Zeitschrift: Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie = Collection criminologie / Groupe suisse de travail de criminologie

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 21 (2003)

Artikel: Interceptions électroniques

Autor: Treccani, Jean

DOI: https://doi.org/10.5169/seals-1051094

JEAN TRECCANI[1]

INTERCEPTIONS ÉLECTRONIQUES

Résumé
Sans distinguer les interceptions licites des interceptions illicites, la présentation tend à décrire les moyens existants dans ce domaine, en particulier les moyens d'interception des données circulant sur les réseaux. Surtout technique, la présentation émet quelques considérations d'ordre juridique au sujet des interceptions judiciaires en Suisse notamment.

Elektronisches Abhorchen
Der Autor versucht – ohne das legale Abfangen von Daten vom illegalen zu unterscheiden – die aktuell in diesem Bereich bestehenden Mittel, insbesondere die Abfangmethoden der im Netz zirkulierenden Daten, zu beschreiben. Obgleich der Beitrag vorwiegend technischer Art ist, werden auch Überlegungen juristischer Natur zur Situation des gerichtlich verfügten Abhorchens von Daten, insbesondere in der Schweiz, geäussert.

1 Introduction juridique

En matière d'interceptions de données informatiques, la Convention du Conseil de l'Europe sur la cybercriminalité[2], signée mais non encore ratifiée par la Suisse, comporte deux obligations:

- l'obligation d'adopter les mesures législatives nécessaires pour ériger en infraction l'interception intentionnelle et sans droit de données informatiques lors de transmissions non publiques à des-

1 Interlaken@treccani.org
2 Ouverte à la signature le 23 novembre 2001, la convention était signée par 34 Etats à la mi-avril 2003, dont 4 Etats non-membres (USA, Canada, Japon et Afrique du Sud), et ratifiée par 2 Etats. Elle attend cinq ratifications, dont trois d'Etats membres du Conseil de l'Europe, pour entrer en vigueur.

tination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques (art. 3)[3];

- l'obligation d'adopter les mesures législatives ou autres permettant à ses autorités d'intercepter en temps réel les données relatives au contenu des communications par leurs propres moyens ou en contraignant les fournisseurs de services à faire usage de leurs capacités techniques existantes (art. 21).[4]

En l'état, le droit suisse satisfait-il à ces exigences?

1.1 L'obligation de sanctionner les interceptions illégales

En l'état, le Code pénal suisse ne sanctionne la soustraction de données (art. 143 CP) que si elle intervient dans un dessein d'enrichissement *et* si elle porte sur des données qui étaient spécialement protégées contre tout accès indu.[5] La simple curiosité et la simple malveillance excluent l'application de cette disposition. En outre, l'interception de données transmises sans protection particulière, comme c'est le cas actuellement de la plupart des flux en circulation

---

3 Article 3 – Interception illégale
Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

4 Article 21 – Interception de données relatives au contenu
1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes relativement à un éventail d'infractions graves à définir en droit interne, à:
a. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire; et
b. obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes, à:
i. collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire , ou
ii. prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique. [...]

5 FF 1991 II p.47: La protection peut être matérielle (verrouillage du local abritant l'ordinateur ou la mise sous clé des supports de données) ou logique (emploi de mots de passe, codage des données). Il faut que l'auteur soit obligé de franchir ces obstacles sans en ignorer le sens.

sur Internet ou sur les réseaux privés, ne saurait donner lieu à une poursuite pénale fondée sur l'art. 143 CP.

Il apparaît ainsi que les conditions d'application restrictives de l'art. 143 CP ne sont pas conformes aux exigences posées par l'art. 3 de la Convention sur la cybercriminalité. Existe-t-il d'autres dispositions susceptibles de corriger cette faiblesse?

Les art. 179ss CP protégeant le domaine secret ou le domaine privé ne corrigent pas cette inadéquation ni non plus les autres dispositions pénales. Les art. 179 à 179^{sexies} CP protègent en effet les seules correspondances papier, les conversations proprement dites (vocales) et les faits relevant du domaine secret à condition que ces faits soient observés au moyen d'un appareil de prise de vues ou qu'ils soient fixés sur un porteur d'images. Ces dispositions ne sanctionnent pas les interceptions portant sur l'activité d'un système informatique, dont le transport d'emails en particulier.

Selon nous, et bien que le législateur n'ait pas pu songer à cette forme de conversation lors de l'élaboration de l'art. 179bis CP, il faudrait toutefois assimiler aux conversations au sens de cette disposition le «chat», soit la conversation écrite en temps réel (IRC, ICQ, etc.). Cette activité humaine présente en effet toutes les caractéristiques de la conversation parlée.

