Sylvain Métille

Mesures techniques de surveillance et respect des droits fondamentaux

en particulier
dans le cadre de l'instruction pénale et du renseignement

Sylvain Métille

Docteur en droit,
Titulaire du brevet d'avocat

Mesures techniques de surveillance et respect des droits fondamentaux

en particulier
dans le cadre de l'instruction pénale et du renseignement

COLLECTION NEUCHÂTELOISE
Helbing Lichtenhahn

Thèse de doctorat
de la Faculté de droit de l'Université de Neuchâtel
soutenue le 14 septembre 2010

FACULTÉ DE DROIT

Information bibliographique de la Deutsche Nationalbibliothek

La Deutsche Nationalbibliothek a répertorié cette publication dans la Deutsche Nationalbibliografie ; les données bibliographiques détaillées peuvent être consultées sur Internet à l'adresse http://dnb.d-nb.de.

ISBN 978-3-7190-3060-5

www.helbing.ch

www.unine.ch

« La justice sans la force est impuissante ; la force sans la justice est tyrannique.

La justice sans force est contredite, parce qu'il y a toujours des méchants ; la force sans justice est accusée. Il faut donc mettre ensemble la justice et la force, et pour cela faire que ce qui est juste soit fort, ou que ce qui est fort soit juste. »,

Blaise PASCAL, *Pensées*

Remerciements

Par ces quelques lignes, je souhaite exprimer ma reconnaissance et ma gratitude à tous ceux qui m'ont apporté leur soutien, régulièrement ou occasionnellement, de près ou de plus loin. Que mes parents, qui n'ont jamais douté et ont toujours été présents durant toutes ces années, soient ici particulièrement remerciés.

Mes remerciements vont également à tous ceux qui m'ont ouvert leur porte et avec qui j'ai eu l'occasion de discuter des sujets abordés dans ma thèse, qu'il s'agisse de juristes ou de professionnels confrontés au quotidien à des questions liées à la surveillance. C'est ici aussi le lieu de remercier les membres du jury de thèse : le Professeur Pascal MAHON dont la relecture attentive et le souci du détail n'ont pas d'égal, le Professeur André KUHN et son regard bienvenu de pénaliste, ainsi que le Professeur Alexandre FLÜCKIGER, qui a accepté la tâche pas toujours évidente de rapporteur externe.

Sommaire

Première partie :
introduction et notions techniques

I. Introduction

Les mesures de surveillance sont aujourd'hui très présentes et il n'est plus rare d'être filmé, observé, écouté ou encore lu au quotidien. L'enregistrement de données publiées sur des sites en ligne ou la vidéosurveillance en sont deux exemples. Ces mesures de surveillance peuvent être mises en place par les pouvoirs publics mais également par des personnes privées. Les connaissances techniques actuelles et leur constante évolution rendent facilement accessibles les appareils et les méthodes de surveillance qui étaient auparavant coûteuses et compliquées. La copie, le transfert et la modification de données numérisées sont maîtrisés depuis longtemps, comme la possibilité d'y accéder n'importe quand et depuis n'importe où. De nombreuses tâches de surveillance sont désormais automatisées et les possibilités de rendre la surveillance invisible sont toujours plus nombreuses. 1

La pratique de la surveillance ne pouvant être réduite à un seul domaine juridique, la présente recherche se situe à la croisée du droit constitutionnel et de la procédure pénale. Elle se veut aussi un lien entre la théorie et la pratique en se concentrant sur les acteurs, qu'ils soient à l'origine de la mesure de surveillance ou qu'ils en fassent l'objet. Certaines digressions et analyses théoriques sont toutefois nécessaires, de même que certaines considérations d'ordre technique. C'est donc presque naturellement que le présent ouvrage débute avec la présentation des principales possibilités techniques de surveillance et des droits individuels qui pourraient être mis en péril par ces mesures de surveillance. Le choix a ensuite été fait de se concentrer sur la procédure pénale, pour aborder ensuite la surveillance préventive et, brièvement, faire état des principales bases de données utilisées pas les autorités policières et judiciaires. Afin de ne pas survoler le sujet ni d'y perdre le lecteur, les cas de surveillance privée ne sont pas abordés, mais quelques renvois ou quelques brèves réflexions sont mentionnés lorsqu'ils ont paru nécessaires. 2

Le cœur de l'analyse concerne la procédure pénale parce que c'est là que les méthodes de surveillance les plus invasives sont autorisées, mais aussi en raison de la nouveauté des dispositions légales qui entreront en vigueur le 1er janvier 2011. Une bonne partie des réflexions pourront être reprises, *mutatis mutandis*, 3

pour la surveillance préventive. Dans ce cadre, le présente ouvrage présente le système en vigueur et, comme pour les bases de données, s'intéresse à la question du droit d'accès de l'individu.

4 La doctrine, du moins francophone, ne s'est guère penchée sur les questions de surveillance jusqu'à ce jour. On trouve certes un commentaire très complet de la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) en allemand[1], mais ces dispositions seront pour l'essentiel remplacées par le nouveau Code de procédure pénale fédérale (CPP) dont l'entrée en vigueur est prévue au 1er janvier 2011[2]. La littérature est encore moins abondante, comme les décisions de justice et les informations officielles, en ce qui concerne la surveillance préventive. Il était donc nécessaire d'aborder au moins les principaux aspects de ce type de surveillance. Au titre des difficultés, il faut encore relever l'évolution législative importante (et inachevée) durant la rédaction de cet ouvrage, même si cette évolution n'a pas suivi le rythme des progrès techniques.

5 La doctrine, la jurisprudence, les lois et projets de lois ont été pris en compte jusqu'au 15 juillet 2010, à l'exception des contributions du Commentaire romand du Code de procédure pénale[3] auquel les auteurs et éditeurs m'ont aimablement laissé accès avant sa parution, et un article à paraître prochainement d'Alexandre FLÜCKIGER[4]. Lorsque des ouvrages étaient annoncés, mais pas encore disponibles à cette date, ils sont mentionnés dans la bibliographie sans détails d'éditeur et de date.

[1] HANSJAKOB, *BÜPF und VÜPF Kommentar*.

[2] Le CPP fera évidemment l'objet de plusieurs commentaires généraux, mais aucun ouvrage n'est annoncé s'agissant précisément des mesures de surveillance.

[3] KUHN / JEANNERET, *CR-CPP*.

[4] FLÜCKIGER, *Droits fondamentaux et vidéosurveillance*.

II. Propos et limites de l'étude

A. Définitions et délimitations du sujet

1. Surveillance technique et exploitation de données

Par mesure technique de surveillance (Überwachung mit technischen Überwachungsgeräten), nous entendons toute méthode utilisée par l'homme au moyen d'un appareil lui permettant d'écouter, d'observer, de localiser, d'identifier ou de recueillir de n'importe quelle manière des informations sur un individu, un objet ou un lieu[5]. Le processus est fréquemment automatisé, en tout ou partie, mais cela ne représente pas un critère déterminant pour autant. L'observation à la lunette ou l'écoute d'une conversation en se branchant directement sur le câble téléphonique ou simplement à l'aide d'un appareil amplificateur de son sont des mesures techniques de surveillance, bien qu'elles ne revêtent aucun caractère automatique. 6

La personne surveillée n'a le plus souvent pas conscience de la surveillance dont elle est l'objet. L'absence de connaissance de la surveillance n'est cependant pas une exigence, ni son seul intérêt, puisque de nombreuses mesures de surveillance sont connues de la personne surveillée et atteignent parfaitement leur but, soit que cette dernière n'y prête pas suffisamment attention, en néglige la portée, ou encore se croie hors d'atteinte[6]. Les caméras de surveillance mises bien en évidence et signalées dans un magasin ou le contrôle annoncé préalablement du courrier des détenus en sont des exemples évidents. Le caractère secret de la surveillance a toutefois pour conséquence qu'il n'est pas possible de s'en protéger seul[7]. A la difficulté de contrer une mesure que l'on ne connaît pas s'ajoute l'impossibilité de contrôler les conditions dans lesquelles la 7

[5] L'expression « mesure de surveillance technique » est aussi utilisée. Pour une définition légèrement plus restrictive : GISLER, *La coopération policière*, p. 90; RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, pp 435-436.

[6] Pour des exemples de mesures de surveillance visibles : CUSSON, *La surveillance et la contre-surveillance*, pp 429-432. Voir également le chapitre 2. La surveillance dissuasive, p. 84 ci-dessous.

[7] WEICHERT, *Überwachung: Einblick in die Praxis*, p. 5.

surveillance est opérée. Contrairement à une fouille par exemple, la personne visée ne sait, ni ne voit, les actes de la police lorsque la surveillance est secrète. Celui qui est surveillé n'a pas la possibilité de s'opposer immédiatement ou de demander des explications.

8 Certains auteurs retiennent cependant une définition plus étroite des mesures techniques de surveillance et font du caractère secret un élément déterminant[8]. Le Code de procédure pénale traite des mesures secrètes de surveillance dans un chapitre, mais d'autres mesures techniques de surveillance, au sens où nous l'entendons, sont traitées de manière éparse[9]. Au vu du nombre croissant d'installations privées et publiques de surveillance, qui ne sont pas secrètes, il est nécessaire de les inclure dans les moyens techniques de surveillance.

9 C'est bien souvent le caractère secret de la mesure qui en fait l'intérêt principal, mais qui suscite également le plus de questions. En effet, la procédure étant secrète, il est difficile pour l'individu de faire respecter ses droits. Les résultats de la surveillance peuvent ensuite être stockés et constituer une base de données, dans laquelle une recherche pourra être effectuée ultérieurement. Il s'agit là aussi d'un moyen technique de surveillance.

10 Le Comité d'experts du Conseil de l'Europe sur les techniques spéciales d'investigation en relation avec les actes de terrorisme (PC-TI) a défini les techniques spéciales d'enquêtes « comme étant des techniques ayant pour but de recueillir systématiquement des informations de telle sorte que la/les personne(s) visée(s) ne soi(en)t pas alertée(s). Ces techniques sont appliquées par les représentants de la loi dans le but de dépister des crimes et des suspects et d'enquêter sur ceux-ci »[10]. Cela recouvre entre autres les opérations sous couverture[11], informateurs, livraisons surveillées, surveillances électroniques, écoutes et interceptions de communications, fouilles et perquisitions, poursuites

[8] GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, p. 45.

[9] Voir à ce sujet le chapitre 3. Les mesures de contrainte assimilables aux mesures de surveillance, p. 155 ci-dessous.

[10] PC-TI, *Rapport final d'activités sur les techniques spéciales d'investigation*, § 19.

