www.jusletter.ch

Dr. Sylvain Métille

Les mesures de surveillance prévues par le CPP

Quelles places pour le cheval de Troie, l'IMSI-Catcher ou les puces RFID ?

L'auteur rappelle les conditions requises pour qu'une mesure de surveillance soit autorisée, de même que les procédures et critères ancrés dans le Code de procédure pénale fédéral. La question de savoir sous quelle catégorie du CPP (surveillance de la correspondance par poste et télécommunication, surveillance des relations bancaires, observation ou autres mesures) est comprise une mesure doit être résolue, afin que cette dernière ne soit pas illégale. En lien avec l'utilisation d'un cheval de Troie, l'auteur propose de retenir comme critère l'objet visé par la surveillance pour déterminer la procédure à suivre. Une nouvelle catégorisation serait illégale.

Catégorie(s) : Télécommunications. Réseaux ; Informatique et droit ; Procédure pénale ; Contributions

Proposition de citation : Sylvain Métille, Les mesures de surveillance prévues par le CPP, in : Jusletter 19 décembre 2011

ISSN 1424-7410, www.jusletter.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 Editions Weblaw

Table des Matières

I. Un équilibre à trouver entre sphère privée et surveillance
1. La protection de la sphère privée
2. Les conditions à respecter pour restreindre la sphère privée
II. La surveillance prévue par le CPP
1. Les mesures de surveillance
2. Les conditions et la procédure
III. Quelques techniques difficiles à classer
1. La surveillance des relations bancaires en temps réel
2. L'IMSI-Catcher
3. Les puces RFID
4. Le cheval de Troie
IV. Conclusion

I. Un équilibre à trouver entre sphère privée et surveillance

1. La protection de la sphère privée

[Rz 1] En Suisse, la protection de la sphère privée est principalement garantie par les articles 13 al. 1 Constitution fédérale (Cst.) et 8 Convention européenne des droits de l'homme (CEDH). Elle confère à toute personne le droit de mener sa vie selon son propre choix, de choisir son mode de vie, d'organiser ses loisirs et d'avoir des contacts avec autrui sans intervention des pouvoirs publics. L'identité, le respect de la sphère intime et secrète, l'honneur et la réputation d'une personne, ses relations avec les autres, ainsi que l'autodétermination en matière sexuelle appartiennent au champ de protection de la vie privée[1].

[Rz 2] La notion de vie privée englobe également les données concernant les activités professionnelles ou commerciales d'un individu[2]. Selon la Cour européenne des droits de l'Homme, la protection de la vie privée est principalement destinée à assurer le développement, sans ingérence, de la personnalité de chaque individu dans ses relations avec ses semblables[3]. L'intégrité physique, l'intégrité morale et la protection des données sont également garanties par la protection de la sphère privée, alors que la Constitution fédérale les protège au travers de la protection de la liberté personnelle.

[Rz 3] Selon la jurisprudence du Tribunal fédéral, le droit au respect de la vie privée protège l'ensemble des informations relatives à une personne qui ne sont pas accessibles au public[4]. L'enregistrement d'images de surveillance prises sur des places ou des voies publiques et la conservation de ces enregistrements portent par exemple atteinte à la sphère privée, comme la conservation de données signalétiques. La conservation de données personnelles non accessibles au public peut constituer une atteinte, quand bien même ces données auraient été collectées sans violation du droit constitutionnel et que les informations recueillies correspondraient aux faits[5]. La Cour européenne des droits de l'Homme a précisé que des données de nature publique peuvent relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics[6].

[Rz 4] On peut ainsi retenir que les mesures de surveillance portent atteinte aux libertés individuelles garanties par le droit conventionnel et constitutionnel, sans qu'il soit ici nécessaire de distinguer entre liberté personnelle, protection des données, protection du domicile, secret des communications, etc. L'Etat n'a donc pas le droit de recourir à des mesures de surveillance, à moins notamment qu'une loi particulière ne l'y autorise. Il s'agit en fait de l'une des conditions à la restriction des droits fondamentaux prévue par la Constitution fédérale et la Convention européenne des droits de l'Homme[7].

---

1 Jean-François Aubert / Pascal Mahon, Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999, Zurich ; Bâle ; Genève 2003, pp 123-135 ; Andreas Auer / Giorgio Malinverni / Michel Hottelier, Droit constitutionnel suisse II, 2ème éd., Berne 2006, pp 184-189 ; Olivier Baum, Rechtliche Fragestellungen im Zusammenhang mit dem kriminalpräventiven Einsatz von Videoüberwachungsanlagen im öffentlichen Raum, 2007, http://jusletter.weblaw.ch/article/fr/_5970?lang=fr ; Giovanni Biaggini, BV: Bundesverfassung der Schweizerischen Eidgenossenschaft und Auszüge aus der EMRK, den UNO-Pakten sowie dem BGG, Zurich 2007, pp 312-134 ; Stéphane Bondallaz, Le « droit à une télécommunication protégée » ou la nécessité de reconsidérer la protection de la vie privée dans les environnements numériques, 2008, ch. 11-17, http://jusletter.weblaw.ch/article/fr/_6256?lang=fr ; Stephan Breitenmoser, Kommentar zu Art. 13 BV, Die schweizerische Bundesverfassung Kommentar, Zurich 2008, pp 190-197 ; Ulrich Häfelin / Walter Haller / Helen Keller, Schweizerisches Bundesstaatsrecht, 7ème éd., Zurich 2008, pp 117-120 ; Regina Kiener / Walter Kälin, Grundrechte, Berne 2007 ; Hanspeter Mock, Le droit au respect de la vie privée et familiale, du domicile et de la correspondance (art.8 CEDH) à l'aube du XXIème siècle, in : Revue universelle des droits de l'Homme 1998, Vol. 10 (7-10), pp 239-240 ; René Rhinow, Grundzüge des schweizerischen Verfassungsrechts, Bâle, Genève, Munich 2003, pp 221-223.