L'art. 179^{novies} CP se montre quant à lui plus répressif que l'art. 143 CP puisqu'il réprime la soustraction de données personnelles sensibles ou de profils de la personnalité non publiques sans égard au dessein de l'auteur et sans égard au niveau de protection des données contre les accès indus. Sa portée reste toutefois restreinte aux seules données personnelles sensibles et aux profils de la personnalité au sens de la loi sur la protection des données, de sorte que, même combinée avec l'art. 173 CP, cette disposition ne suffit pas à rendre la législation suisse conforme aux exigences de l'art. 3 de la Convention sur la cybercriminalité.

L'art. 321ter CP sanctionne la personne qui viole le secret des télécommunications ou celui qui incite celle-ci à violer ce secret mais pas celui qui intercepte l'information électronique confidentielle sans pousser une personne à violer le secret auquel elle est astreinte en sa qualité de fonctionnaire, d'employé ou d'auxiliaire d'une organisation fournissant des services de télécommunication.

Quant à l'art. 50 LTC/FMG[6], il sanctionne – sans égard au dessein ou aux circonstances de l'accès aux données – celui qui utilise ou communique à des tiers des informations non publiques destinées à une autre personne et reçues au moyen d'une installation de télécommunication. Bien qu'elle ait été conçue en principe pour viser le cas où les informations sont parvenues par erreur à la connaissance de l'auteur, cette disposition s'applique sans doute aussi aux interceptions illicites. Elle trouve toutefois ses limites dans le fait qu'elle protège les informations transmises sur un réseau entrant dans le champ d'application de la LTC, ce qui n'est pas le cas d'un réseau informatique interne même si sa taille est très étendue. Au surplus, elle relève du seul droit pénal administratif.

En définitive, force est de constater qu'en l'état, la législation pénale suisse ne répond qu'imparfaitement aux exigences de l'art. 3 de la Convention sur la cybercriminalité.

1.2 L'obligation de favoriser les interceptions judiciaires en temps réel

La Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT/BÜPF) paraîtrait conforme en soi à l'obligation de l'article 21 de la Convention

6 Art. 50 Utilisation abusive d'informations
Quiconque ayant reçu au moyen d'une installation de télécommunication des informations non publiques qui ne lui sont pas destinées et les aura sans droit utilisées ou communiquées à des tiers, sera puni de l'emprisonnement pour une année au plus ou de l'amende.

sur la cybercriminalité s'il n'y avait son ordonnance d'application du 31 octobre 2001 (OSCPT/VÜPF) qui, pour des raisons incompréhensibles, a singulièrement restreint les moyens d'interception mis à la disposition des autorités de poursuite pénale en limitant les interceptions Internet aux seules interceptions d'emails.[7] On se prive ainsi de l'interception des sessions IRC ou ICQ, pour ne citer qu'elles, pourtant très prisées de certains délinquants actifs sur Internet. En cela, la législation suisse paraît nettement en retrait des obligations de l'art. 21 de la Convention sur la cybercriminalité.

Après cette brève introduction juridique, passons en revue de manière large les moyens d'interception envisageables d'un point de vue technique, sans distinction entre les moyens licites et les moyens illicites, et en nous intéressant d'abord aux moyens les plus éloignés de la cible pour nous rapprocher peu à peu de celle-ci.

2 Interceptions depuis Internet

2.1 Interceptions globales

Par essence, Internet ne connaît ni centre de contrôle ni routage figé. Lorsqu'il quitte l'ordinateur, le flux de données est haché en paquets de données indépendants les uns des autres pendant leur déplacement vers le destinataire et capables de voyager par des itinéraires variés, au gré des routeurs, rendant ainsi l'interception sur Internet de tous les paquets d'un même flux théoriquement impossible. En outre, la masse gigantesque des données en circulation rend illusoire la pose de filtres efficaces sur les routeurs, filtres qui auraient pour rôle d'isoler les paquets d'un expéditeur et d'un destinataire déterminés de la masse considérable de tous les autres paquets. Une interception pratiquée dans Internet au-delà du fournisseur d'accès, à

7 Cf. art. 24 OSCPT.

une échelle planétaire et focalisée sur un individu, paraît difficile à réaliser.

On a pourtant beaucoup parlé des interceptions pratiquées dans le système Echelon, système mis en place conjointement par les services de renseignements des Etats-Unis, du Royaume-Uni, du Canada, d'Australie et de Nouvelle-Zélande. Si l'existence de ce système de surveillance ne fait aucun doute, si l'existence d'interceptions des flux transitant par des satellites (du moins ceux de la voie descendante) ne fait aucun doute, il n'est pas certain en revanche qu'Echelon parvienne à contrôler efficacement les liaisons par câble ou par radio, intercontinentales voire continentales.

Bien qu'il existe des avis plus alarmistes à ce sujet, la Commission temporaire du Parlement européen sur le système d'interception Echelon estime, quant à elle, dans son rapport du 11 juillet 2001, que les pays en cause n'ont accès qu'à une partie très restreinte des communications par câble ou par radio et qu'en raison du personnel nécessaire, une partie plus limitée encore des communications peut être exploitée. A son avis, «quelle que puisse être l'ampleur des moyens et capacités d'interception des communications disponibles, il est établi que le nombre extrêmement important des communications empêche, dans la pratique, un contrôle total et minutieux de l'ensemble des communications».[8]

On trouve une analyse juridique de ce type d'interception dans le rapport de la Commission temporaire du Parlement européen.

