ist es doch vielfach gerade der Sinn des entwickelten Programms, weiteren Entwicklern einen sog. «plausible promise»[25], vorzustellen um sie für die Weiterentwicklung gewinnen zu können. Typisch für diese Phase des Projekts ist allerdings weniger die Miturheberschaft als vielmehr die Urheberschaft an Werken zweiter Hand oder Sammelwerken.

Der Urheber eines Werkes zweiter Hand bzw. einer Bearbeitung erwirbt ein eigenständiges Urheberrecht, das sog. Bearbeiterurheberrecht. Die kontinuierliche Weiterentwicklung von Computerprogrammen kann somit dazu führen, dass unzählige Bearbeiterurheberrechte entstehen, welche bei der weiteren Verwendung der Software berücksichtigt werden müssen. Nicht jede Modifikation begründet allerdings ein Bearbeiterurheberrecht, da es dazu einer Bearbeitung mit selbständigem und individuellem Charakter bedarf. Wer mehrere Computerprogramme als Programmpaket derart zusammengestellt, dass bezüglich Auswahl oder Anordnung von einer geistigen Schöpfung mit individuellem Charakter auszugehen ist, gilt als Urheber des geschaffenen Sammelwerkes.

C. Welcher Entwickler ist Urheber?

Da sich die aufgezeigten Formen der Urheberschaft bei Open Source Software in beliebiger Reihenfolge, Kombination und Häufigkeit mischen können, kann eine präzise Bestimmung der Urheber äusserst schwierig ausfallen. Neben den rechtlichen Schwierigkeiten treten bei grösseren Projekten auch faktische Probleme hinzu. Obwohl Kollaborationsplattformen und Versionisierungssysteme die Erfassung der Entwickler erleichtern und die meisten Open Source Softwarelizenzen die Pflicht zum Anbringen eines Copyrightvermerks statuieren, werden viele Personen anonym oder unerkannt an der Software arbeiten. Lassen sich in einer solchen Situation nicht sämtliche Urheber eruieren, so gilt gemäss Art. 8 URG als Urheber, wer auf dem Werk als solcher bezeichnet wird. Wer die durch die Urheberrechtsvermerke wiedergegebenen Urheberverhältnisse somit bestreiten will, muss deren Unrichtigkeit beweisen.

3. Nutzungsbefugnisse

Nachdem feststeht, dass Open Source Software unter den allgemeinen urheberrechtlichen Schutzvoraussetzungen als Computerprogramm im Sinne des URG zu betrachten ist und auch die Urheberschaft freier Software geklärt ist, gilt es aufzuzeigen, welcher Mechanismus es Dritten rechtlich ermöglicht, an der Entwicklung freier Software teilzunehmen.

A. Gesetzliche Nutzungsbefugnisse

Faktisch wird die Weiterentwicklung dadurch ermöglicht bzw. initiiert, dass Dritten die Software zur Verfügung gestellt wird. Dies geschieht typischerweise durch das Abspeichern der Software auf einer über das Internet zugänglichen Kollaborationsplattform oder seltener durch die direkte körperliche Verbreitung der Software an die interessierten Kreise. Wird der Zugang auf die Kollaborationsplattform nicht eingeschränkt und der Download jedermann gestattet, lässt sich eine derart zur Verfügung gestellte Software als veröffentlicht betrachten. Dieser Umstand ermöglicht bei anderen Werkarten die Nutzung des Werks im Rahmen des Eigengebrauchs (Art. 19 URG). Da Art. 19 URG gemäss dessen Abs. 4 allerdings auf Computerprogramme keine Anwendung findet, erlaubt der Upload eines Computerprogramms nicht auch dessen Weiterentwicklung. Lässt sich der Upload der Software als Veräusserung, d.h. als ein definitives un- oder entgeltliches Weggeben des Programmexemplars qualifizieren[26], kann sie im Rahmen von Art. 12 Abs. 2 URG gebraucht oder weiterveräussert werden. Da die Erschöpfung allerdings

24 JANN M., Werkeinheit und Werkmehrheit im Urheberrecht, Zürich 1999, S. 29.
25 RAYMOND E., a. a. O. (Fn3), Kap. 9.
26 NEFF/ARN, aaO (FN 19), S. 246; BARRELET/EGLOFF (Fn 19), Rz. 9 zu Art. 12 URG.

an das jeweils in Frage stehende Werkexemplar knüpft, muss geprüft werden, ob die Bestimmung nach Sinn und Zweck unabhängig von einem Werkexemplar anzuwenden ist. Dies ist zu bejahen, da das Ziel sowohl der körperlichen als auch der unkörperlichen Verbreitung darin besteht, dem Dritten den Gebrauch des Computerprogramms zu ermöglichen. Die unkörperliche wie auch die körperliche Verbreitung kann somit zur Erschöpfung führen[27]. Damit kann der Empfänger das Computerprogramm im Rahmen von Art. 12 Abs. 2 URG i.V.m. Art. 17 Abs. 1 URV gebrauchen, was ihm allerdings noch nicht erlaubt, das Computerprogramm zu modifizieren. Wer das Recht hat, ein Computerprogramm zu gebrauchen, darf das Computerprogramm im Rahmen von Art. 21 URG auch entschlüsseln und nach Art. 24 URG eine Sicherungskopie erstellen. Weitere Rechte hat der Erwerber von Gesetzes wegen nicht. Der Urheber muss deshalb entsprechend rechtlich disponieren, um die Entwicklung von Open Source Software zu ermöglichen.