2 Arrêt Amann c. Suisse [GC], no 27798/95, § 65, CEDH 2000-II, résumé in : JAAC 64.144. La Cour a aussi admis que les locaux professionnels peuvent faire partie de la sphère privée, y compris dans le cas d'un employé d'une autorité publique dont le bureau se trouve dans un bâtiment propriété du gouvernement (arrêt Peev c. Bulgarie, no. 64209/01, § 39, du 26 juillet 2007).

3 Arrêt Botta c. Italie, no 21439/93, § 32, CEDH 1998-I, ainsi que S. et Marper c. Royaume-Uni, no 30562/04 et 30566/04, § 45 , du 4 décembre 2008.

4 Par exemple des données d'identification (ATF 124 I 85, 87, Polizeibeamtenverband Basel-Stadt, du 23 avril 1998), des données concernant un traitement médical, l'identité sexuelle (ATF 119 II 264, 268, X., du 3 mars 1993), la participation à une association, les dossiers de procédures judiciaires (ATF 119 Ia 99, 101, H., du 17 mars 1993) ou encore l'adresse IP (ATF 136 II 508, PFPDT c. Logistep SA, du 8 septembre 2010).

5 ATF 122 I 360, 362, B. et consorts, du 28 novembre 1996.

6 Arrêt Rotaru c. Roumanie (exceptions préliminaires) [GC], no 28341/95, § 43, CEDH 2000-V.

7 Ce système est conforme à la tradition continentale, mais diffère fondamentalement du système américain où le champ d'application du IVe Amendement est beaucoup plus limité. Dès lors, une mesure de surveillance qui ne tombe pas sous le champ (limité) du IVe Amendement sera légale à moins qu'une loi particulière ne l'interdise.

2. Les conditions à respecter pour restreindre la sphère privée

[Rz 5] Les droits individuels ne sont pas absolus. Ils peuvent être limités à des conditions précises, qui figurent dans les textes même qui assurent ces droits. La CEDH déclare dans une formule désormais célèbre que l'ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée et familiale n'est admissible que si cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui[8]. Quant à la Cst., elle exige que toute restriction soit fondée sur une base légale, justifiée par un intérêt public ou par la protection d'un droit fondamental d'autrui et proportionnée au but. L'essence des droits fondamentaux (noyau dur) est inviolable et les restrictions graves doivent être prévues par une loi[9].

[Rz 6] La base légale pour les mesures de surveillance dans le cadre de l'investigation pénale n'est autre que le Code de procédure pénale suisse (CPP), entré en vigueur le 1er janvier 2011[10]. La jurisprudence de la Cour européenne des droits de l'Homme et celle du Tribunal fédéral précisent un certain nombre d'exigences que doivent respecter les mesures de surveillance pour que l'atteinte aux droits soit admissible[11]. Premièrement, la surveillance exploratoire ou une surveillance générale et préventive est exclue. Deuxièmement, la surveillance doit être prévisible, c'est-à-dire que la loi autorisant la surveillance doit être accessible et suffisamment précise pour permettre au citoyen de prévoir les conséquences de son comportement. Elle doit user de termes clairs pour indiquer de manière suffisante en quelles circonstances et sous quelles conditions les autorités publiques peuvent prendre des mesures secrètes. Troisièmement, la surveillance doit être autorisée par une autorité judiciaire. Quatrièmement, celui qui est visé par une surveillance doit pouvoir introduire un recours devant une autorité judiciaire indépendante et impartiale. Cinquièmement, des droits doivent être garantis en lien avec les résultats de la surveillance (droit de consulter les enregistrements au plus tard lors de la clôture de l'instruction, conservation des enregistrements intacts jusqu'à la fin du procès pénal, possibilité de faire expertiser les enregistrements et mention des circonstances dans lesquelles les informations obtenues peuvent ou doivent être détruites).

II. La surveillance prévue par le CPP

1. Les mesures de surveillance

[Rz 7] Plusieurs types de mesures de surveillance secrètes figurent dans le chapitre 8 du titre 5 du CPP : surveillance de la correspondance par poste et télécommunication[12], autres dispositifs techniques de surveillance[13], observation[14], surveillance des relations bancaires[15] et investigation secrète[16]. Ces catégories de surveillance sont établies en fonction de l'objet de la surveillance, et, dans une moindre mesure, de l'importance de l'atteinte, plutôt que de la technique utilisée. Ainsi le CPP traite de la surveillance de la correspondance, soit d'un ensemble de moyens de communication pouvant être surveillé, indépendamment de la technique utilisée pour opérer cette surveillance.