8 Cf. http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_fr.pdf, not. ch.13.1.

2.2 Interceptions ponctuelles

2.2.1 Technique de déviation du flux

Par des techniques d'imposture bien connues des hackers[9], il est possible pour un individu, un service public ou privé de détourner vers sa propre machine les flux de données destinés à des tiers pour en prendre abusivement connaissance. Ces techniques passent par une tromperie des serveurs DNS[10].

On rappelle que les machines en communication sur Internet s'identifient entre elles par une séquence de chiffres unique, dite «numéro IP». Pour des raisons de mnémotechnie et de marketing, les humains ont ressenti le besoin d'attacher des noms de fantaisie («noms de domaine») à ces numéros d'identification. Comme les machines ne comprennent que les chiffres, il a fallu construire des tables de conversion permettant de retrouver un numéro IP à partir d'un nom de domaine.

C'est la fonction du serveur DNS que de traiter les requêtes en résolution de noms. Pour diminuer les temps de latence résultant des divers échanges entre serveurs sur Internet, le serveur DNS sollicité par la requête regarde dans un premier temps dans sa mémoire temporaire (dite «cache») s'il a déjà résolu récemment une requête similaire. Dans l'affirmative, il restitue le numéro IP délivré précédemment, s'épargnant ainsi des échanges externes. Ce n'est que s'il ne trouve rien dans sa mémoire-cache qu'il sollicitera l'aide en cascade d'autres serveurs sur Internet.

Pour détourner les informations destinées à un nom de domaine déterminé («Ucentrale.com» par exemple), il suffira à l'imposteur de polluer la mémoire-cache du serveur DNS utilisé par la victime en y

9 «DNS spoofing» ou «cache poisoning», voir par exemple http://www.sans.org/rr/firewall/DNS_spoof.php

10 «Domain Name Server»

associant Ucentrale.com à un faux numéro IP désignant sa propre machine. Dorénavant, et pendant toute la durée de vie de la mémoire-cache, les communications destinées à Ucentrale.com aboutiront sur la machine de l'imposteur, lequel rendra l'interception imperceptible en réexpédiant aussitôt une copie des emails interceptés à leur destinataire légitime. L'imposteur peut aussi décider de laisser transiter simplement les requêtes web à travers sa machine pour espionner l'activité de l'internaute. Il peut aussi restituer une réplique parfaite de la page web recherchée et simuler ainsi un échange durant lequel il s'appropriera sans effort les identifiant et mot de passe de la victime. Il peut aussi profiter de la confiance inspirée par l'apparence familière d'une page web usurpée afin d'inciter la victime à contaminer sa machine par un virus ou un cheval de Troie.

La méthode conduisant à la pollution de la mémoire-cache du serveur DNS peut être appliquée à distance, depuis n'importe où sur Internet. Elle requiert peu de moyens et des connaissances techniques peu évoluées. Elle est donc à la portée de maintes personnes, autorisées ou non.

En l'état, un tel comportement semble échapper au Code pénal suisse si l'auteur est mû par la simple curiosité ou la simple malveillance, l'infraction de soustraction de données (art. 143 CP) supposant, on l'a rappelé, un dessein d'enrichissement illégitime. Quant à l'infraction d'accès indu à un système informatique (art. 143bis CP), elle suppose que le système informatique pénétré soit spécialement protégé contre tout accès de tiers, ce qui n'est généralement pas le cas d'un serveur DNS, lequel est ouvert aux requêtes extérieures en principe. Cette dernière infraction suppose aussi que l'introduction intervienne dans le système informatique appartenant à autrui. Or, on ne saurait soutenir selon nous que l'interception par l'espion, sur Internet, d'un flux en transit sur sa machine puisse être considérée comme une introduction dans un système informatique tiers. En fin de compte, seul le droit pénal administratif (art. 50 LTC/FMG) paraît

en mesure de réprimer plus directement les interceptions de cette nature.[11]

D'entente avec le fournisseur d'accès de la personne à surveiller, l'autorité de poursuite pénale pourrait organiser une interception partielle à moindre coût et à moindre dérangement en réglant le serveur DNS de façon que tout courrier destiné à tel nom de domaine soit délivré au préalable à la machine du policier, ou bien de façon que les requêtes web destinées à un site à contenu pédophile transitent par la machine du policier, qui pourrait ainsi identifier tous les visiteurs du site illicite et connaître leur activité sur le site.