[11] Les opérations sous couverture sont menées par des agents infiltrés dans le milieu criminel, dont l'identité et la qualité réelles ne sont pas reconnaissables. Ils utilisent en principe une identité d'emprunt. Leur engagement est notamment régi par la Loi fédérale sur l'investigation secrète (RS 312.8).

transfrontalières, agents provocateurs, etc.[12]. Il s'agit là d'un cadre bien plus large que celui des mesures techniques de surveillance. Le projet de révision de la Loi instituant des mesures visant au maintien de la sûreté intérieure parle de moyens spéciaux de recherche d'information (Besondere Mittel der Informationsbeschaffung). Cette dénomination est souvent utilisée en matière de renseignement, celle de surveillance technique étant préférée en matière pénale, bien que ces notions soient similaires.

L'informatique a apporté un nouveau développement des moyens de surveillance, notamment en permettant le traitement automatique des données, leur stockage et leur mise en réseau. Les mêmes données peuvent être accessibles instantanément en tous lieux, et les capacités de stockage semblent ne plus avoir de limites. 11

L'exploitation de données regroupe toutes les utilisations qui peuvent être faites des données brutes : sélection et tri des informations pertinentes, traduction et conversion dans d'autres formats, analyse et recoupement avec d'autres données, diffusion, etc. Les données sont habituellement enregistrées dans des fichiers, soit un système structuré de classement de l'information, généralement appelé base de données[13]. Une base de données peut revêtir des formes très diverses. La plupart du temps, elle permet de relier entre elles les informations qu'elle contient, voire les relier avec des données contenues ailleurs. Consultable par de multiples utilisateurs simultanément, elle est le plus souvent dotée d'un système permettant d'effectuer des recherches par mots-clés. 12

2. Procédure pénale et renseignement

Avec l'entrée en vigueur du Code fédéral de procédure pénale, le déroulement du procès pénal sera globalement le même dans tous les cantons. La procédure pénale se divise en deux phases : la phase préparatoire du procès pénal, appelée procédure préliminaire, et la phase décisoire, soit le jugement et les éventuels recours[14]. 13

[12] PC-TI, *Rapport final d'activités sur les techniques spéciales d'investigation*, § 21.

[13] Parfois aussi banques de données.

[14] Sur la notion de procédure pénale en général : KUHN, *Procédure pénale unifiée*, pp 12-27. Pour une description du déroulement de l'enquête pénale et d'une procédure pénale ordinaire :

14 La procédure préliminaire se compose de la procédure d'investigation de la police et de l'instruction conduite par le ministère public[15]. L'investigation policière, menée d'office ou sur les instructions du ministère public, par les officiers et agents de la police judiciaire, a pour but d'établir la commission des infractions et d'en découvrir les auteurs, afin de les faire traduire devant les tribunaux répressifs pour être jugés[16].

15 L'instruction conduite par le ministère public doit établir l'état de fait et l'appréciation juridique du cas de telle sorte qu'il puisse mettre un terme à la procédure préliminaire. Si le ministère public procède à une mise en accusation, l'instruction doit fournir au tribunal les éléments essentiels lui permettant de juger la culpabilité du prévenu et de fixer la peine[17].

16 Alors que la procédure préliminaire doit permettre d'établir les faits et de décider s'il faut renvoyer ou non le prévenu devant un tribunal, la phase décisoire du procès pénal a pour but de procéder, avant que ne soit prise la décision sur le fond, à une instruction dite définitive de l'affaire au cours de laquelle seront administrées et discutées les preuves pour aboutir au jugement[18]. Le tribunal vérifie si l'acte d'accusation et le dossier sont établis régulièrement. Il peut procéder à l'administration de nouvelles preuves, compléter des preuves déjà administrées ou encore réitérer l'administration de certaines preuves[19]. Il procède encore à l'audition du prévenu, puis statue. Le jugement rendu en première instance est sujet à appel devant la juridiction d'appel[20]. Une fois la

ALBERTINI, *Tableaux synoptiques des enquêtes de police*, p. 139; *Message du CF relatif à l'unification de la procédure pénale*, p. 1090; CORNU, *L'enquête selon le CPP*, pp 52-64; KUHN, *Choix du modèle et droit transitoire*, pp 15-19; KUHN, *La procédure pénale suisse selon le futur CPP unifié*, pp 138-141; KUHN, *Procédure pénale unifiée*, pp 28-33; KUHN / PERRIER, *Quelques points problématiques du CPP*, ch. 2-8; PIETH, *Schweizerisches Strafprozessrecht*, pp 15-16; WINZAP, *La procédure de première instance*.

[15] Art. 299 CPP. Sur le rôle et les compétences du ministère public en général : CORNU, *Le nouveau ministère public*.

[16] PIQUEREZ, *Traité*, p. 668.

[17] Art. 308 CPP.

[18] PIQUEREZ, *Traité*, p. 697.

[19] Art. 343 CPP.

[20] Art. 398ss CPP.

décision entrée en force[21], elle doit être exécutée. L'exécution des jugements est encore essentiellement du ressort des cantons.

Le renseignement sert à rendre accessible toute connaissance utile à la prévention, à la répression et à la planification des opérations et des stratégies. Il se distingue de l'enquête qui vise la découverte de l'auteur d'un crime et des preuves de sa culpabilité[22]. L'activité de renseignement ne relève pas de la procédure pénale, mais fait l'objet d'une réglementation particulière en fonction de son but. Le renseignement consiste donc en la recherche d'information, notamment par l'exercice d'une surveillance préventive[23]. 17

On peut distinguer le renseignement en fonction de son objet (renseignement civil ou renseignement militaire), ou en fonction de son orientation dans le pays ou à l'étranger (renseignement intérieur ou renseignement extérieur), etc.[24]. En Suisse, l'activité de renseignement civil vise la détection précoce des dangers liés au terrorisme, au service de renseignement prohibé, à l'extrémisme violent, à la violence lors de manifestations sportives, au commerce illicite d'armes et de substances radioactives, ainsi qu'au transfert illégal de technologie[25]. Ces tâches sont prévues par l'art. 2 de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). 18

Dans le présent ouvrage, le renseignement sera distingué de l'investigation pénale, même si les termes de renseignement de sécurité sont parfois utilisés par opposition à celui de renseignement criminel ou pénal. C'est essentiellement l'activité de renseignement prévue par la LMSI qui sera abordée. 19

[21] Art. 437ss CPP.

[22] CUSSON, *De l'action de sécurité*, p. 48. Pour d'autres définitions plus complètes : BRODEUR, *Le renseignement*; LEMAN-LANGLOIS / LEMIEUX, *Renseignement de sécurité et renseignement criminel*.

[23] Voir à ce sujet le chapitre a) La surveillance préventive, p. 79 ci-dessous.

[24] Sur ces distinctions, voir le chapitre a) La surveillance préventive, p. 79 ci-dessous.

[25] RS 120.

3. Champ de l'étude

a) Du point de vue technique

20 L'objet de la présente étude se limitera aux moyens purement techniques. Les interrogatoires, perquisitions, saisies et fouilles ne seront pas traités, car ils dépasseraient largement le cadre de la thèse[26]. De même l'investigation secrète, soit le recours à des agents infiltrés, et la livraison surveillée ne seront pas abordées[27].

21 Un certain nombre de moyens techniques, indépendamment de savoir s'ils constituent ou non des mesures techniques de surveillance, ne sont pas admis comme moyens de preuve et ne seront pas abordés, soit qu'ils soient généralement considérés comme peu fiables, soit qu'ils portent manifestement atteinte à la dignité humaine[28]. Ils sont simplement mentionnés ci-après, avec quelques observations.

22 L'emploi de substances pharmacodynamiques, tel que le « sérum de vérité » (penthotal et scopolamine) a fait l'objet de sévères critiques en raison de son défaut de valeur probante et de la privation de la liberté de volonté de la

[26] Le lecteur est invité à consulter GRAFFENRIED, *Actes de la police judiciaire*, pp 69-143; PIQUEREZ, *Traité*, pp 463-469 et 577-609, ainsi que les références bibliographiques. Sur la distinction entre la saisie du courrier, d'un téléphone ou d'un ordinateur et la surveillance de la correspondance, voir notamment : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 81-85.

[27] Sur l'investigation secrète : ALBERTINI, *Tableaux synoptiques des enquêtes de police*, pp 210-211 et 214; BAUMGARTNER, *Zum V-Mann-Einsatz*; BÉNÉDICT, *Le sort des preuves illégales*, pp 157-182; GISLER, *La coopération policière*, pp 94-96; HANSJAKOB, *Das neue BVE*; HANSJAKOB, *Verdeckte Ermittlung*, pp 361-362; JOSET / RUCKSTUHL, *V-Mann-Problematik*; PIETH, *Schweizerisches Strafprozessrecht*, pp 132-138; PIQUEREZ, *Traité*, pp 629-634; RHYNER / STÜSSI, *Kommentar zu Art. 286-298 StPO*; SCHMID, *Praxiskommentar*, pp 543-568; VETTERLI, *Verdeckte Ermittlung und Grundrechtsschutz*; WOHLERS, *Revue de droit suisse*. Sur la livraison surveillée : GISLER, *La coopération policière*, pp 92-94.

[28] Sur les moyens de preuves prohibés : BÉNÉDICT, *Le sort des preuves illégales*, pp 108-109; CLERC, *Initiation à la justice pénale*, pp 147-149; DELESSERT, *Les méthodes techniques de surveillance*, pp 189-192; GRAFFENRIED, *Actes de la police judiciaire*, pp 86-89; KUHN, *La procédure pénale suisse selon le futur CPP unifié*, p. 135; PIQUEREZ, *La preuve pénale*, pp 19-21; PIQUEREZ, *Traité*, pp 433-436. Sur les notions d'incertitudes juridiques et d'incertitudes scientifiques : FLÜCKIGER, *La preuve juridique à l'épreuve du principe de précaution*. Pour un schéma des preuves prévues par le CPP : ALBERTINI, *Tableaux synoptiques des enquêtes de police*, p. 165.

personne interrogée[29]. Il en va de même pour l'investigation sous hypnose[30]. Le recours à la violence physique est également interdit, de même que les techniques dites « de démantèlement », soit les méthodes qui permettent d'obtenir des aveux en brisant la résistance physique ou psychique, qu'il s'agisse de privation de sommeil, de procédés chimiques, médicaux ou psychiatriques[31]. Pour terminer, les procédés qui ne reposent pas sur la raison sont dénués de toute force probante, tels le duel judiciaire, les ordalies ou la cartomancie. Ils ne seront dès lors pas retenus ici.