[Rz 8] La première catégorie trouve son origine dans la protection du secret postal et des téléphones. La surveillance de la correspondance par poste et télécommunication est probablement la mesure la plus ancienne. Elle englobe l'acquisition de toute information contenue dans une lettre ou un paquet, ainsi que des communications faites par téléphone, téléfax, SMS, MMS, pager, message électronique, téléphonie par Internet (VoIP), etc.[17]. La récolte des données

---

[8] Art. 8 al. 2 CEDH.

[9] Art. 36 Cst., Jean-François Aubert / Pascal Mahon, Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999, Zurich ; Bâle ; Genève 2003, pp 319-331 ; Andreas Auer / Giorgio Malinverni / Michel Hottelier, Droit constitutionnel suisse II, 2ème éd., Berne 2006, pp 79-119 ; Giovanni Biaggini, BV: Bundesverfassung der Schweizerischen Eidgenossenschaft und Auszüge aus der EMRK, den UNO-Pakten sowie dem BGG, Zurich 2007, pp 75-109 ; Peter Goldschmid, Der Einsatz technischer Überwachungsgeräte im Strafprozess: unter besonderer Berücksichtigung der Regelung im Strafverfahren des Kantons Bern, Berne 2001, , pp 23-42 ; Ulrich Häfelin / Walter Haller / Helen Keller, Schweizerisches Bundesstaatsrecht, 7ème éd., Zurich 2008, pp 90-101 ; Walter Haller, The Swiss Constitution in a comparative context, Zurich 2009, pp 157-162 ; René Rhinow, Grundzüge des schweizerischen Verfassungsrechts, Bâle, Genève, Munich 2003, pp 199-206 ; René Rhinow / Markus Schefer, Schweizerisches Verfassungsrecht, 2ème éd., Bâle 2009, pp 237-245 ; Rainer J. Schweizer, Kommentar zu Art. 36 BV, Die schweizerische Bundesverfassung Kommentar, pp 727-742, Zurich 2008, pp 727-742.

[10] La Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) sert de base légale en matière de surveillance préventive, alors que d'autres lois fédérales permettent la création et l'exploitation de bases de données.

[11] Notamment au niveau européen, les arrêts Klass c. Allemagne, du 6 septembre 1978, série A no 28 ; Kruslin c. France, du 24 avril 1990, série A no 176-A ; Dumitru Popescu c. Roumanie (N° 2), no 71525/01, du 26 avril 2007 ; et Natunen c. Finlande, no 21022/04, du 31 mars 2009. Au niveau national, les ATF 120 Ia 314, G., du 27 décembre 1994 ; 122 I 182, T., du 2 mai 1996 ; 125 I 96, 103, A.G., B.G., C.G. et D.G, du 28 janvier 1999 ; 133 IV 182, Ministère public de la Confédération, du 15 mars 2007 ; et 1B_226/2010, du 23 juillet 2010.

[12] Art. 269ss CPP.

[13] Art. 280s CPP.

[14] Art. 282s CPP.

[15] Art. 284s CPP.

[16] Art. 286ss CPP

[17] N'en font pas partie les conversations tenues sur une messagerie publique sur Internet (chat) car elles sont librement accessibles. Le TF ne retient pas un cas de surveillance des télécommunications mais considère que le

secondaires, soit les données relatives au trafic, à la facturation et à l'identification des usagers est une sous-catégorie de la surveillance de la correspondance qui représente une atteinte plus limitée à la sphère privée, étant donné que ces informations ne se rapportent pas au contenu[18].

[Rz 9] Les autres mesures ou autres dispositifs techniques correspondent à ceux qui, avant l'entrée en vigueur du CPP, n'étaient pas couverts par la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication et restaient de la compétence des cantons. C'était les moyens de surveillance qui visaient autre chose que ce qui était protégé par le secret des télécommunications. Cette catégorie est large et contient les dispositifs techniques de surveillance aux fins d'écouter ou d'enregistrer des conversations non publiques, d'observer ou d'enregistrer des actions se déroulant dans des lieux qui ne sont pas publics ou qui ne sont pas librement accessibles, ou de localiser une personne ou une chose[19].

[Rz 10] L'observation est la surveillance d'événements et de personnes sur la voie publique. Elle se définit par l'espace surveillé mais ne précise pas les moyens techniques utilisables. Elle doit revêtir une certaine durée et un caractère systématique. Elle inclut également l'enregistrement des résultats en vue de leur utilisation dans le cadre de la poursuite pénale[20].

[Rz 11] L'investigation secrète est une mesure de surveillance particulière car elle implique le comportement actif de la police. L'agent infiltré va non seulement constater une situation et recueillir des preuves, mais il va également interagir avec les personnes surveillées[21].

[Rz 12] Quelques mesures peuvent encore être utilisées comme des mesures de surveillance, bien qu'elles figurent dans des dispositions éparses du chapitre consacré aux mesures de contrainte, comme la recherche de personnes[22], l'analyse d'ADN[23], la récolte de données signalétiques[24] ainsi que la récolte d'échantillons d'écriture ou de voix[25]. Elles ne sont pas abordées ici par souci de concision.