En droit suisse, face à une infraction comprise dans le catalogue légal, ce moyen serait tout à fait compatible avec la LSCPT. Il faudrait toutefois aménager son ordonnance d'application du 31 octobre 2001 (OSCPT), qui, on l'a relevé, a singulièrement restreint quant à elle les moyens de lutte contre la criminalité mis à la disposition des autorités de poursuite pénale. Au surplus, il faudrait vaincre aussi la mauvaise volonté des fournisseurs d'accès, fréquente en Suisse comme nous avons eu l'occasion de le constater encore dans une affaire récente.[12]

2.2.2 Technique du cheval de Troie

Sous l'appellation générique de «cheval de Troie», on désigne le logiciel conçu pour s'infiltrer discrètement dans la machine tierce en s'agrippant et se cachant derrière un fichier d'apparence sympathique. Contrairement au virus, qui a pour vocation de dégrader le comportement de la machine, le cheval de Troie a pour vocation de

11 A moins que la modification provisoire de la mémoire-cache du serveur DNS puisse constituer une détérioration de données au sens de l'art. 144bis ch.1 CP, ce dont nous doutons.

12 Dans cette affaire, il était frappant de constater à quel point nombre d'informaticiens résistaient opiniâtrement aux décisions judiciaires par souci de protéger le bastion de leur pouvoir sur l'information. A cela s'ajoute souvent une conception surannée d'Internet, qui doit échapper selon eux à tout contrôle étatique nonobstant les atteintes à l'ordre juridique.

tourner discrètement en arrière-plan et d'ouvrir des portes secrètes à des visiteurs venus d'Internet ou du réseau interne. Celui qui a inoculé le cheval de Troie parvient à prendre le contrôle à distance de la machine et ainsi, suivant les variantes, à y prélever ou modifier des fichiers, à écouter et à voir au moyen des microphones et caméras web de la machine infectée, et bien d'autres choses étonnantes encore.

Mise au point par des hackers, cette méthode a été récupérée par une société américaine, qui a commercialisé le cheval de Troie D.I. *.* auprès des autorités gouvernementales. Introduit dans la machine cible, le logiciel enregistre toutes les frappes au clavier dans un fichier, lequel est transmis discrètement et périodiquement à l'observateur via le serveur de messagerie de la personne sous surveillance. Les mots de passe et textes saisis au clavier sont stockés en clair dans le fichier, avant leur éventuel chiffrement par un logiciel actif dans l'unité centrale. L'efficacité de D.I.*.* est telle qu'il parvient à neutraliser les pare-feu[13] logiciels personnels les plus courants. Initialement et tant que son existence fut méconnue du public[14], il n'était pas détecté par les logiciels de détection de virus.

Le FBI aurait écrit de toutes pièces un logiciel de cette nature dans le cadre d'un projet intitulé «Magic Lantern». Les programmes antivirus ne le détecteraient pas, soit parce qu'ils n'auraient pas connaissance de la structure (signature) du logiciel, soit parce que le FBI serait parvenu à convaincre les producteurs de programmes antivirus de l'ignorer.

En Suisse, la LSCPT ou les codes cantonaux de procédure pénale autorisent-ils l'emploi de ce procédé? Sans base légale expresse, l'introduction clandestine d'un corps étranger dans une machine distante située généralement dans des locaux privés ou dans une machine spécialement protégée contre les accès indus paraît difficilement ad-

13 «Firewalls»

14 Aujourd'hui, une page web référencée par les moteurs de recherche le décrit en détail.

missible. A cela s'ajoute que l'OSCPT, qui paraît limitative quant aux moyens mis à la disposition des autorités de poursuite pénale, ne dit rien d'un tel procédé.

3 Interceptions depuis l'infrastructure du fournisseur d'accès

L'interception au niveau de l'infrastructure du fournisseur d'accès devrait être le moyen d'interception le plus naturel pour l'autorité. Le policier installe un ordinateur sur le réseau du fournisseur d'accès pour y capter l'entier des données provenant ou destinées à l'abonné sous surveillance. L'abonné continue à recevoir et à émettre en temps réel sans percevoir la mesure de surveillance. Les données sont enregistrées sur un support de masse puis réinterprétées grâce à des logiciels capables de reproduire l'information en clair à l'écran.

Le moyen est bon marché et s'applique à presque toutes les formes d'accès, dont les accès par la ligne téléphonique (y compris l'ADSL), par le câble de la télévision, par le réseau électrique, etc. Tous les services peuvent être interceptés (web, ftp, smtp, etc.). C'est un moyen presque absolu, sous réserve des communications chiffrées (SSL par exemple), dont le contenu demeure inaccessible en principe.

Ce moyen est praticable à condition:
- que l'usager fasse usage d'un fournisseur d'accès situé en Suisse, plus précisément d'un fournisseur d'accès dont l'infrastructure se situe en Suisse[15];
- qu'il n'utilise qu'un seul fournisseur d'accès (ce qu'un examen des factures téléphoniques révèlera le cas échéant);

15 Certains fournisseurs d'accès offrent un numéro de téléphone suisse mais redirigent de manière transparente la requête de connexion à l'étranger, où se trouve en fait l'infrastructure technique.
Par ailleurs, on trouve depuis peu des accès par la voie satellitaire, tant montante que descendante, qui échappent aux contrôles suisses si le fournisseur d'accès se situe à l'étranger.