Les appareils « détecteurs de mensonges », notamment le polygraphe, suscitent les mêmes critiques et n'offrent en plus pas une fiabilité suffisante, la personne interrogée pouvant facilement fausser le résultat. La fiabilité du détecteur de mensonges pourrait s'améliorer ces prochaines années, des expériences étant en cours à l'aide de scanners et d'imageries par résonnance magnétique. Les zones en activité du cerveau ne sont semble-t-il pas les mêmes selon que le sujet dit la vérité ou un mensonge conscient[32]. Malgré leur manque de fiabilité, ces détecteurs ont toujours fasciné le grand public. Ils sont d'ailleurs toujours plus populaires, au point que l'on en trouve sur les sites de ventes aux enchères sur Internet et qu'un complément gratuit au logiciel de téléphonie par Internet Skype est disponible gratuitement pour découvrir si son interlocuteur dit la vérité (Kish Kish Lie Detector[33]). 23

Le Code de procédure pénale prévoit l'interdiction absolue des preuves recueillies par la contrainte, le recours à la force, les menaces, les promesses, la tromperie et les moyens susceptibles de restreindre les facultés intellectuelles ou le libre arbitre, même si la personne concernée a consenti (art. 140 et 141 CPP). 24

[29] DELESSERT, *Les méthodes techniques de surveillance*, p. 190.

[30] Le témoignage sous hypnose présente des risques quant à sa fiabilité et porte atteinte aux droits de la défense. Il a fait l'objet d'une jurisprudence importante aux Etats-Unis : VUCHER-BONDET, *La recevabilité d'un témoignage sous hypnose*.

[31] PIQUEREZ, *Traité*, p. 435.

[32] Pour une évolution historique et un regard critique : ROBERT, *Les mensonges du détecteur*. Sur le fonctionnement du polygraphe : KAUFMANN, *Beweisführung und Beweiswürdigung*, pp 138-141.

[33] http://www.kishkish.com.

Le recours à l'alcool ou aux stupéfiants, la privation de repas ou de sommeil, la narco-analyse ou encore l'usage du détecteur de mensonges sont donc exclus[34].

25 En revanche, des techniques qui ne sont pas initialement de surveillance, mais qui peuvent aboutir à une surveillance, seront prises en compte, notamment les tests d'ADN, les puces RFID ou encore les appareils GPS.

b) Du point de vue juridique

26 Le présent travail s'intéressera à la phase d'instruction au sens large, soit l'instruction proprement dite, mais également l'investigation policière. La phase de jugement ne sera pas étudiée, mais ce qui sera dit concernant l'instruction pourra s'appliquer *mutatis mutandis* à la récolte et l'administration des preuves lors des débats.

27 L'exécution des jugements dépasse trop largement le cadre de cette étude. L'assignation à résidence, également connue sous le nom d'arrêts domiciliaires, est simplement mentionnée. Elle consiste à maintenir un condamné en détention à son domicile. L'assignation à résidence sous surveillance électronique (également appelée « bracelet électronique ») en est la forme la plus actuelle. En pratique, on fixe au poignet ou à la cheville du « détenu » un petit bracelet émetteur ressemblant à une montre et permettant à une centrale de contrôle de savoir si la personne sous surveillance est bien à l'emplacement prescrit aux heures prévues par le juge[35].

28 L'assignation à résidence sous surveillance électronique peut être utilisée comme peine, comme mode d'exécution d'une peine ou partie de peine privative de liberté, ou comme substitut à la détention provisoire. Dans le cas hypothétique où le bracelet électronique serait utilisé dans le cadre de mesures

[34] *Message du CF relatif à l'unification de la procédure pénale*, p. 1162; KUHN, *La procédure pénale suisse selon le futur CPP unifié*, p. 135.
[35] KUHN, *Sanctions pénales*, pp 61-65.

d'enquête à la suite de la fuite d'un « détenu » par exemple, ce qui sera dit sur les méthodes de géolocalisation pourra être repris[36].

Quant à la surveillance opérée dans le cadre des services de renseignement, elle sera abordée de manière plus limitée. L'application de La Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) et l'exploitation des données récoltées seront néanmoins approfondies. La surveillance par un Etat étranger ou à l'étranger n'est en revanche pas abordée[37]. Finalement, et par souci de ne pas trop s'étendre, le droit militaire ne sera pas abordé, bien qu'il existe de très nombreuses similitudes entre le Code de procédure pénale et le Code de procédure pénale militaire. 29

B. Évolution historique des méthodes de surveillance

Si les mesures de surveillance ont toujours existé, elles étaient il y a encore quelques dizaines d'années relativement difficiles à mettre en place. Des procédés alors réservés aux services secrets, comme l'enregistrement de conversations téléphoniques à l'insu de l'interlocuteur, sont aujourd'hui à la portée de chacun[38]. Il s'agissait alors essentiellement de l'observation à la lunette, de l'ouverture de plis postaux, d'écoutes téléphoniques en direct nécessitant une retranscription ou la pose d'enregistreurs dont il fallait récupérer les bandes. L'évolution de l'informatique et la miniaturisation des appareils ont provoqué un véritable essor et une démocratisation des mesures de surveillance. Leur prix a baissé et les a rendues accessibles au particulier. Dans le même temps, le développement des communications sans fil et des réseaux numériques a aussi permis une surveillance beaucoup plus facile, et souvent sans laisser de 30

[36] Voir à ce sujet le chapitre 11. Les autres méthodes de localisation, p. 70 ci-dessous. A noter que l'avant-projet de révision de la LSCPT prévoit la possibilité de recourir à une surveillance de la correspondance par poste et télécommunication pour rechercher une personne condamnée (art. 28) : *Rapport du CF relatif à l'AP LSCPT*, p. 36.

[37] Même si l'activité en Suisse de services étrangers de renseignement ne doit pas être sous-estimée : SRC, *Rapport annuel 2009*, pp 80-83.

[38] JACQUARD, *Quand espionner les téléphones portables devient un jeu d'enfant*; LHUILLIE, *De la loyauté de la preuve.*

trace[39]. L'évolution est donc plutôt due aux possibilités techniques nouvelles qu'à un besoin plus important de pouvoir surveiller.

31 Actuellement, les moyens de surveillance permettant la collecte de données dans les environnements numériques paraissent déjà ne plus avoir de limite technique[40]. Ils se développent pourtant chaque jour un peu plus et gagnent en qualité et en fiabilité. De manière générale d'ailleurs, tout ce qui a trait à la sécurité et à la surveillance est en pleine expansion depuis plusieurs années[41].

32 L'utilité des mesures techniques de surveillance dans le cadre d'enquêtes pénales n'est plus contestée depuis de nombreuses années. La surveillance de la correspondance et des télécommunications est devenue un moyen d'investigation classique à disposition des autorités de poursuite[42].

33 La criminalité, qu'il s'agisse de criminalité organisée, de terrorisme, ou d'actes plus classiques, utilise toutes les possibilités techniques qui lui sont offertes, souvent même avant les autorités répressives. PIQUEREZ décrit les mesures de surveillance comme « des moyens d'investigation très performants[43] ». Quant à VON BENTIVEGNI, elle relevait déjà en 1986, soit à une époque où les moyens de communication n'étaient pas encore aussi développés qu'aujourd'hui, que l'évolution de l'organisation et de la technique de la criminalité oblige les autorités de poursuite pénale à recourir à des moyens et à des techniques modernes[44].

[39] Il est difficile de surveiller la correspondance postale sans retarder sa livraison et laisser des traces, alors que la surveillance des courriers électroniques, même nombreux, peut se faire de manière quasi automatique et sans laisser la moindre trace (sauf si l'expéditeur a pris des précautions particulières, ce qui est plutôt rare).

[40] BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 41-43; WEICHERT, *Überwachung: Einblick in die Praxis*, p. 9.

[41] Voir à ce sujet STEVENS, *Les facteurs de la demande de biens et services de sécurité.*

[42] Au sujet de l'efficacité des mesures de surveillance des télécommunications et des informations qui sont recherchées lors d'une surveillance (essentiellement en droit allemand) : ALBRECHT / DORSCH / KRÜPE, *Rechtswirklichkeit und Effizienz der TKÜ*. Pour un avis critique sur la vidéosurveillance et l'efficacité de la lutte contre la criminalité : CUSSON, *La télésurveillance*, pp 454-460; SHARANDIN, *Rapport sur la vidéosurveillance des lieux publics*, pp 7-9.

[43] PIQUEREZ, *Traité*, p. 612.

[44] VON BENTIVEGNI, *Les mesures officielles de surveillance*, p. 1.

Les mesures techniques de surveillance ne sont pas pour autant la solution à tous les maux[45]. Elles ne remplacent pas le travail du policier, mais sont plutôt un complément utile à ce travail. Quant au côté « rassurant » pour la population, si la présence de caméras de surveillance est souvent présentée comme un moyen de lutter contre le sentiment d'insécurité, il convient d'être prudent. C'est une opération toujours périlleuse que d'évaluer le poids de différentes mesures développées conjointement[46], d'autant plus que le sentiment d'insécurité ne correspond pas forcément à un risque objectif[47]. 34

Si l'on veut assurer le respect des droits de chacun, il ne faut pas se laisser emballer par les évolutions techniques mais rester dans un cadre juridique établi en fonction de droits à respecter et de choix juridiques : « Als Jurist muss man auf dem Postulat bestehen, dass die Grenzen der Überwachung durch das Recht und nicht durch die Technik bestimmt werden »[48]. 35

[45] Pour un regard nuancé sur l'utilité de certaines techniques : JOBARD / SCHULZE-ICKING, *Preuves hybrides*.

[46] Pour un exemple : RUEGG / FLÜCKIGER / NOVEMBER, *et al.*, *Vidéosurveillance et risques dans l'espace à usage public*, pp 245-246. Sur l'efficacité de la vidéosurveillance : FAVRE / DSIC, *Rapport à l'attention du Conseil administratif*, pp 3-5; GILL / SPRIGGS, *Assessing the impact of CCTV*; SALLAZ / DEBROSSE / HAN, *Rapport sur l'efficacité de la vidéoprotection*; WELSH / FARRINGTON, *Crime prevention effects of CCTV*.

[47] Sur la distinction entre le risque objectif et le sentiment d'insécurité : KUHN, *Sommes-nous tous des criminels*, pp 22-23. Sur le sentiment d'insécurité en général : VIREDAZ, *Le sentiment d'insécurité*.

[48] WELP, *Auf dem Weg zum Überwachungsstaat*, p. 22.

III. Les mesures techniques de surveillance

A. Catalogue des techniques actuelles et futures

1. La surveillance du courrier postal

36 La surveillance de la correspondance par poste est probablement une des plus anciennes et des plus classiques méthodes de surveillance. Elle consiste dans la surveillance d'une adresse postale, identifiée par un nom, un prénom et une localité, ainsi que selon les cas une adresse, une case postale ou un office postal en cas de mention « poste restante »[49].