[Rz 13] Lorsque l'autorité de poursuite pénale entend recourir à une surveillance, elle doit choisir la mesure technique qu'elle souhaite utiliser et regarder à quelle catégorie légale cette mesure appartient pour savoir quelles sont les conditions à respecter et la procédure à suivre. Cela ne soulève aucun problème pour la plupart des mesures actuelles de surveillance, qu'elles soit clairement visées par le texte du CPP ou que la jurisprudence ait eu l'occasion de les confirmer.

[Rz 14] En revanche, le législateur n'a pas indiqué ce qu'il entendait faire de l'évolution future de la technique et il a oublié certaines mesures de surveillance déjà existantes. Il y a certes la disposition sur les autres dispositifs de surveillance prévus par l'art. 280 CPP. Cet article vise d'abord l'utilisation de micros, caméras et balises GPS. Le législateur n'ayant rien prévu de particulier pour les nouveaux moyens techniques, l'art. 280 CPP sera vraisemblablement utilisé de manière extensive dans un avenir proche pour les moyens qui n'existaient pas au moment de l'adoption du CPP et qui peuvent correspondre à sa définition.

[Rz 15] Lorsqu'une mesure technique de surveillance n'appartient pas clairement à une catégorie prévue, mais qu'elle existait déjà au moment de l'adoption du CPP, il convient de se demander si le législateur a voulu l'exclure (silence qualifié), s'il a oublié de l'intégrer (lacune) ou encore s'il a considéré qu'elle était intégrée dans une catégorie existante. Il n'est pas possible d'apporter une réponse globale et certaine à ces questions, les voix du législateur demeurant plutôt impénétrables. Bien plus faut-il essayer de déterminer son intention et recourir aux méthodes habituelles d'interprétation.

---

policier qui suit la conversation de manière générale sans se concentrer en particulier sur certains participants est dans la même situation qu'un policier patrouillant en civil (ATF 134 IV 266, 278, Oberstaatsanwaltschaft des Kantons Zürich, du 16 juin 2008). Celui qui ne se contente pas de lire la conversation mais y prend part sera considéré comme un agent infiltré (Beat Rhyner / Dieter Stüssi, Kommentar zu Art. 269-279 StPO, VSKC-Handbuch, Zurich 2008, p. 443 ; Beat Rhyner / Dieter Stüssi, Kommentar zu Art. 286-298 StPO, VSKC-Handbuch, Zurich 2008, pp 498-499).

18 Art. 273 CPP,

19 Art. 280 CPP. L'enregistrement audio ou vidéo dans un lieu librement accessible au public est soumis aux dispositions concernant l'observation (Nicolas Dubuis, Note sur les mesures de surveillance optique par caméra en procédure pénale, in : Revue valaisanne de jurisprudence (RVJ) 2009, p. 211). La surveillance vidéo ou la photographie d'une cabine téléphonique n'est pas un cas de surveillance de la correspondance, mais bien un cas d'usage d'un autre dispositif technique (Thomas Hansjakob, Die ersten Erfahrungen mit dem Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), in : Revue pénale suisse 2002, Vol. 120 (3), p. 268).

20 Gianfranco Albertini, Tableaux synoptiques des enquêtes de police : moyen d'instruction et de travail élaboré par l'Association des chefs de police judiciaire suisses relative à l'investigation policière selon le code de procédure pénale suisse, Zurich 2009, p. 1235 ; Conseil fédéral, Message relatif à l'unification du droit de la procédure pénale du 21 décembre 2005 FF 2006 1057-1372,; Frédéric Gisler, La coopération policière internationale de la Suisse en matière de lutte contre la criminalité organisée, Gauch, Peter (Ed.), Travaux de la Faculté de droit de l'Université de Fribourg, Zurich 2009, pp 87-90 ; Olivier Guéniat / Frédéric Hainard, Commentaire ad art. 282-283 CPP, Commentaire romand du Code de procédure pénale, Bâle 2011, n 1 ad art. 282 ; Beat Rhyner / Dieter Stüssi, Kommentar zu Art. 282-283 StPO, VSKC-Handbuch, Zurich 2008, pp 471-474 ; Niklaus Schmid, Schweizerische Strafprozessordnung, Praxiskommentar, Zurich 2009, pp 533-535. Si les événements enregistrés n'ont pas lieu sur la voie publique, ce sera un cas d'autres dispositifs techniques de surveillance. L'observation se distingue de l'investigation secrète car elle n'a pas lieu (passivement) à distance mais elle implique un comportement actif du policier infiltré dans un milieu déterminé (ATF 134 IV 266, 270, Oberstaatsanwaltschaft des Kantons Zürich, du 16 juin 2008.)