- qu'il soit identifié lors de ses accès, soit parce qu'enregistré comme abonné, il se prête à une procédure d'identification rigoureuse, soit parce que le fournisseur d'accès enregistre le numéro de téléphone appelant ou l'identité de la carte réseau utilisée («MAC address»).

Parmi les inconvénients, on relève l'absence de confidentialité puisque le fournisseur d'accès est nécessairement mis au courant de la mesure.

Ce moyen est mis en œuvre par les autorités françaises de poursuite pénale depuis l'année 2000. En Suisse, bien que compatible avec la LSCPT, il n'est pas prévu par l'OSCPT, qui omet de prévoir le recours à l'interception générale de flux Internet depuis l'infrastructure du fournisseur d'accès, limitant ce moyen à la seule interception de la correspondance par emails. Les délinquants actifs sur Internet utilisent pourtant intensément d'autres services que l'email pour communiquer, tels ICQ ou IRC. La limitation introduite par l'OSCPT, incompatible avec l'art. 21 de la Convention sur la cybercriminalité, paraît d'autant moins compréhensible que la mise en œuvre du moyen est aisée d'un point de vue technique.[16]

Le Service des tâches spéciales (ci-après STS/DBA) du DETEC/UVEC met, depuis le 1er avril 2003, à la disposition des autorités de poursuite pénale le moyen d'intercepter des emails tel que prévu par l'OSCPT, soit le moyen d'intercepter les emails d'une personne expédiés et reçus par le biais de la messagerie de son fournisseur d'accès suisse.

Cette approche fait abstraction d'une réalité: sur Internet, bien des délinquants renoncent à utiliser la messagerie trop visible de leur propre fournisseur d'accès, lui préférant une messagerie située à

16 En France, on trouve l'appareillage nécessaire, clef en main, au prix de 30'000 Euros.

l'étranger, capable de préserver leur anonymat (par exemple hotmail.com ou caramail.com).

On comprend donc que ce moyen d'interception sera d'une utilité toute relative face à certaines formes de délinquance comme la cyberdélinquance, la délinquance liée à la pédophilie ou encore la délinquance organisée impliquant des personnes situées en Suisse[17]. Et une fois encore, on doit regretter que l'OSCPT ne prévoie pas le moyen plus général et plus efficace décrit ci-avant, permettant l'interception de tous les paquets reçus et expédiés par un internaute déterminé en transit chez le fournisseur d'accès, sans égard au service utilisé.

4 Interceptions depuis la ligne téléphonique

Confronté à un prévenu utilisant sa ligne téléphonique pour changer régulièrement de point d'accès à Internet ou pour entrer sur Internet par un fournisseur d'accès dont l'infrastructure est située à l'étranger, l'efficacité commandera la pose d'une sonde produite au Danemark, sonde indépendante du fournisseur d'accès car placée sur la ligne téléphonique de la personne à surveiller. A large spectre, la sonde enregistre simultanément les conversations téléphoniques, les télécopies et les divers services principaux d'Internet (web, smtp, pop, ftp, etc.) pour permettre leur reproduction ultérieure. Elle prend en charge l'ADSL aussi.

La sonde est placée avant le fournisseur d'accès, et l'écoute peut sans autre être dérivée vers le centre d'écoutes téléphoniques habituel; la confidentialité est ainsi assurée. Elle enregistre tout ce qui passe sur la ligne et permet une restitution différée sous la forme appropriée (sonore pour la voix, écran pour Internet ou le fax). Si un

17 Bien entendu, ce moyen d'interception devient intéressant vis-à-vis d'un délinquant actif depuis l'étranger, plus enclin à ouvrir une boîte pour ses emails en Suisse, pays lointain pour lui.

service n'est pas encore pris en charge par le module standard au moment de l'interception, les données sont néanmoins stockées sur le support de masse dans l'attente de la création d'un interpréteur adapté. Sitôt l'interpréteur mis au point, il devient possible de reproduire la session, même longtemps après l'enregistrement. Le chiffrement de la communication peut néanmoins constituer un obstacle insurmontable suivant les cas.

Le principal inconvénient du système réside dans son coût élevé. En France, l'un des services centraux a acheté une telle sonde. D'autres services de police recourent quant à eux à la location et paient 10'000 Euros par mois pour profiter de l'équipement complet (sans l'ADSL toutefois), montant auquel s'ajoute le coût de l'écoute téléphonique proprement dite.[18]

Le STS/DBA a prévu d'offrir un service de cette nature en 2004 en principe. L'ADSL est toutefois totalement délaissé, ce qui surprend face à l'essor rapide de ce mode de communication et au prix de vente raisonnable de la sonde ADSL[19]. L'art. 21 de la Convention sur la cybercriminalité imposera l'introduction de ce moyen de surveillance selon nous.