37 Lorsqu'elle a lieu en temps réel, la surveillance du courrier postal consiste dans l'interception des envois postaux dirigés vers l'adresse surveillée, leur rétention temporaire, l'ouverture de l'enveloppe ou du colis, l'examen du contenu, ainsi que la duplication éventuelle du contenant et/ou du contenu (par photocopies, photographies, numérisation, etc.)[50]. Si la surveillance doit rester secrète, on procédera alors à la remise du contenu dans le contenant, la fermeture de ce dernier et finalement l'acheminement de l'envoi à son destinataire de sorte que celui-ci ne puisse se douter de l'existence d'une surveillance. Si nécessaire, une rétention durable de l'envoi est possible. La remise doit toutefois intervenir dès que l'avancement de la procédure le permet, à moins évidemment que le contenu ne soit illicite[51].

38 Il est également possible de surveiller la personne qui vient relever une case postale et à quel moment, quels ordres de réacheminement ont été donnés et par qui, etc.

---

[49] Pour des définitions analogues : BIEDERMANN, *BÜPF*, pp 103-104; HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 71-72; PIQUEREZ, *Traité*, p. 615; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 95-99.

[50] Dans certains cas, une modification de la lettre ou du colis peut intervenir : HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 72.

[51] L'art. 69 CP prévoit la confiscation des objets qui ont servi ou devaient servir à commettre une infraction ou qui sont le produit d'une infraction, si ces objets compromettent la sécurité des personnes, la morale ou l'ordre public. Le juge peut également en ordonner la destruction.

La surveillance du courrier peut également avoir lieu de manière rétroactive. Elle consiste alors dans la récolte des données enregistrées et conservées par les fournisseurs de services postaux : identités de l'expéditeur et du destinataire, nature de l'envoi (lettre ou colis, pli simple ou recommandé, urgent, fragile, etc.), lieu, date et heure d'expédition et d'acheminement, prix et mode de paiement. Ces données peuvent évidemment aussi être recueillies dans le cadre d'une surveillance en temps réel. 39

2. La surveillance du courrier électronique

Le courrier électronique (également appelé courriel ou e-mail) désigne le service permettant le transfert de messages envoyés par un système de messagerie électronique via un réseau informatique (le plus souvent Internet) vers la boîte aux lettres électronique d'un destinataire choisi par l'émetteur[52]. Par extension, on désigne également le message envoyé par ce biais du nom de courrier électronique ou courriel. 40

L'objet de la surveillance est une boîte aux lettres électronique identifiable par son adresse électronique. Une telle adresse peut être créée en quelques secondes auprès de n'importe quel fournisseur d'accès ou d'un site spécialisé (les plus connus étant Hotmail[53], Gmail[54], Yahoo[55], etc.), et ce sans qu'il soit nécessaire de prouver son identité. 41

La surveillance est similaire à celle du courrier postal, si ce n'est que les données électroniques peuvent être beaucoup plus facilement interceptées et copiées que les données physiques. Les en-têtes des messages comportent aussi de précieuses informations d'adressage (notamment le lieu et le moment de l'expédition). La boîte aux lettres garde également très souvent en mémoire tout ou partie des courriers entrants, sortants et effacés, ce qui n'est pas le cas d'une boîte aux lettres postale. 42

[52] Sur internet en général : DUFOUR / GHERNAOUTI-HÉLIE, *Internet*. Sur le fonctionnement du courrier électronique : BÉNÉDICT, *Internet*, pp 275-277; DUFOUR / GHERNAOUTI-HÉLIE, *Internet*, pp 40-45; HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 57-60.

[53] http://www.hotmail.com.

[54] http://www.gmail.com.

[55] http://www.yahoo.com.

43 La surveillance du courrier électronique permet en outre de surveiller aussi aisément le courrier reçu que le courrier envoyé. C'est une différence fondamentale avec le courrier postal où la lettre est déposée dans n'importe quel office de poste ou boîte aux lettres publique. Elle est directement émise par la boîte aux lettres électronique correspondant à l'adresse surveillée, qui fonctionne simultanément comme expéditeur et destinataire, comme un téléphone sert d'émetteur et de récepteur[56].

44 La manière la plus simple de surveiller une adresse électronique est de demander à celui qui met l'adresse à disposition, fournisseur d'accès ou site Internet, de transmettre en temps réel une copie de l'activité de l'adresse ainsi que les données liées aux messages déjà transmis. Les autres possibilités de surveillance sont celles applicables à toutes données informatiques[57].

3. Les écoutes téléphoniques

45 Les communications téléphoniques (y compris les SMS, les télécopies ou téléfax ou transmissions de données) sont transmises par câble (cuivre ou fibre optique), par faisceau hertzien ou par satellite, alors que les téléphones mobiles sont reliés au réseau téléphonique par ondes radio. Un abonnement à un opérateur téléphonique classique n'est plus nécessaire aujourd'hui, puisque le téléphone peut aussi transiter par le réseau câblé de la télévision, le réseau électrique ou encore par Internet[58].

46 L'objet de la surveillance est un raccordement à un réseau fixe de télécommunication (identifiable par son numéro d'appel), un raccordement à un réseau mobile de télécommunication (identifiable par son numéro d'appel ou MSISDN, son numéro IMSI ou son numéro SIM) ou un téléphone mobile

[56] Des logiciels ou sites internet permettent aussi d'envoyer anonymement un courrier électronique, mais leur usage n'est pas très courant.

[57] Voir à ce sujet le chapitre 4. L'interception de données électroniques sur Internet, p. 40 ci-dessous.

[58] Pour un exposé technique en matière de téléphonie fixe et mobile : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 39-51. Voir au sujet des autres vecteurs de conversations téléphoniques le chapitre 4. L'interception de données électroniques sur Internet, p. 40, et concernant la téléphonie sur internet : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 60-64.

(identifiable par son numéro IMEI)[59]. Dans les faits, la surveillance d'un raccordement fixe dans le cadre d'une enquête pénale est de plus en plus rare.

Les méthodes d'interception les plus simples consistent à se brancher directement au réseau, soit au câble de transmission ou à une station de réception et de transmission[60]. Les mesures de surveillance officielles sont pour l'essentiel effectuées par le biais du fournisseur de services de télécommunications[61]. Pour les communications mobiles, par signaux à hyperfréquences ou par satellite, il est également possible d'intercepter le signal concerné[62]. L'écoute des téléphones sans fil (DECT)[63] est particulièrement facile à réaliser, les communications entre l'appareil et la base n'étant généralement pas cryptées[64]. 47

Le IMSI-Catcher est un appareil électronique simulant une antenne relais GSM dans le but de se placer entre l'antenne authentique et le téléphone portable. Cet appareil permet d'intercepter les numéros IMSI et IMEI à une portée pouvant aller jusqu'à plusieurs kilomètres, de localiser les appareils dans cette zone et d'écouter les conversations téléphoniques. L'utilisation de l'IMSI-Catcher ne 48

[59] Le MSISDN (Mobile Station ISDN Number) est le numéro d'appel. Il se compose de l'indicatif du pays, d'un indicatif régional ou d'opérateur et finalement du numéro de l'abonné. Il correspond au numéro d'appel des raccordements fixes.
L'IMSI (International Mobile Subscriber Identity) est un numéro unique stocké dans la carte SIM qui permet à un réseau d'identifier un usager. Ce numéro n'est pas connu de l'utilisateur.
La carte SIM (Subscriber Identity Module) est une carte à puce que l'on insère dans son téléphone portable.
L'IMEI (International Mobile Equipment Identity) est un numéro de 15 chiffres qui permet d'identifier de manière unique un téléphone mobile. Il permet ainsi à l'opérateur du réseau de téléphonie mobile d'identifier le mobile appelant et de l'autoriser ou non à se connecter. Ce numéro s'obtient en tapant *#06# et son rôle le plus connu est de pouvoir bloquer un mobile volé auprès de l'ensemble des opérateurs.

[60] Le « branchement » peut avoir lieu physiquement, mais aussi virtuellement c'est-à-dire en se connectant à l'installation de l'opérateur par le biais d'un réseau informatique.

[61] Il est tenu de prêter son concours aux mesures de surveillance de par la loi et la concession dont il bénéficie généralement.

[62] SCHMID, *Rapport Echelon*, pp 16-19. Voir également à ce sujet le chapitre 6. L'interception de champs électromagnétiques et d'ondes hertziennes, p. 46. Si l'appareil de téléphone et le téléphone portable sont souvent l'objet d'une surveillance, ils peuvent aussi, selon la manière dont ils sont utilisés, jouer le rôle de l'appareil d'écoute : ATF 133 IV 249, 254, X., du 13 août 2007.

[63] Digital Enhanced Cordless Telecommunications.

[64] Emission nouvo du 20 juillet 2009, disponible à l'adresse http://www.nouvo.ch/s-027.

nécessite aucune intervention de l'opérateur téléphonique[65]. On trouve également des petits logiciels espions que l'on peut installer sur un téléphone portable et qui permettent ensuite de surveiller l'utilisation qui est faite de cet appareil, y compris écouter les conversations et l'environnement du téléphone[66].

49 En plus des écoutes en temps réel[67], une surveillance rétroactive est également possible. Elle consiste à recueillir les données relatives au trafic enregistrées par les fournisseurs de services de télécommunications[68]. En plus des données nécessaires à la facturation, ceux-ci conservent, durant un certain temps du moins, les numéros composés et reçus, l'heure, la date, le lieu et la durée de ces communications, la durée de la sonnerie, la raison de la fin de la communication, les éventuelles déviations d'appel, les services activés, ainsi que l'utilisation d'une boîte vocale et les données relatives à sa consultation, etc.

4. L'interception de données électroniques sur Internet

50 Le courrier électronique ressemble au courrier postal, mais il utilise une infrastructure similaire à celle utilisée pour les conversations téléphoniques. La surveillance du courrier électronique peut ainsi s'apparenter à celle du courrier postal, mais le courrier électronique peut également être surveillé comme n'importe quelle donnée transitant sur un réseau informatique[69].

---

[65] DE SAUSSURE, *Le IMSI-Catcher*, ch. 1-22; EISENBERG, *Beweisrecht der StPO*, pp 906-907; STROBEL, *IMSI Catcher*, pp 13-17. Voir également la note de bas de page n° 468.

[66] JACQUARD, *Quand espionner les téléphones portables devient un jeu d'enfant*; JACQUARD, *Quatre questions sur un «mouchard»*.

[67] Dans la notion d'écoute des conversations téléphoniques est également incluse la surveillance des SMS et autres messages transitant par un téléphone.

[68] On distingue ainsi le contenu de la conversation (CC, Call Content) des autres informations liées aux communications (IRI, Intercept Related Informations).