21 Voir note de bas de page 1.

22 Art. 210 CPP

23 Art. 255ss CPP.

24 Art. 260s CPP.

25 Art. 262 CPP.

[Rz 16] Une interprétation grammaticale de l'art. 280 CPP laisse penser que seuls les dispositifs utilisés pour écouter, observer ou localiser sont couverts par cet article. Une interprétation historique permet en revanche d'admettre que l'écoute, l'observation et la localisation sont plutôt des exemples et que le législateur a plutôt voulu créer une sorte de base légale subsidiaire pour les techniques qui ne correspondent pas aux types de surveillance énumérés préalablement[26]. L'interprétation systématique va également dans ce sens puisque la disposition concernant les autres techniques de surveillance suit immédiatement la surveillance de la correspondance. Jusqu'à l'entrée en vigueur du CPP, la surveillance de la correspondance était soumise à la LSCPT, alors que tous les autres dispositifs techniques de surveillance relevaient du droit cantonal de procédure[27]. A moins que la nouvelle technique ne se rapproche plus spécifiquement d'une autre disposition, l'art. 280 CPP sera en quelque sorte la base légale par défaut pour les mesures qui ne visent ni la correspondance, ni les relations bancaires, ni l'espace public (observation). Il en va différemment des méthodes déjà connues mais oubliées par le CPP, car il faut d'abord vérifier que le législateur n'a pas voulu les exclure, puis cas échéant trouver un moyen de les intégrer dans les dispositions légales existantes.

2. Les conditions et la procédure

[Rz 17] Les mesures de surveillance sont ordonnées selon des procédures différentes en raison de l'atteinte portée à la personne surveillée : plus l'atteinte est importante, plus l'autorité qui autorise la surveillance sera indépendante.

[Rz 18] Ainsi une procédure « simplifiée » permet à la police ou au ministère public d'ordonner les mesures de surveillance portant le moins atteinte à la personne, sans devoir recueillir l'autorisation d'une autorité supérieure. Une observation ne dépassant pas un mois peut être ordonnée simplement par la police, alors que le ministère public devra l'autoriser si elle s'étend au-delà d'un mois[28].

[Rz 19] La procédure « classique » est celle que prévoyait la LSCPT avant l'entrée en vigueur du CPP : les mesures sont ordonnées par le ministère public puis autorisées par le tribunal des mesures de contrainte. Sa décision doit intervenir dans les cinq jours suivants le début de la surveillance et elle a un effet rétroactif. La décision du ministère public n'a donc qu'un effet provisoire, même si elle est immédiatement exécutoire. L'exploitation des résultats de la surveillance ne sera pourtant pas possible si le tribunal des mesures de contrainte n'accorde pas l'autorisation demandée. Cette procédure s'applique à la surveillance de la correspondance, à l'obtention de données accessoires, à l'utilisation d'autres dispositifs de surveillance et à l'investigation secrète.[29].

[Rz 20] Troisièmement, la procédure « compliquée » (et surprenante) qui régit la surveillance des relations bancaires. Selon le texte français du CPP, le tribunal des mesures de contrainte peut autoriser la surveillance, alors que les versions allemande et italienne de l'art. 284 CPP parlent d'ordonner la surveillance. Le tribunal des mesures de contrainte doit également définir les modalités d'exécution en se fondant sur la requête du ministère public[30]. La surveillance des relations bancaires ne débuterait alors qu'avec la décision du tribunal des mesures de contrainte. Aucun délai ne lui est pourtant imparti pour statuer sur la proposition du ministère public[31]. Logiquement, la procédure aurait dû être la même que pour la surveillance de la correspondance et les autres mesures. D'ailleurs, comme il s'agit d'une surveillance en temps réel (nous le verrons ci-après), il serait certainement plus sage d'appliquer par analogie, la procédure appliquée pour la surveillance de la correspondance. Le tribunal des mesures de contrainte autoriserait la surveillance que le ministère public aurait précédemment ordonnée. Conformément à la version française, la surveillance serait effective dès la décision du ministère public[32].

[Rz 21] Les conditions à remplir pour mettre en place une surveillance dépendent également du type de mesures, même si l'exigence de soupçons suffisants laissant présumer la commission d'une infraction, de proportionnalité et de subsidiarité sont applicables dans tous les cas. La poursuite d'un délit ou d'un crime ouvre la voie à la surveillance des relations bancaires, l'observation, et la récolte des données relatives au trafic, à la facturation et à l'identification des usagers[33]. Pour permettre la surveillance de la correspondance par poste et télécommunication, ou une autre mesure

[26] Conseil fédéral, Message relatif à l'unification du droit de la procédure pénale du 21 décembre 2005 FF 2006 1057-1372.

[27] Les soumettant selon les cantons par analogie à la procédure de la LSCPT ou considérant que la procédure cantonale pouvait être différente.

[28] Art. 282 CPP.

[29] Art. 274 et 289 CPP.

[30] Conseil fédéral, Message relatif à l'unification du droit de la procédure pénale du 21 décembre 2005 FF 2006 1057-1372.

[31] Contrairement à la surveillance de la correspondance qui prévoit des délais brefs de vingt-quatre heures pour transmettre le dossier et cinq jours pour statuer. Des délais courts s'imposent vu que la surveillance est déjà en cours.