5 Interceptions depuis le réseau local

L'interception au niveau du réseau local est facile à mettre en œuvre avec le concours de l'administrateur du réseau, lequel est d'ailleurs tenu selon le droit suisse de tolérer sinon de participer à la surveillance.[20] Elle obéit aux mêmes conditions techniques que l'interception opérée depuis chez le fournisseur d'accès. Elle permettrait facilement l'interception de *toutes* les données en relation avec un internaute déterminé si l'OSCPT, dont on suppose qu'elle est aussi ap-

18 En Suisse, env. fr 10'000.– pour trois mois (contre 300 Euros pour la même prestation en Allemagne).
19 On trouve en France un fournisseur de sondes ADSL qui les vend à 30'000 Euros l'unité.
20 Art.1 al.4 LSCPT/BÜPF, art. 1er al.2 litt.f, 28 et 29 OSCPT/VÜPF.

plicable à la surveillance depuis un réseau local des échanges concernant Internet,[21] n'était pas limitative quant aux types de surveillance possibles en matière d'Internet.[22]

En ce qui concerne la correspondance échangée *à l'intérieur* des réseaux internes, il semble bien que l'OSCPT se montre moins restrictive qu'en cas d'échanges via Internet[23] en ce qu'elle n'énonce pas de manière limitative les types de surveillance comme le fait l'art. 24 OSCPT en matière de surveillance des accès à Internet. Il s'ensuit qu'en matière de surveillance de la correspondance sur un réseau interne, les formes de correspondance autres que celle de l'email («chat» par exemple) devraient pouvoir donner lieu à interceptions judiciaires aussi.

Au sujet des interceptions non autorisées, on note que l'interception de paquets de données échangées sur un segment du réseau local[24] ne requiert aucun moyen matériel; seule l'exécution d'un logiciel est nécessaire, logiciel au demeurant facile à utiliser. Il est troublant de constater que déployé sur un réseau privé et sans dessein d'enrichissement[25], ce comportement est mal réprimé en droit suisse malgré l'atteinte grave à la sphère privée. En effet, les art. 179ss CPS ne sanctionnent les atteintes à la sphère privée que si l'enregistrement illicite porte sur des conversations entre personnes, et l'art. 50 LTC ne trouve pas application dans le cas d'échanges de données sur le seul réseau local, lequel échappe au champ d'application de la LTC.

21 L'OSCPT parle sous section 6 de «Surveillance des accès à Internet» – «Überwachung der Internet-Zugänge» – «Sorveglianza dell'accesso a Internet».
22 Art. 24 OSCPT
23 Cf. art. 28 et 29 OSCPT
24 «Sniffing»
25 La soustraction de données de l'art. 143 CP suppose un dessein d'enrichissement illégitime.

6 Interceptions aux alentours de la cible

6.1 Interception des champs électromagnétiques

On connaît le cas célèbre du télécopieur doté d'un élément Rockwell DataPump ou le cas de certains modems fabriqués par U.S. Robotics, appareils dont les fortes émissions électromagnétiques pouvaient être captées et démodulées par le biais d'un simple poste radio VHF. Ce phénomène spectaculaire est aussi connu pour certains microphones utilisés dans les salles de conférence.

En fait, tout composant électronique émet des champs électromagnétiques susceptibles d'être interceptés puis interprétés à plusieurs dizaines voire centaines de mètres de la source d'émission.[26] C'est particulièrement vrai pour les télécopieurs, les écrans d'ordinateur, les lecteurs de CD-R ou DVD externes, les scanners, les imprimantes, les photocopieurs et autres périphériques. Au point que la National Security Agency a créé la norme TEMPEST[27] pour distinguer les appareils obéissant à des critères rigoureux de protection contre ce type d'interception.

Il existerait dans certains milieux gouvernementaux un savoir-faire en matière d'interception et d'interprétation des champs électromagnétiques émis par les appareils électroniques, savoir-faire qui, s'il existe vraiment, pourrait être récupéré par les autorités de poursuite pénale. Si la LSCPT n'interdit pas en soi le recours à un moyen d'interception de la correspondance par voie de télécommunication fondé sur les champs électromagnétiques, l'OSCPT ne prévoit pas toutefois cette possibilité dans la panoplie des moyens offerts aux autorités de poursuite pénale. Il faut donc y renoncer (du moins en matière d'Internet).

---

26 En 1985, Wim van Eck a publié le résultat de ses recherches démontrant la facilité d'interception des champs électromagnétique émis par un écran tv [d'une technologie largement dépassée aujourd'hui] situé à des centaines de mètres: http://www.tscm.com/vaneck85.pdf

27 «Telecommunications Electronics Material Protected From Emanating Spurious Transmissions»

Quant à l'interception de champs électromagnétiques à des fins illicites, elle semble difficile à réprimer sur la base des dispositions du droit suisse en vigueur. En cela, une adaptation de la législation suisse devra être envisagée pour la rendre conforme à l'art. 3 de la Convention sur la cybercriminalité, qui prévoit expressément la nécessité de sanctionner ce type d'interception.