[69] Internet est un réseau de réseaux informatiques composé de millions d'ordinateurs qui peuvent entrer en contact les uns avec les autres au moyen d'un logiciel adapté les reliant à un serveur. Chaque ordinateur se voit attribuer une adresse IP (Internet Protocol Address), soit une série de chiffres réunis en sous-groupes, pour qu'il puisse être identifié et recevoir des données. Pour une description du fonctionnement d'internet : ATF 128 III 353, 356-357, Institut Montana Betriebs AG, du 23 juillet 2002, ATF 4C.9/2002 du 23 juillet 2002, consid. 4 et BÉNÉDICT, *Internet*, pp 268-271. Concernant les différentes interceptions possibles : TRECCANI, *Interceptions électroniques*, pp 223-230. Pour un aperçu technique et historique d'internet : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 51-57.

L'échange des données entre les ordinateurs reliés à Internet s'effectue par paquets de données, qui dans le réseau suivent en principe chacun leur chemin propre et qui, au moment où ils atteignent leur destination, sont recombinés. Un paquet de données pouvant être lu à chaque station intermédiaire, cela signifie que les messages transmis par courrier électronique sont réputés extrêmement peu sûrs. Leur confidentialité est volontiers comparée à celle d'une carte postale. Des mesures spéciales, telles que le recours à la cryptographie, permettent cependant d'éviter que le contenu des messages ne puisse être lu par un tiers non autorisé[70]. 51

S'il est difficile pour un pirate informatique de surveiller l'ensemble du réseau mondial, il lui est en revanche facile d'en surveiller une petite partie. Celui qui souhaite avoir accès à un ordinateur précis doit se procurer un accès à un ordinateur proche de celui-ci (dans l'architecture du réseau et non pas au sens géographique), alors que pour celui qui veut simplement pénétrer un nombre maximal de messages, n'importe quel point du réseau est bon. Le risque que les messages soient incomplets, certains paquets du message seulement étant obtenus, croît en fonction de la distance le séparant de l'expéditeur. La meilleure façon d'obtenir des messages complets consiste donc à avoir une position très proche de l'expéditeur du courrier électronique dans le réseau ou à avoir accès au fournisseur de services Internet de l'expéditeur ou du destinataire[71]. Les programmes Omnivore et Carnivore (DCS-1000) développés par le FBI, mais également de nombreux autres programmes commerciaux librement accessibles, permettent de surveiller facilement un ordinateur donné[72]. 52

Si la surveillance d'une adresse électronique ou de l'activité d'une personne précise requiert une certaine proximité, la surveillance de certains contenus indépendamment de leur expéditeur ou destinataire n'implique pas un point de connexion particulier. Une telle surveillance recourt par exemple à des mots-clés. Le pourcentage de messages trouvés dépendra alors de la capacité à surveiller l'ensemble du réseau, puisque les messages peuvent aussi emprunter 53

[70] Sur les possibilités de chiffrement et déchiffrement : MEUWLY, *L'Ordonnance sur le service de surveillance de la correspondance postale et des télécommunications.*

[71] SCHMID, *Rapport Echelon*, pp 19-20.

[72] Pour une description de ces programmes et un exemple illustré de la surveillance à distance d'un ordinateur : ANDRES, *Die Internet-Überwachung in der Praxis*, pp 239-253.

un autre chemin sur le réseau. Ce genre de surveillance nécessite de gros moyens et est plutôt utilisé par les services nationaux (voire supranationaux) de renseignement, comme dans le cadre du programme Echelon[73]. Si l'on connaît l'adresse électronique ou le fournisseur d'accès utilisé, il est beaucoup plus facile de surveiller cet élément précis, puisqu'il permet de connaître l'ensemble des données transitant par ce point-là du réseau. La surveillance du point de départ ou d'arrivée des données est évidemment plus facile à mettre en place que la surveillance de l'ensemble des points du réseau mondial par lequel passeront hypothétiquement des données intéressantes[74].

54 Dans le cas d'une surveillance ciblée, il est possible de détourner le flux de données à destination d'un nom de domaine en polluant la mémoire-cache du serveur DNS. De manière simplifiée, toutes les données destinées à un site Internet sont déviées vers le surveillant, puis éventuellement redirigées vers la bonne adresse. Il est alors facile de connaître tous les visiteurs d'un site Internet, les messages adressés, etc.

55 Une autre méthode consiste à installer un « cheval de Troie » sur la machine que l'on veut surveiller[75]. On appelle ainsi de petits programmes en apparence anodins, qui une fois installés permettent de prendre le contrôle à distance de l'ordinateur sur lequel ils se trouvent, et évidemment d'en surveiller en temps réel tout le contenu. Les « chevaux de Troie » sont notamment utilisés pour surveiller les discussions par messagerie instantanée (MSN) ou la téléphonie par

[73] Un tel système d'interception existe également en Suisse, connu sous le nom de Onyx (anciennement SATOS-3) : BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 525-527; *Rapport de la DélCdG du 10 novembre 2003 sur le projet Onyx*.

[74] Certaines entreprises se sont spécialisées dans la surveillance des communications effectuées par messagerie instantanée et VoIP, ou la récolte d'adresse IP (particulière sur les sites d'échanges de fichier *peer-to-peer*), par exemple Logistep SA (www.logistepag.com) en Suisse et Nexicon inc. (www.nexiconinc.com) aux Etats-Unis. La légalité de l'activité de ces entreprises est problématique du point de vue de la protection des données et de l'utilisation de pouvoirs d'enquête réservés à l'Etat : FANTI, *Alcatraz numérique*, pp 29-42 et 54-87. Le Tribunal fédéral a confirmé dans une audience publique tenue le 8 septembre 2010 que l'adresse IP est une donnée personnelle protégée par la sphère privée et qu'une entreprise privée ne peut pas se substituer à la police pour les récolter (arrêt à paraître dans la cause PFPDT c. Logistep SA, 1C_285/2009).

[75] On parle de Gov-Ware ou Government-Software lorsqu'il s'agit de programmes installés par une autorité pour surveiller l'activité d'un ordinateur ou sur internet : RHYNER / STÜSSI, *Kommentar zu Art. 280-281 StPO*, p. 469.

Internet (VoIP, Skype,…)[76]. Une variante consiste à transmettre périodiquement des rapports de tout ce qui a été frappé sur le clavier, permettant à celui qui reçoit le rapport de connaître toute l'activité de l'ordinateur surveillé, y compris les mots de passe tapés.

La technique de surveillance la plus souvent opérée dans le cadre d'une enquête pénale est l'interception depuis le fournisseur d'accès. Comme dit précédemment, elle permet de surveiller la correspondance électronique, mais pas seulement. Il est en effet possible d'y capter l'ensemble des données à destination ou en provenance de l'ordinateur surveillé. Lorsque seuls certains sites ou services sont utilisés, il peut être fait appel à l'aide du fournisseur de services[77]. Des sondes que l'on pose sur la ligne téléphonique permettent également une surveillance similaire, sans toutefois devoir passer par un fournisseur d'accès. Cette solution plus coûteuse est utile si la coopération d'un fournisseur d'accès n'est pas possible ou si la personne surveillée recourt à un grand nombre de fournisseurs d'accès différents. 56

On notera encore l'existence des pixels-espions (webbugs) soit des images transparentes comportant un seul pixel et figurant sur des pages Internet. Invisibles du visiteur de la page en question, ils permettent de connaître l'adresse IP utilisée, la date, l'heure et la durée de la visite, les pages visitées antérieurement, ainsi que des caractéristiques techniques de l'ordinateur du visiteur telles que le système d'exploitation, le type de navigateur et la résolution de l'écran[78]. 57

[76] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 103-106.

[77] Un document intitulé « Microsoft® Online Services Global Criminal Compliance Handbook » décrit dans le détail les informations qui peuvent être transmises sur demande à la justice concernant les adresses électroniques (hotmail, msn, live), la messagerie électronique (Windows Live Messenger), les réseaux sociaux (Windows Live Spaces, MSN Groups), l'hébergement de site et le stockage de documents (Office Live Small Business, Office Live Workspace, Windows Live SkyDrive) et les consoles de jeux (XBOX LIVE) :
http://cryptome.org/isp-spy/microsoft-spy.zip ou
http://www.scribd.com/doc/27394899/Microsoft-Spy.

[78] PFPD, *Explications relatives aux webbugs*.

5. L'interception de données électroniques sur l'ordinateur ou le serveur

58 L'interception des données de n'importe quel ordinateur est possible à celui qui y a accès. Cet accès peut aussi être réalisé au travers du serveur auquel il est relié, voire d'un autre ordinateur appartenant au même réseau local. Dès que l'accès est ouvert, il est possible d'obtenir toutes les données présentes sur la machine ou le réseau.

59 La majeure partie du trafic international des paiements est effectuée par l'intermédiaire de la Society for Worldwide Interbank Financial Telecommunication (SWIFT), dont le siège est en Belgique. Une surveillance de flux financiers est donc possible à ce niveau, indépendamment de la banque utilisée. La société SWIFT disposait de deux centres qui enregistraient et traitaient des données identiques, l'un au siège en Belgique et l'autre aux Etats-Unis. Peu après les attentats du 11 septembre 2001, la CIA et le département du Trésor américain ont ainsi mis en place un programme de surveillance des transactions bancaires internationales lui permettant de suivre en temps réel toutes les opérations bancaires transitant par SWIFT. Elles avaient également accès à des données qui ne concernaient pas les Etats-Unis. Depuis, deux nouveaux centres ont été ouverts en Suisse et les données concernant les transactions intra-européennes sont uniquement stockées en Suisse ou en Belgique[79]. Après de longues négociations, un accord avec les Etats-Unis a finalement été accepté par le Parlement européen pour permettre l'accès à ces données dans le cadre de procédures pénales. Il exige que la requête américaine soit motivée par une enquête et adaptée pour limiter le nombre de données à transmettre[80].

[79] Voir notamment : CNIL, *Communiqué de presse du 13 juin 2007*; *Rapport annuel 2007 des CdG et de la DélCdG*, pp 4602-4604; *Rapport annuel 2009 des CdG et de la DélCdG*, pp 2456-2457; GROUPE 29, *Avis 10/2006 (SWIFT)*; PFPDT, *14ème rapport*, pp 73-74; PFPDT, *17ème rapport*, p. 80.

[80] A fin 2009, les ministres de l'intérieur des pays membres de l'Union européenne s'étaient déjà mis d'accord pour maintenir l'accès des Etats-Unis aux données bancaires des citoyens européens, mais le Parlement européen avait rejeté cette convention en février 2010. Un nouvel accord a toutefois été accepté par le Parlement européen le 8 juillet 2010 : AFP, *Terrorisme: UE et Etats-Unis s'accordent pour partager les données bancaires*; PFPDT, *17ème rapport*, p. 80.