[32] Cela se justifie aussi parce que le CPP ne prévoit pas comment le tribunal des mesures de contrainte doit ordonner les mesures qu'il prend à la demande du ministère public, contrairement à la procédure d'autorisation des mesures ordonnées par le ministère public. Les délais impartis au ministère public pour transmettre le dossier et au tribunal des mesures de contrainte pour statuer, la durée maximale de la surveillance ou encore le sort de découvertes fortuites ne sont pas prévus en matière de surveillance bancaire. Cette lacune doit être comblée par une application par analogie des normes régissant la surveillance de la correspondance.

[33] Lors d'une procédure visant l'utilisation abusive d'une installation de télécommunications (art. 179septies CP), les données relatives au trafic, à la facturation et à l'identification des usagers peuvent être obtenues (art CPP). Cela se justifie par l'objet de l'infraction, même s'il s'agit seulement d'une contravention (art. 273 al. 1 CPP).

technique de surveillance, l'infraction poursuivie doit en revanche figurer dans une liste exhaustive de contraventions, délits et crimes mentionnés à l'art. 269 al. 2 CPP. La personne surveillée doit être informée à l'issue de la surveillance, ce qui ouvre également la voie à une procédure judicaire de contrôle[34].

III. Quelques techniques difficiles à classer

1. La surveillance des relations bancaires en temps réel

[Rz 22] Les articles 284ss CPP ne décrivent pas ce que le législateur entend par la surveillance des relations bancaires. A l'examen des travaux préparatoires, on se rend compte que l'intérêt de ces dispositions sur la surveillance des relations bancaires, soit la surveillance en temps réel, a été perdu de vue. Les autres informations et documents peuvent en effet être réclamés par une simple injonction de dépôt ou une mesure de séquestre et il est inutilement compliqué d'imposer l'autorisation du tribunal des mesures de contrainte pour obtenir des extraits de comptes bancaires alors que le ministère public continue à être compétent pour les perquisitions et les séquestres.

[Rz 23] La surveillance des relations bancaires est aussi la concrétisation de l'art. 4 de la Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime[35] qui mentionne les techniques spéciales (ordonnances de surveillance de comptes bancaires, observation, interception de télécommunications, accès à des systèmes informatiques et ordonnances de production de documents déterminés).

[Rz 24] Avec l'autorisation qu'il accorde, le tribunal des mesures de contrainte doit donner des directives écrites à la banque sur le type d'informations et de documents à fournir, de même que les mesures visant à maintenir le secret qu'elle doit observer. Si la banque est vraisemblablement tenue de disposer des informations qui lui seront demandées dans le cadre des obligations découlant du droit bancaire, il aurait mieux valu régler à l'avance et de manière générale ces questions, comme en matière de surveillance de la correspondance. Les conséquences de l'impossibilité pour une banque de fournir certaines informations ne sont pas résolues. Des compétences pratiques et la compétence d'adopter des directives techniques auxquelles les banques devraient se conformer pourraient être accordées au Service de surveillance de la correspondance et des télécommunications(Service SCPT) dans le cadre d'une modification légale[36]. Ainsi une véritable surveillance en temps réel serait mise en place au lieu de demandes continuelles de documents dont les résultats dépendront tout autant de l'établissement bancaire sollicité que du tribunal requérant.

2. L'IMSI-Catcher

[Rz 25] L'IMSI-Catcher est un appareil simulant une antenne relais GSM dans le but de se placer entre l'antenne authentique et le téléphone portable. Cet appareil permet, sans aucune intervention de l'opérateur téléphonique, d'intercepter les numéros IMSI et IMEI à une portée pouvant aller jusqu'à plusieurs kilomètres, de localiser les appareils dans cette zone et même parfois d'écouter les conversations téléphoniques[37].

[Rz 26] Il doit être considéré comme une mesure de surveillance de la correspondance, puisque c'est une transmission de données par le truchement de techniques et d'installations de communications qui est visée, et cela même si le concours de l'opérateur ou du Service SCPT n'est pas nécessaire. Ce sera aussi le cas si l'IMSI-Catcher est utilisé uniquement pour localiser un téléphone, car ce n'est pas tant l'objet qui est localisé mais plutôt sa position par rapport au système de communication qui est recherché.

3. Les puces RFID

[Rz 27] Un système RFID[38] se base sur la propagation d'ondes radio. Il est composé d'un marqueur et d'un lecteur. Le marqueur RFID est passif. Il contient une petite quantité de mémoire pour la conservation des données et ne nécessite pas d'énergie. Le lecteur est actif et alimente les marqueurs présents dans son champ pour lire leurs données[39].

[Rz 28] Chaque fois que le marqueur se trouve à proximité d'un lecteur RFID, le lecteur détecte sa présence et peut lire les données qu'il contient. Le faible coût des puces RFID les rend particulièrement intéressantes pour marquer plusieurs

---

[34] Art. 279 CPP.

[35] RS 0.311.53.

[36] Actuellement rattaché au Centre de services informatiques du Département fédéral de justice et police CSI-DFJP.

[37] L'IMSI-Catcher est également connu sous le nom de Triggerfish. Sophie de Saussure, Le IMSI-Catcher : fonctions, applications pratiques et légalité, 2009, http://jusletter.weblaw.ch/article/fr/_7875?lang=fr, ch. 1-22 ; Ulrich Eisenberg, Beweisrecht der StPO Spezialkommentar, 6, Munich 2008, pp 906-907.