6.2 Interception des ondes hertziennes

Nous entrons dans une époque caractérisée par l'essor des liaisons ou des réseaux sans fil[28] (Bluetooth, Wi-Fi 802.11b, UWB, HomeRF). Les ordinateurs et leurs périphériques tendent de plus en plus à communiquer entre eux par ondes hertziennes, tout comme les ordinateurs entre eux sur le réseau.

Nous entrons ainsi de plain-pied dans l'âge d'or des interceptions électronique, bien que les données soient en principe[29] protégées par la technique des sauts de fréquence, ainsi que par une authentification et un chiffrement des données transmises de 128 bits au moins. Il n'est pas rare en effet que l'authentification et le chiffrement soient inactifs par suite de paresse ou d'ignorance[30], permettant ainsi des abus. A lire certains documents publiés dans les milieux interlopes d'Internet, il semblerait facile de casser le chiffrement et la procédure d'authentification. Cette assertion mériterait d'être vérifiée.

Les remarques formulées au sujet des interceptions de champs électromagnétiques s'appliquent ici également: la LSCPT ne s'oppose pas fondamentalement à la surveillance de la correspondance par

28 WLAN = wireless local area network

29 Le clavier sans fil n'est pas particulièrement protégé contre les interceptions.

30 Souvent la configuration par défaut exclut le chiffrement et l'authentification par la «Mac Address», soit le numéro d'identification unique attribué à la carte réseau.

l'interception des ondes hertziennes. L'OSCPT ne prévoit pas ce moyen toutefois (du moins en matière d'Internet).

7 Interceptions depuis l'ordinateur de la personne sous surveillance

7.1 L'espion clavier logique

On trouve sans difficulté sur Internet des logiciels payants ou gratuits[31] intitulés «keylogger». Après leur premier lancement, ces logiciels démarrent automatiquement à chaque mise en route de l'ordinateur et tournent de manière invisible en arrière-plan pour enregistrer toutes les frappes au clavier. L'information est stockée dans un fichier du disque dur dans l'attente d'être copiée et lue par l'intrus. Les échanges avec d'autres périphériques sont bien entendu ignorés, les informations affichées à l'écran ne figurant dans le fichier occulte que si elles résultent de frappes au clavier. Le fichier occulte contient les mots de passe en clair puisqu'ils sont enregistrés avant d'être transformés par un logiciel de chiffrement en aval de la saisie clavier, au niveau de l'unité centrale.

Sauf à adopter un mode de contamination du type cheval de Troie, l'installation clandestine d'un espion clavier logique passe par un accès direct à la machine et au compte exploité par la personne à espionner. Il suppose aussi des droits d'administrateur autorisant l'installation d'un nouveau programme dans le compte.

En principe, il y aura infraction à l'art. 143bis CP, du moins si l'observateur a fait usage d'un mot de passe usurpé pour entrer dans la machine afin d'y placer le logiciel espion. S'il a profité d'un moment d'inattention de l'ayant droit pour s'introduire dans son bureau et

31 S'ils sont gratuits, ces logiciels sont eux-mêmes souvent piégés par des chevaux de Troie; lorsque l'intéressé lance le programme sur sa propre machine pour le tester juste après son téléchargement, il infecte sa propre machine. Tel est pris qui croyait prendre.

dans son compte informatique restés ouverts, l'infraction ne sera pas réalisée.

Sans dessein d'enrichissement, l'interception n'est pas en soi réprimée par le code pénal suisse à moins d'interception de données relevant de la LPD.

Le secret des télécommunications de la LTC ne protège pas l'email au moment de sa rédaction déjà, pas plus que le secret de la correspondance par poste ne protègerait le contenu d'une lettre dès sa rédaction. L'email ne bénéficie de cette protection qu'au moment où il intègre un réseau public, ce qui suppose donc au préalable la rédaction de l'email, la mention d'un destinataire, l'ordre de transmission donné au logiciel de messagerie de l'ordinateur local puis la prise de contact et l'identification du client de messagerie auprès du serveur de messagerie, lequel se trouve suivant les cas sur le réseau local ou directement sur Internet; ce n'est qu'ensuite que l'email est véritablement transféré sur Internet. L'interception par un espion clavier intervient avant le processus d'expédition; elle ne saurait dès lors enfreindre le secret des télécommunications de la LTC ni, partant, être réprimée sur la base de l'art. 50 LTC.

7.2 L'espion clavier matériel

L'espion clavier matériel peut être pourvu ou non d'un émetteur radio transmettant l'information en temps réel à l'observateur. Il peut se fixer dans le clavier ou plus simplement entre le clavier et l'unité centrale. S'il suppose un accès physique à la machine, il ne requiert quant à lui aucun accès au compte de l'utilisateur dans la machine. Sans émetteur radio, il stocke dans sa propre mémoire les frappes opérées au clavier; après un certain temps, l'observateur retire l'espion clavier matériel puis l'installe sur son propre ordinateur pour y lire le contenu de la mémoire. Ce moyen s'avère d'une simplicité d'utilisation et d'une efficacité redoutables.