Une autre méthode est le recours à un espion clavier, logique ou matériel[81]. Cet espion ne permet pas de connaître tout ce qui est dans la mémoire de l'ordinateur, comme dans le cas précédent, mais tout ce qui est fait avec l'ordinateur depuis que l'espion est actif. Une surveillance rétroactive n'est pas possible. 60

L'espion clavier[82] est un dispositif chargé d'enregistrer les frappes des touches du clavier, à l'insu de l'utilisateur. L'espion clavier logique prend la forme d'un logiciel, qui peut être installé directement sur la machine ou par le truchement d'un « cheval de Troie ». L'espion clavier matériel se fixe lui dans le clavier ou plus simplement sous la forme d'une rallonge entre la prise du clavier et l'ordinateur. Il peut être pourvu d'un émetteur radio pour transmettre les informations. Si l'installation d'un espion clavier matériel implique un accès physique à l'ordinateur, il n'est en revanche pas nécessaire de connaître les codes d'accès de celui-ci, ni même de pouvoir l'allumer. Il existe aussi des espions clavier matériels qui peuvent être installés à distance et qui réagissent aux bruits des différentes touches du clavier. 61

Actuellement, la grande majorité des photocopieurs et autres appareils multifonctions (toutes les combinaisons imaginables de téléphone, téléfax, répondeur, scanner, imprimante et photocopieur) possèdent des composants de stockage (mémoires flash et autres disques durs). Ces éléments servent initialement à améliorer le confort de l'utilisateur. Ils peuvent pourtant être lus ultérieurement, comme n'importe quel disque dur d'ordinateur. Autrement dit, il est relativement facile, pour une personne possédant les compétences informatiques requises, de retrouver ce qui a été numérisé, copié ou imprimé. Les photocopieurs des entreprises et bibliothèques publiques sont couramment utilisés pour réaliser des copies de papiers d'identité, de déclarations d'impôts, etc., alors que leur accès n'est en général pas contrôlé. 62

Si la très grande majorité des utilisateurs de ces appareils ignorent ces faits, les fabricants de photocopieurs, eux, ne s'en cachent pas. Ainsi en 2003 déjà, Ricoh 63

Pour une analyse juridique en droit européen et américain : MONTBEYERE, *Aspects juridiques de l'Affaire SWIFT*.

[81] TRECCANI, *Interceptions électroniques*, pp 234-236.

[82] En anglais keylogger, soit littéralement « enregistreur de touches ».

et Xerox confirmaient au journal en ligne ZDNet que des informations étaient stockées sur les disques durs[83]. Une dépêche d'Associated Press publiée par le Boston Globe indiquait que plus de la moitié des Américains ignoraient encore ce risque en 2007[84].

64 Une surveillance en temps réel est envisageable, mais le plus simple est encore l'extraction des données après avoir récupéré le disque dur.

6. L'interception de champs électromagnétiques et d'ondes hertziennes

65 On a vu précédemment qu'il était possible d'intercepter des communications téléphoniques. Si la communication téléphonique se fait par satellite, il est possible d'intercepter cette communication à l'aide de grandes antennes paraboliques (« grandes oreilles »). Pour avoir la conversation complète entre les deux personnes, il est nécessaire d'intercepter le signal descendant aux deux points de communication, autrement dit sur les deux continents[85].

66 Dans le cas d'une communication par signaux à hyperfréquences, ces signaux peuvent être interceptés par l'intermédiaire d'une station terrestre à proximité de la ligne invisible reliant deux relais hyperfréquences[86]. Quant aux communications mobiles, en plus des possibilités énumérées précédemment, il est possible d'intercepter et de décoder le signal radio d'un appareil situé à proximité. L'avantage de cette technique est de permettre d'écouter les conversations passées au moyen d'un téléphone dont on ne connaît pas le numéro[87].

67 Les conversations téléphoniques ne sont pourtant pas les seules à pouvoir être « écoutées ». 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. C'est notamment le

[83] GUILLEMIN, *Le photocopieur*.
[84] ASSOCIATED PRESS, *The Boston Globe*.
[85] SCHMID, *Rapport Echelon*, p. 18.
[86] SCHMID, *Rapport Echelon*, p. 17.
[87] SCHMID, *Rapport Echelon*, pp 16-17.

cas des télécopieurs, écrans d'ordinateur, lecteurs externes de CD ou DVD, scanners, imprimantes et photocopieurs[88]. Pour se protéger de telles interceptions, il est possible de recourir à un blindage électromagnétique ou une cage de Faraday, celle-ci empêchant la propagation des ondes à l'extérieur de la cage.

Il y a ensuite les liaisons et réseaux sans fil (Bluetooth, WiFi, etc.) qui sont en pleine évolution. Les ordinateurs communiquent ainsi entre eux ou avec leurs périphériques (imprimantes, modems, etc.) en utilisant les ondes hertziennes[89]. Ces ondes peuvent être interceptées très facilement et il ne serait pas surprenant que de telles méthodes de surveillance soient toujours plus utilisées à l'avenir[90]. Ces données peuvent être protégées, notamment par un chiffrement et une authentification. Le chiffrement est une protection relative, puisqu'il peut être cassé à certaines conditions par des spécialistes[91]. Nombreux sont ceux qui, par paresse ou ignorance, ne mettent pas en place de simples mesures de protection et laissent ainsi des tiers d'utiliser leur infrastructure à leur insu[92]. 68

7. La vidéosurveillance

a) Les composants

Un système de vidéosurveillance traditionnel se compose de quatre éléments : des caméras, des lignes de transmission du signal vidéo, plusieurs écrans de contrôle qui affichent les images ou les séquences saisies par les caméras et, de plus en plus souvent, un dispositif d'enregistrement qui stocke les images 69

[88] Sur l'interception des champs électromagnétiques : TRECCANI, *Interceptions électroniques*, pp 232-233.

[89] Sur l'interception des ondes hertziennes : TRECCANI, *Interceptions électroniques*, pp 233-234.

[90] Un ordinateur équipé d'une simple carte VoIP peut ainsi se faire passer pour la base d'un téléphone sans fil et permettre l'écoute des communications, même si celle-ci est chiffrée : KREMPL, *Serious security vulnerabilities in DECT wireless telephony*.

[91] Sur les possibilités de chiffrement et déchiffrement : MEUWLY, *L'Ordonnance sur le service de surveillance de la correspondance postale et des télécommunications.*

[92] Le comportement d'un tiers pourrait alors être imputé au propriétaire de l'infrastructure informatique. Dans le cas d'un téléchargement illégal par exemple, le propriétaire de l'accès internet sera présumé être à l'origine du téléchargement, à moins qu'il n'arrive à prouver le contraire.

transmises[93]. Il s'agit alors d'un circuit fermé (Closed Circuit Television, CCTV). Les caméras, les écrans et le dispositif de stockage peuvent être dans des lieux très éloignés.

70 La caméra capture les images. Elle peut être optique, thermique ou radar. La caméra optique est dérivée de l'appareil photo. Elle saisit la lumière réfléchie par les objets se trouvant dans le champ de vision de l'appareil. Elle peut réagir au spectre visible, infrarouge, ultraviolet ou aux rayons X. La caméra thermique est, elle, basée sur des capteurs qui savent lire les émissions infrarouges qu'un objet émet en fonction de sa température. L'électronique restitue une image en fonction de la température de chaque point. Enfin, la caméra radar est capable de fournir une image à partir de la réflexion d'ondes électromagnétiques sur un objet. Cette technologie est la plus récente. Elle permet même de voir un objet à travers un mur[94]. Les caméras peuvent être extrêmement discrètes, puisqu'il existe des caméras miniatures à objectif de la taille d'une tête d'épingle.

71 Le système de transmission classique de l'information consiste à faire voyager des signaux électriques variables dans un câble semblable à celui qui amène la télévision dans les foyers. Aujourd'hui, un signal vidéo peut circuler sur un réseau informatique, pour autant qu'il ait été numérisé préalablement. Il peut ainsi transiter par Internet, un faisceau laser, un faisceau radio (wi-fi notamment), un réseau électrique, un téléphone ou encore un satellite.

72 Le stockage (ou archivage) des données se faisait à l'origine sur des bandes vidéo. Ce support est peu performant (capacité limitée et durée de vie aléatoire) et n'est pas très praticable lorsqu'il faut rechercher des données. L'archivage numérique, soit sur des disques durs ou des supports de type CD-ROM ou DVD est donc mieux adapté. Pour économiser de la place, on peut compresser les images ou en réduire la résolution.

---

[93] Pour une définition plus complète de la vidéosurveillance et une description de ses composants : BEDDIAF, *Vidéosurveillance*; CUSSON, *La télésurveillance*; GEIGER, *Verfassungsfragen zur polizeilichen Video-Überwachung*, pp 27-43; KÖNIG, *Videoüberwachung*, pp 19-26; RUEGG / FLÜCKIGER / NOVEMBER, *et al.*, *Vidéosurveillance et risques dans l'espace à usage public*, pp 6-7 et 31-37; SHARANDIN, *Rapport sur la vidéosurveillance des lieux publics*.

[94] Sur les caméras infrarouges et les méthodes similaires : ARZT, *Polizeiliche Überwachungsmassnahmen in den USA*, pp 48-53.

Plusieurs autres éléments peuvent venir se greffer sur un système de vidéosurveillance, en fonction du but poursuivi[95]. De nos jours, les systèmes de vidéosurveillance peuvent compter plusieurs centaines de caméras distribuées dans le monde entier[96]. 73

b) Quelques utilisations particulières

Actuellement, de nombreux systèmes de vidéosurveillance sont installés dans les transports et lieux publics. A Lutry (VD), des caméras de surveillance filment la cour de l'école vingt-quatre heures par jour, sept jours par semaine[97], alors qu'à Middlesbrough (GB), plusieurs caméras sont équipées de haut-parleurs permettant de tancer les passants au comportement inadéquat. En 2006, la société Digital Bridge diffusait en continu sur le câble local Shoreditch TV, soit les images des caméras de surveillance publiques de ce quartier de Londres[98]. Cette chaîne a été interrompue après quelque temps. Une société anglaise appelée Internet Eyes propose depuis 2009 aux internautes de visionner en direct des images prises par des caméras de surveillance et de dénoncer les crimes et délits qu'ils découvriraient. Celui qui a dénoncé le plus de crimes à la fin du mois reçoit une récompense de GBP 1 000.-. Quant aux commerces et magasins, ils peuvent s'abonner pour que leurs images soient visibles sur le site[99]. 74

[95] Voir à ce sujet la section suivante.

[96] PFPDT, *16ème rapport*, p. 21.