[38] Radio Frequency Identification ou identification par radiofréquences.

[39] Commission d'accès à l'information du Québec (CAI), La technologie d'identification par radiofréquence (RFID), doit-on s'en méfier ? , Québec 2006 ; Klaus Finkenzeller, RFID-Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, 3ème éd., 2010 ; Steve Hodges / Duncan McFarlane, RFID : le concept et l'incidence, L'économie de la sécurité, Paris 2004, pp 62-65 ; Préposé fédéral à la protection des données et à la transparence (PFPDT), 17ème rapport d'activités 2009/2010, Berne 2010, pp 34-36.

objets et être informé de leurs passages à des points de contrôle donnés.

[Rz 29] La détection de puces RFID correspond parfaitement à un moyen de localisation tel que visé par les autres dispositifs de surveillance. La localisation d'une puce RFID ne recourt en effet pas à une infrastructure de télécommunications, contrairement à la localisation d'un numéro IMSI qui est précisément un identifiant de l'usager du réseau de téléphonie mobile, et cela indépendamment de savoir où est placée la puce RFID.

4. Le cheval de Troie

[Rz 30] Un « cheval de Troie » ou « Government-Software » est un programme informatique que l'on introduit dans l'ordinateur cible sous une apparence anodine et/ou sans que le propriétaire ne s'en rende compte. Ce programme peut alors prendre le contrôle de la machine et accéder aux informations qu'elle contient. Dans le cadre de la procédure pénale, le « cheval de Troie » est en particulier utilisé pour intercepter des communications entre deux ordinateurs (messagerie, VoIP, etc.)[40]. Les résultats peuvent être transmis en temps réel ou sous la forme de rapports périodiques. Le « cheval de Troie » peut revêtir des formes et des buts variés, au point qu'il est difficile d'en définir un type précis.

[Rz 31] Il n'y a à ce jour pas de réponse définitive quant à savoir si le CPP permet ou non l'installation d'un « cheval de Troie ». Cette question est d'autant plus difficile à résoudre en fonction des nombreux visages que peuvent avoir ces logiciels. Si rien n'indique que le CPP a voulu exclure cette méthode de surveillance, il est difficile de la classer définitivement comme étant une mesure de surveillance de la correspondance ou un autre dispositif de surveillance. Jusqu'à l'entrée en vigueur du CPP, la doctrine était partagée sur cette question mais considérait plutôt qu'il s'agissait d'un autre dispositif de surveillance parce qu'elle concernait la surveillance d'un ordinateur par opposition aux écoutes téléphoniques opérées par les PTT, puis les opérateurs téléphoniques.

[Rz 32] L'avant-projet de révision de la LSCPT prévoit d'ajouter au CPP un article 270bis qui autoriserait l'introduction dans un système informatique de programmes informatiques à l'insu de la personne surveillée dans le but d'intercepter et de lire des données. Le Conseil fédéral a eu l'occasion de préciser que cela concerne uniquement la surveillance de la correspondance et non des perquisitions à distance. La procédure serait semblable à celle de la surveillance de la correspondance et le ministère public devrait préciser quel type de données il souhaite obtenir. Même s'il n'est pas nécessaire, ce nouvel article aurait l'avantage de préciser quel type de programme informatique est admissible et à quelles conditions. Le projet de loi et le message ne sont toutefois pas attendus avant l'année prochaine.

[Rz 33] Actuellement, lorsqu'un « cheval de Troie » est placé dans un téléphone ou un ordinateur relié à un réseau de communication (Internet par exemple), il faut le considérer comme une mesure de surveillance de la correspondance : on surveille la transmission d'informations par le biais d'installations et de techniques de communication[41]. Il n'y a pas de différence que le logiciel espion soit placé sur un téléphone mobile ou sur un ordinateur fixe ou portable. Sachant que d'autres données que les données transmises dans le cadre de la communication visée peuvent techniquement aussi être récoltées, l'ordre de surveillance doit indiquer précisément ce qui est recherché et quels modes de communications sont visés (messagerie électronique, logiciel de téléphonie, session internet, etc.). Cela évite une surveillance disproportionnée et ainsi non conforme. Les informations qui seraient obtenues en plus de ce qui est surveillé, par exemple parce qu'il ne serait pas techniquement possible de séparer les flux de données, sont inexploitables. Lorsque des limites techniques ne peuvent pas être imposées, il est toujours possible de mettre des limites juridiques.

[Rz 34] L'environnement d'un ordinateur peut être surveillé par le biais d'une webcam ou d'un micro actionné par un « cheval de Troie ». La situation est alors semblable au fait de placer des caméras et micros dans une chambre, ce que permet l'art. 280 CPP.

[Rz 35] Le « cheval de Troie » pourrait finalement être utilisé, d'un point de vue technique, pour infiltrer une machine et en retirer des informations enregistrées. Les mesures techniques de surveillance se distinguent d'une perquisition qui répond à des règles et des conditions différentes, en particulier le fait que le détenteur doit être informé préalablement à la perquisition et qu'il a le droit de demander à ce que soit mises sous scellés des informations qui ne peuvent être ni examinées, ni exploitées par les autorités pénales. Une perquisition à distance et à l'insu de la personne visée est interdite. Cela n'empêche pas l'utilisation d'un logiciel informatique pour fouiller un ordinateur lors d'une perquisition, mais l'intéressé doit en être informé et les dispositions en matière de perquisitions et de séquestre doivent être respectées[42].