B. Vertragliche Nutzungsbefugnisse

Um Dritten die Weiterentwicklung von Open Source Software zu ermöglichen, kann der Urheber auf sein Urheberrecht verzichten. Dieser Verzicht - wie immer man ihn dogmatisch bewerten mag - führt dazu, dass der Urheber nicht mehr über die weitere Verwendung der Software bestimmen kann und es Dritten unbenommen ist, die Software nach ihrem Gutdünken zu nutzen. Die Freiheiten der Software sind dadurch nicht mehr für alle Personen in der Distributionskette garantiert, womit auch die Möglichkeit zur Weiterentwicklung nicht gesichert ist. Aus diesem Grund ist der Verzicht nicht das probate Mittel, um die Entwicklung freier Software zu fördern. Gleiches muss für die Übertragung von Urheberrechten gelten, da damit der Urheber seine Rechtsposition vollumfänglich und definitiv aufgibt und so nur dem Ersterwerber die Freiheiten garantieren kann. Danach liegt es im Ermessen des Rechtsinhabers wie er die ihm übertragenen Urheberrechte nutzt. Um freie Software nachhaltig entwickeln zu können, bedarf es deshalb der Einräumung von Nutzungsrechten. Diese kann konkludent oder explizit erfolgen. Während beide Arten die Entwicklung von freier Software ermöglichen, garantiert nur die explizite Einräumung von Nutzungsrechten die Einhaltung der Free Software Definition bzw. der Open Source Definition. Wie die Umsetzung dieser Definitionen im Rahmen der expliziten Rechtseinräumung erfolgt, lässt sich nur anhand einer Analyse der im konkreten Fall verwendeten Open Source Softwarelizenzen eruieren.

C. Open Source Softwarelizenzen

Open Source Softwarelizenzen sind Lizenzen, welche die Open Source Definition erfüllen. Da es nicht jedermann möglich ist, die unzähligen Softwarelizenzen auf ihre Konformität mit der Open Source Definition zu prüfen, führt die Open Source Initiative auf ihrer Website[28] eine Liste derjenigen Lizenzen, welche von ihr als Open Source Softwarelizenzen betrachtet werden. Diese lediglich alphabetisch strukturierte Liste lässt sich nach dem Kriterium «Copyleft» grundsätzlich in drei Lizenzkategorien teilen: Copyleft Lizenzen, Copyleft-light Lizenzen und Lizenzen ohne Copyleft.

Die prominenteste aller Open Source Softwarelizenzen, die GNU General Public License, fällt in die erste Kategorie und sichert somit die Freiheiten nicht nur dem Ersterwerber, sondern auch jedem Folgeerwerber. Zu ihr gesellen sich unter anderem auch noch die Open Software License und die Affero General Public License. Charakteristisch für die Vertreter der zweiten Kategorie ist ein beschränktes Copyleft in dem Sinn, dass Modifikationen der Software entweder nicht gesamthaft dem Copyleft unterliegen (Mozilla Public License 1.1), das Copyleft auf den Eigengebrauch beschränkt werden kann (GNU Lesser General Public License) oder anderweitig das Copyleft nicht die modifizierte Software als Ganzes betrifft. Die BSD-Lizenz ist die

27 BÜHLER L., Schweizerisches und Internationales Urheberrecht im Internet, Freiburg 1999, S. 275 f.; NEFF E./ARN M. (Fn 19), S. 248.
28 http://www.opensource.org/licenses/index.php.

meistverwendete Open Source Softwarelizenz ohne Copyleft. Sie räumt dem Lizenznehmer umfassende Nutzungsrechte ein und insbesondere auch das Recht die Software unter proprietären Lizenzbestimmungen weiterzuverbreiten.

IV. Schlussbemerkung

Open Source Software liegt heute im Trend und wird in vielen Bereichen als echte Alternative zu proprietärer Software anerkannt. Während die technischen und wirtschaftlichen Aspekte freier Software bereits heftig diskutiert wurden und immer noch werden, hat sich die rechtliche Diskussion erst in letzter Zeit intensiviert. Dies möglicherweise gerade noch rechtzeitig, um festzustellen, dass die Entwicklung von Open Source Software von verschiedenen Seiten bedroht wird: Neben der steten Gefahr, welche von einer möglichen Neuregelung im Patentrecht zugunsten von Softwarepatenten ausgeht, könnten sich auch die urheberrechtlichen Regelungen zugunsten technischer Schutzmassnahmen (Digital Rights Management[29]) indirekt negativ auf die Entwicklung von Open Source Software auswirken. Es bleibt deshalb zu hoffen, dass in der anstehenden Revision des Urheberrechtsgesetztes auch die Bedenken der Open Source Softwaregemeinde gehört werden, denn Open Source Software führt nicht zu einer Umkehr des heutigen Urheberrechtsverständnisses, sondern basiert gerade auf einem starken und ausgewogenen Urheberrecht. ■

29 Zum Verhältnis Open Source Software und Digital Rights Management vgl. das Statement von Openlaw unter http://www.openlaw.ch/Documents/OSSundDRM.pdf.

L'AUTRE REGARD
DIE ANDERE SICHT

„Der Computer behauptet, ich müsste mein Hirn updaten, um mit seiner neuen Software kompatibel zu sein."