[97] Saisi d'une action introduite par plusieurs syndicats d'enseignants lui demandant de constater que l'Etat de Vaud devait agir pour faire cesser la surveillance, le Tribunal de prud'hommes de l'administration cantonale a constaté par jugement préjudiciel du 3 septembre 2007 que l'Etat de Vaud n'avait pas les moyens juridiques pour agir contre les communes ayant installé des système de vidéosurveillance dans les établissement scolaires. Les décisions judiciaires principales sont disponibles à l'adresse : http://www.sud-vd.ch/politique_generale_finances_publiques/camera.

[98] Parfois aussi appelé crime channel. Emission nouvo du 23 novembre 2006, disponible à l'adresse http://www.nouvo.ch/110-3, HARKIN, *"Big Brother" may be over but we still love watching ourselves*; HYDE, *This surveillance onslaught is draconian and creepy*.

[99] http://www.interneteyes.co.uk, MALINGRE, *Caméras de surveillance*; VERDONNET, *Les internautes britanniques invités à dénoncer les crimes et les délits*.

75 PRIVATIM, l'association regroupant les commissaires suisses à la protection des données, estime à 450 000 le nombre de caméras de surveillance en fonction en Suisse au mois de juin 2007[100]. A fin 2007, le Royaume-Uni comptait à lui seul quatre millions de caméras de surveillance et 85 % des municipalités du pays étaient équipées de réseaux de vidéosurveillance. Un citoyen britannique était ainsi filmé en moyenne plus de 500 fois par semaine, et un Londonien 300 fois par jour[101]. A cela s'ajoutent évidemment les caméras mises en place de manière temporaire par les autorités policières dans le cadre d'enquêtes.

76 L'informatique a permis l'automatisation de certaines tâches précédemment dévolues à des opérateurs[102]. La détection d'incendies, d'objets immobiles ou en mouvement, de mouvements de foule, de contresens sur une autoroute, le comptage, l'identification de véhicules et de plaques d'immatriculation, ou encore la reconnaissance faciale peuvent avoir lieu automatiquement[103]. Il est ainsi possible de repérer, sans la moindre intervention humaine, une voiture à l'arrêt dans un tunnel, une mallette abandonnée dans un couloir, une tentative de suicide le long des voies de métro, un corps flottant en-dessous de la surface de l'eau dans une piscine ou encore des traits particuliers sur un visage. Un système automatique de détection est alors couplé à un système d'alarme, qui avertit la personne responsable par téléphone, courrier électronique, ou autre. Il est également possible d'avoir des caméras embarquées à bord d'avions sans pilote (drones) ou de dirigeables[104].

77 Les entreprises suisses figurent en bonne place dans le développement des techniques liées à la vidéosurveillance. La société lausannoise VisioWave (rachetée par General Electric) a élaboré un système de compression vidéo permettant de transmettre les images par Internet, ainsi que des programmes

[100] PRIVATIM, *Communiqué de presse du 14 juin 2007*. Sur la vidéosurveillance dans les gares : DFJP, *Rapport sur la vidéosurveillance*, pp 14-15.

[101] SHARANDIN, *Rapport sur la vidéosurveillance des lieux publics*, p. 6.

[102] Pour des exemples : FLÜCKIGER / AUER, *La vidéosurveillance dans l'œil de la constitution*, p. 925; RUEGG / FLÜCKIGER / NOVEMBER, *et al.*, *Vidéosurveillance et risques dans l'espace à usage public*, pp 35-36.

[103] Sur le système automatisé d'identification de numéros de plaques de véhicules (AFNES) : RÉMY, *Droit des mesures policières*, pp 111-112. De tels systèmes sont par exemple utilisés dans les cantons de Zurich, Thurgovie et St-Gall : DFJP, *Rapport sur la vidéosurveillance*, p. 21.

[104] PFPDT, *17ème rapport*, pp 21-24.

d'analyse « intelligents » qui animent les écrans lorsqu'un comportement suspect est détecté, ce qui permet à un seul opérateur de surveiller un très grand nombre de caméras simultanément[105].

Quant à la société Emitall Surveillance, basée à Montreux, elle a développé un système permettant de rendre anonymes les personnes filmées. Celles-ci ne peuvent ensuite être rendues visibles qu'au moyen d'une clé qui pourrait être détenue par exemple par un magistrat[106]. La surveillance peut alors s'opérer sans que les personnes ne soient identifiées, mais elles demeurent identifiables *a posteriori* par les autorités de poursuite pénale[107]. 78

c) Quelques techniques assimilées à la vidéosurveillance

L'utilisation de micros et magnétophones est une technique relativement ancienne[108]. Initialement, on recourait à des micros, des câbles, des amplificateurs, des batteries et des casques, et des opérateurs sténographiaient ce qui se disait. Des micros sans fil, dotés d'un petit émetteur, étaient déjà présentés lors de la conférence des commandants de police du 8 mai 1951[109]. On parlait alors de miniespions. Il y a actuellement sur le marché des microphones paraboliques ou lasers, permettant une écoute à une distance de 300, respectivement 500 mètres[110]. De petits logiciels peuvent être installés sur un téléphone portable et permettent ensuite d'écouter l'environnement du téléphone[111]. 79

[105] PÉCLET, *Ayant mis un pied à New York, VisioWave regarde la Chine*. Ces techniques sont appliquées dans des aéroports (Londres, Paris, Stockholm et Zurich par exemple) et sur des réseaux de transports publics comme la Régie autonome des transports parisiens (RATP).

[106] Des systèmes à deux clés sont aussi envisageables : PFPDT, *16ème rapport*, p. 20.

[107] http://www.emitall.com/surveillance.php?privacy-protection&scrambling-technologies=privacy-protection-system et CARNIEL, *Protection de la sphère privée*.

[108] DELESSERT, *Les méthodes techniques de surveillance*, p. 189.

[109] KREIS / DELLEY / KAUFMANN, *et al.*, *La protection politique de l'Etat en Suisse*, pp 230-231.

[110] RUEGG / FLÜCKIGER / NOVEMBER, *et al.*, *Vidéosurveillance et risques dans l'espace à usage public*, p. 37.

[111] JACQUARD, *Quand espionner les téléphones portables devient un jeu d'enfant*; JACQUARD, *Quatre questions sur un «mouchard»*. Pour un exemple du logiciel développé par une société suisse : http://www.promibs.ch.

80 La prise de vues au moyen d'un appareil photo est similaire à la vidéosurveillance. Il arrive d'ailleurs souvent actuellement que les clichés proviennent de caméras de surveillance. Il existe néanmoins des téléobjectifs permettant de photographier quelqu'un à des centaines de mètres, avec une qualité que ne permet généralement pas une caméra.

81 En plus des portiques à rayons X, certains aéroports sont dotés de scanners corporels. Ces appareils produisent des images comme si la personne était nue, évitant ainsi une fouille. A la suite d'une tentative d'attentat sur un vol entre Amsterdam et Detroit le 25 décembre 2009, plusieurs pays ont installé ces scanners à titre expérimental dans les aéroports internationaux. Alors qu'une évaluation d'impact des scanners corporels de la Commission européenne est attendue suite à la demande du Parlement d'octobre 2008, de nombreuses interrogations subsistent aux niveaux éthique, juridique et technique[112].

8. Les données biométriques

a) En général

82 Les données biométriques recouvrent un large spectre de méthodes différentes[113]. Elles seront abordées globalement, puis quelques-unes d'entre elles seront étudiées séparément. La biométrie[114] consiste à convertir des caractéristiques physiques propres à chaque individu, tels le visage, la voix ou encore l'empreinte digitale, en une empreinte numérique[115]. Pour remplir son rôle, la donnée biométrique doit être universelle, unique, permanente, accessible

[112] BARTHET, *Quelles technologies alternatives aux scanners corporels* ; CHECOLA, *Le scanner corporel*; EICHENBERGER, *La Suisse n'échappera pas aux scanners corporels.* Sur la question des risques pour l'homme : IRSN, *Evaluation du risque sanitaire des scanners corporels*.

[113] Sur les différentes techniques biométriques : CAI, *La biométrie*, pp 10-19; YON, *Etude sur la biométrie*.

[114] Le terme exact est « anthropométrie », mais « biométrie » s'est imposé à cause de sa similitude avec son pendant anglais « biometrics ». Par commodité et pour suivre la majorité de la littérature, nous utiliserons « biométrie ».

[115] ARNAUD / LEIN / MATHÉ, *et al.*, *L'insertion de données biométriques dans les documents d'identité*, p. 1. Il existe de nombreuses autres définitions : CASTEX / ACCARDO, *Encadrement et risques de la biométrie*; CEYHAN, *La biométrie*, p. 64. Pour une réflexion philosophique et éthique : RIPPE, *Der menschliche Körper als Datenträger*.

et quantifiable[116]. Il existe deux grandes catégories de techniques biométriques[117] : celles fondées sur l'analyse morphologique et celles qui reposent sur l'étude du comportement. On parle également de caractéristiques physiologiques (passives) et de caractéristiques comportementales (actives). Ces caractéristiques physiques uniques et particulières d'une personne peuvent, du moins théoriquement, lui être attribuées en tous lieux et en tout temps avec une certitude quasi absolue.

L'ADN, l'empreinte digitale, la longueur des doigts, la structure du visage, la structure de l'iris, la rétine, la forme de l'oreille, le réseau veineux de la paume de la main ou d'un doigt, la peau, les odeurs ou encore les émanations de chaleur sont les principales caractéristiques physiologiques. Quant aux caractéristiques comportementales, il s'agit de la voix et son intonation, de l'écriture et la manière d'écrire, de la dynamique des attaques du clavier, ainsi que de la démarche et du mouvement. 83

Les données biométriques sont d'abord saisies et enregistrées sous forme de données brutes (empreintes) à l'aide d'une caméra, d'un microphone ou d'un autre capteur spécialisé. Ces données brutes sont ensuite traitées à l'aide d'un algorithme, afin de ne conserver que les éléments pertinents et utilisables. Il en résulte alors une signature (aussi appelé échantillon, gabarit ou encore « template »)[118]. Il existe actuellement un problème de standardisation de ces gabarits, car toutes les technologies ne répondent pas à des modes opératoires identiques[119]. Si les mêmes éléments ne sont pas toujours retenus lors de l'élaboration d'un gabarit, la moindre comparaison est impossible. 84

Le gabarit a l'avantage d'être beaucoup plus petit que les données d'origine, ce qui facilite le stockage. Une fois l'échantillon obtenu, il peut être comparé avec un autre échantillon. C'est ce qu'on appelle la vérification (comparaison 1 : 1 ou « one-to-one matching »). L'identification (comparaison 1 : n ou « one-to-many 85

[116] CNIL, *22ème rapport*, pp 158-159.