[Rz 36] L'art. 280 CPP vise les dispositifs techniques de surveillance qui permettent d'écouter ou d'enregistrer des conversations non publiques, d'observer ou d'enregistrer des actions dans des lieux qui ne sont pas publics ou de localiser une personne ou une chose. Ces mesures de surveillance

[40] Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, in : Jusletter 5 décembre 2011.

[41] L'ordinateur relié à un réseau (par câble, modem ou autre) est une installation de communication : Bernhard Sträuli, La surveillance de la correspondance par poste et télécommunication : aperçu du nouveau droit, Mehr Sicherheit – weniger Freiheit? Ermittlungs- und Beweistechniken hinterfragt = Plus de sécurité – moins de liberté ? Les techniques d'investigation et de preuve en question, Zurich ; Coire 2003, pp 101-102.

[42] Art. 241ss et 263ss CPP.

appréhendent des faits qui se déroulent en temps réel, à distinguer de données enregistrées comme les fichiers d'un ordinateur. A mi-chemin entre la surveillance des communications et la perquisition de l'ordinateur pourrait se trouver la surveillance de l'activité de l'ordinateur (activité de certains programmes, etc.). On pourrait éventuellement se trouver en présence d'un cas couvert par l'art. 280 CPP, mais il faudrait examiner précisément l'objet de la surveillance et le fonctionnement du logiciel pour donner une réponse claire.

[Rz 37] Thomas Hansjakob relève que l'introduction du « cheval de Troie » est prohibée par l'art. 143bis CP (accès indu à un système informatique) et qu'une base légale spéciale est nécessaire[43]. Un argument au moins s'oppose à cette analyse. Lorsque la police installe des micros et caméras (autres dispositifs de surveillance), l'introduction dans les locaux ou véhicules n'est pas considérée comme une violation de domicile au sens de l'art. 186 CP. Si s'introduire dans un local pour y placer un micro fait partie des actes autorisés par le CPP dans le cadre d'une surveillance, s'introduire dans un ordinateur devrait l'être aussi. Finalement, un policier agissant en respectant la procédure des art. 269ss CPP ne serait probablement pas sanctionné pour un d'accès indu à un système informatique, car il pourrait se réfugier derrière un acte autorisé par la loi au sens de l'art. 14 CP[44].

[Rz 38] Ainsi le « cheval de Troie » utilisé pour surveiller l'environnement de la machine doit suivre les règles prévues pour les autres dispositifs techniques, alors que celui qui est utilisé pour surveiller des communications doit obéir aux règles en matière de surveillance de la correspondance. L'ordre de surveillance du procureur, respectivement l'autorisation du tribunal des mesures de contrainte, devront être très précis sur ce qui est recherché et autorisé. Les mesures techniques nécessaires doivent aussi être prises pour garantir l'authenticité et l'intégrité des données.

IV. Conclusion

[Rz 39] Le Code de procédure pénale entré en vigueur le 1er janvier 2011 prévoit une procédure et des conditions précises pour mettre en place des mesures techniques de surveillance, respectant ainsi les exigences découlant de la protection de la sphère privée garantie par la Constitution fédérale et la Convention européenne des droits de l'Homme. Le CPP regroupe les mesures de surveillance en catégories en fonction de l'objet visé par la surveillance. Le procureur, respectivement le juge, doit vérifier que la technique prévue appartient à l'une de ces catégories et que les conditions légales sont respectées.

[Rz 40] Les mesures les plus anciennes sont facilement rattachées à la bonne catégorie, alors que les plus récentes sont parfois discutées. Parmi celles-là, on peut retenir que la surveillance des relations bancaires permet la transmission d'informations en temps réel, que l'IMSI-Catcher est une mesure de surveillance de la correspondance et que les puces RFID sont un moyen essentiellement de localisation et doivent être autorisées comme un autre dispositif de surveillance. Quant au « cheval de Troie », on propose de considérer en premier l'objet visé par ce moyen de surveillance. Lorsque la surveillance porte sur la correspondance par communications, le « cheval de Troie » est admissible et doit répondre aux règles en matière de surveillance de la correspondance. Lorsqu'il sert à observer l'environnement de l'ordinateur (son et images), c'est un autre dispositif de surveillance, également admissible s'il répond aux conditions prévues pour cette catégorie. En revanche, le « cheval de Troie » ne peut pas être utilisé pour effectuer une perquisition à distance, les conditions légales de l'autorisant pas.

Sylvain Métille est avocat et docteur en droit. Il est notamment l'auteur d'une thèse de doctorat intitulée « Mesures techniques de surveillance et respect des droits fondamentaux, en particulier dans le cadre de l'instruction pénale et du renseignement » ainsi que du blog « Nouvelles technologies et droit ».

---

* * *

[43] Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, in : Jusletter 5 décembre 2011.

[44] ATF 100 IB 13, Ligue marxiste révolutionnaire, du 8 mars 1974.