Les LSCPT et son ordonnance d'application donnent-ils aux autorités de poursuite pénale le droit d'utiliser un clavier espion matériel lorsque la police peut accéder à l'ordinateur sans commettre de violation de domicile (cybercafé, bureau de l'employeur lésé, etc.)?

Il faut en douter en l'état actuel de l'OSCPT pour ce qui est d'une mesure de surveillance portant sur Internet. En ce qui concerne l'interception d'une saisie au clavier liée à de la correspondance à l'intérieur d'un réseau, cela paraît admissible au regard de l'art. 28 OSCPT. Enfin, s'agissant de la saisie au clavier sans relation avec Internet ni avec de la correspondance à l'intérieur du réseau (saisie dans un traitement de textes ou dans un tableur par exemple), la LSCPT ne trouve pas application. La question délicate de savoir si un code de procédure pénale pourrait prévoir valablement ce moyen est laissée ouverte.

Non autorisée et sans dessein d'enrichissement, une telle interception ne peut être sanctionnée sur la base de l'art. 143 CP. Sous l'angle de l'art. 143bis CP, la question se pose de savoir s'il y a «introduction» proprement dite dans un système informatique au sens de cette disposition dans le fait de placer un appareil espion *entre* le clavier et l'unité centrale, appareil se bornant à enregistrer les frappes au clavier. Il ne fait pas de doute que la notion de *système informatique* englobe tous les éléments actifs d'une structure informatique autonome, sans égard au fait qu'ils soient épars ou réunis dans un même coffret, ou qu'ils soient reliés entre eux matériellement ou par ondes.

8 Conclusion

En Suisse, l'autorité de poursuite pénale se trouve excessivement limitée dans ses moyens d'action dans Internet parce que l'OSCPT/VÜPF s'est montrée frileuse à cet égard. Ce constat a conduit la

CAPP[32] à formuler en automne 2002 une résolution tendant à obtenir une révision de l'OSCPT sur ce point.

Les interceptions illicites fleurissent sur Internet, favorisées en partie par la disponibilité de logiciels clef en main (les chevaux de Troie en particulier) dont l'emploi n'exige que de maigres connaissances techniques.

Mais il est un endroit insoupçonné où les interceptions abusives peuvent se développer dangereusement et en toute discrétion, endroit oublié où l'on cultive parfois l'ignorance des dirigeants pour maintenir cet état de fait: le centre informatique de l'entreprise. Parce qu'ils se sont persuadés que ce pouvoir allait de soi, parce que les dirigeants de l'entreprise l'ignorent souvent ou parce qu'on leur a fait croire que cela était indispensable à l'exécution de leur travail, les informaticiens s'arrogent des droits d'accès exorbitants aux informations les plus sensibles circulant sur le réseau voire stockées sur les disques durs locaux[33], droits dont quelques-uns abuseront d'autant plus facilement que leur abus ne laissera aucune trace.[34] Il serait temps de faire preuve de la même clairvoyance que celle des magistrats canadiens[35] et d'instaurer des interdictions expresses d'accès aux données de l'entreprise. Sur le plan technique, il serait judicieux d'incorporer dans les logiciels d'administration des solutions permettant d'aménager des mots de passe conjoints entre informati-

32 Conférence des autorités de poursuite pénale de la Suisse romande et du Tessin.

33 Dans sa configuration par défaut, Windows ouvre un accès invisible en faveur de l'administrateur du réseau aux disques locaux des utilisateurs. Il faut une gymnastique complexe pour fermer cette voie d'accès.

34 Parmi d'autres, les aveux d'un ex-informaticien devenu journaliste: http://www.largeur.com/expArt.asp?artID=37

35 Ces derniers ont édicté des règles interdisant aux informaticiens le moindre accès à leurs données (http://www.cjc-ccm.gc.ca/francais/aim/CJC33F.pdf – «Lignes de conduite sur la surveillance informatique»).

ciens et dirigeants de l'entreprise pour accéder à certaines fonctionnalités sensibles.[36]

A mon unité centrale.

36 Un logiciel de chiffrement et d'authentification portant sur les données sensibles d'une banque nous a été présenté récemment. Si le concepteur du logiciel a bien prévu d'écarter les données en exploitation de la curiosité directe de l'informaticien chargé de l'administration du logiciel, il a oublié en revanche de prévoir un système de mots de passe obligatoires *entre plusieurs personnes* pour autoriser la création d'un nouvel utilisateur. De sorte que l'informaticien malhonnête trouvera aisément une voie d'accès aux données secrètes en créant un utilisateur fantaisiste doté de tous les droits, avec pour seul risque de laisser dans les fichiers d'audit une trace de la création abusive, risque dont la force dissuasive nous paraît dérisoire face à la masse gigantesque des informations enregistrées dans les fichiers d'audit.