[117] Pour des définitions analogues : PRIVATIM, *Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données*, p. 4. Certains auteurs considèrent que les traces biologiques comme l'ADN constituent une catégorie à part qui doit être distinguée des caractéristiques physiologiques : CEYHAN, *La biométrie*, pp 64-65.

[118] CAI, *La biométrie*, pp 8-9.

[119] CEYHAN, *La biométrie*, p. 80.

matching ») consiste à comparer l'échantillon avec un grand nombre d'autres échantillons, généralement ceux d'une base de données. L'authentification est similaire à la vérification, mais elle implique la présence d'un tiers de confiance qui aura précédemment enregistré l'échantillon correspondant à la personne. Il s'agit également d'une comparaison 1 : 1. Le résultat obtenu n'est cependant plus simplement la concordance entre deux échantillons, mais la concordance entre un échantillon et l'échantillon d'une personne connue. Autrement dit, la vérification permet de savoir si des traces appartiennent à un individu, l'identification permet de savoir si l'individu figure dans la base de données, et l'authentification permet de savoir si l'individu est bien celui qu'il prétend être[120].

86 Une ressemblance à 100 % entre deux échantillons n'est presque jamais obtenue. La fiabilité des procédés biométriques est alors une question de probabilité. Elle dépend du seuil de décision prédéfini, soit le taux de ressemblance à partir duquel deux échantillons sont considérés comme identiques. Il faut ensuite tenir compte du fait qu'une partie de la population est impossible à enregistrer (iris très clair, handicap, impossibilité d'atteindre le capteur). C'est ce qui est appelé la défaillance à l'enregistrement (FTE, « Failure To Enroll »). Le taux de fausses acceptations (FA, fausses comparaisons, ou FMR « False Match Rate ») est la proportion d'individus déclarés identiques à tort, alors que le taux de faux rejets (FR, fausse « non-identification », ou FNMR, « False Non Match Rate ») est la proportion d'individus qui sont déclarés différents à tort. Ces deux taux sont inversement proportionnels, puisque si le seuil de ressemblance exigé est très élevé, on n'aura presque pas de fausses identifications, mais beaucoup de faux rejets (les deux échantillons légèrement différents d'une même personne ne se ressemblent pas assez). Alors que si le seuil est bas, il y aura peu de faux rejets, mais beaucoup de fausses admissions (deux personnes différentes, mais se ressemblant, donneront des échantillons considérés comme identiques)[121]. A cela s'ajoutent encore les failles des puces et des logiciels, qui peuvent être détournées ou piratées, ainsi

[120] Sur les différentes comparaisons possibles : CEYHAN, *La biométrie*, pp 65-66; DIDIER, *Biométries*, pp 41-42; PRIVATIM, *Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données*, pp 4-5.

[121] Sur les notions d'erreurs : CAI, *La biométrie*, p. 20; DIDIER, *Biométries*, pp 43-44; PRIVATIM, *Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données*, p. 6.

que l'usage de leurres biométriques (faux iris notamment) ou d'éléments anatomiques morts (les doigts par exemple)[122].

b) Les empreintes digitales et palmaires

L'utilisation des empreintes digitales est très ancienne, puisque les Chinois de la dynastie Tang (618-906) sont généralement considérés comme les premiers à les avoir utilisées pour authentifier les contrats, méthode qui a été reprise en 1858 dans un district des Indes britanniques par Sir William Herschel pour authentifier les contrats passés avec les hommes d'affaires indigènes[123]. Actuellement, la majorité des Etats membres du Conseil de l'Europe autorisent le prélèvement obligatoire des empreintes digitales et d'échantillons de cellules dans le cadre de procédures pénales[124]. 87

Les points caractéristiques des empreintes digitales sont les lignes tracées par les crêtes (en contact avec les capteurs) et les vallées (les creux). La prise d'empreintes digitales s'effectue à partir de ces points de contact et permet de détecter les minuties (terminaisons et bifurcations) propres à chaque individu[125]. 88

Depuis quelques années, les polices ne sont plus les seules à s'intéresser aux empreintes digitales. Les fabricants de composants électroniques ont rapidement compris l'intérêt de proposer des capteurs à très faible coût pour sécuriser l'accès aux ordinateurs, téléphones et autres assistants numériques personnels (PDA)[126]. Les systèmes policiers (AFIS, Automatic Fingerprint Identification Systems) se distinguent toutefois par leur capacité à identifier des personnes à partir du relevé des empreintes des dix doigts et à identifier des traces parcellaires d'empreintes digitales, souvent de mauvaise qualité, laissées sur les scènes de crimes. Ces systèmes ont actuellement des capacités impressionnantes, puisque celui dont s'est doté le FBI au milieu des années 90 89

[122] CEYHAN, *La biométrie*, p. 80.

[123] Pour un aperçu de l'histoire des empreintes digitales : CNIL, *21ème rapport*, pp 103-104.

[124] Arrêt S. et MARPER c. Royaume-Uni, no 30562/04 et 30566/04, § 45 , du 4 décembre 2008.

[125] Sur la technique d'enregistrement et de reconnaissance de l'empreinte digitale : CEYHAN, *La biométrie*, p. 80; CHAMPOD / LENNARD / MARGOT, *et al.*, *Fingerprints*; CAI, *La biométrie*, pp 10-12; CNIL, *21ème rapport*, pp 105-107.

[126] Pour une présentation des différents acteurs industriels sur le marché de la biométrie : DIDIER, *Biométries*, pp 45-46.

permet d'effectuer environ 40 000 recherches par jour sur une population de 40 millions de personnes[127].

90 Aujourd'hui, la biométrie par empreinte digitale représente plus de 50 % des techniques biométriques utilisées dans le monde[128]. Il s'agit d'une méthode qui a fait ses preuves et dont le coût reste modeste comparé aux autres méthodes biométriques. Les principales critiques concernent les falsifications potentielles et les modifications dues à l'âge, aux frottements, etc. Pour éviter certaines falsifications, certains capteurs sont couplés avec un matériel établissant la présence d'un doigt, en vérifiant par exemple les battements du cœur ou la pression sanguine[129].

91 Pour ce qui est de l'empreinte palmaire, ce sont les principales caractéristiques de la main qui sont mesurées : la forme et la géométrie générale de la main, la longueur et la largeur des doigts, les formes des articulations et le dessin formé par le réseau des veines. Cette technique présente toutefois un risque élevé d'erreur, au sein d'une même famille notamment[130]. Le centre de loisirs de Disneyland (Floride) recourt à une application biométrique fondée sur la géométrie de la main pour établir si un visiteur a ou non le droit d'accéder à tel ou tel service de loisirs du parc. Ce système est toutefois anonyme et n'a pas pour objet d'identifier les visiteurs[131].

c) Les données génétiques

92 L'ADN (acide désoxyribonucléique) est une molécule immensément longue qui porte l'information génétique d'un individu. Il est comparable à un « texte » qui comporte trois milliards de « lettres ». Seules certaines parties de ce texte ont un sens, ce sont les gènes. Ainsi, seul 1 % environ de l'ADN humain présent dans

[127] Sur les systèmes AFIS utilisés par les polices : CEYHAN, *La biométrie*, p. 69; DIDIER, *Biométries*, pp 46-47.

[128] DIDIER, *Biométries*, p. 50.

[129] CASTEX / ACCARDO, *Encadrement et risques de la biométrie*. En 2009, la Section Services AFIS-ADN (le centre national de prestations de l'Office fédéral de la police pour l'identification biométrique des personnes sur la base d'empreintes digitales et palmaires ou de l'ADN) a traité environ 155 000 demandes d'identification, soit 27 000 sur la base de profils d'ADN et 128 000 au moyen d'empreintes digitales (FEDPOL, *Rapport 2009*, p. 69.).

[130] CASTEX / ACCARDO, *Encadrement et risques de la biométrie*.

[131] CNIL, *21ème rapport*, p. 101.

le génome contient une information génétique (ADN codant), une partie importante de l'ADN étant interrompue par des segments ne contenant pas de gènes (ADN non codant). Chaque individu possède une structure particulière. C'est une spécificité qui permet l'identification d'un individu par l'analyse de son ADN[132].

Le « texte » de l'ADN est extrêmement similaire entre deux individus. On trouve toutefois, dans les parties non codantes, des éléments répétitifs à plusieurs milliers d'endroits comme si l'ADN bégayait. Ces répétitions et leur nombre varient d'un individu à l'autre et sont précisément exploitées pour procéder à une identification[133]. 93

L'analyse des séquences non codantes ne permet pas aujourd'hui de tirer de conclusions relatives à l'état de santé d'un individu, et ne fournit pas d'informations sur son ascendance, contrairement à la partie codante de l'ADN. Les caractères génétiques répétitifs (on parle souvent de marqueurs génétiques) peuvent être analysés en exploitant les différences de taille entre les variantes, soit le nombre de répétitions. Un profil est ensuite établi. C'est la comparaison de ce profil avec un autre ou avec une base de données contenant d'autres profils qui est intéressante et permettra de déterminer si deux mêmes profils existent. 94

Les marqueurs analysés doivent être les mêmes pour qu'une comparaison soit possible. Si les marqueurs sont les mêmes, on dit qu'il y a concordance. Pour être certain que deux profils concordent, il faudrait comparer tous les marqueurs, ce qui prendrait énormément de temps. On se limite dès lors à en analyser un certain nombre. Plus leur nombre est important, plus le risque d'erreur est faible. Selon Raphaël Coquoz, il y a une chance sur vingt qu'un individu pris au hasard ait le même profil que celui qui est analysé si on retient un seul marqueur 95

[132] Pour une définition analogue : BOMMER, *DNA-Analyse*, pp 132-133; COQUOZ, *Profils ADN*, pp 161-162; ROHMER, *Spécificité des données génétiques*, pp 6-7. Pour une définition du profil ADN par le Tribunal fédéral, ainsi que les buts de son utilisation : ATF 128 II 259, 265-267, Z., du 29 mai 2002, et les nombreuses références citées. Le lecteur qui s'intéresse à une approche scientifique plus complète est invité à consulter COQUOZ / TARONI, *Preuve par l'ADN*.

[133] Sur l'utilisation de l'ADN dans le cadre d'une identification : COQUOZ, *Profils ADN*, pp 162-163; ROHMER, *Spécificité des données génétiques*, pp 63-64; VOSER, *Kommentar zu Art. 255-259 StPO*, pp 371-375.

génétique. Avec trois marqueurs, il y a une chance sur 8000, et avec six marqueurs plus qu'une chance sur 64 millions[134]. Il convient toutefois de ne pas perdre de vue qu'il s'agit toujours de probabilités et que celles-ci dépendent des valeurs variables de probabilité *a priori*[135]. On peut en revanche être certain que deux profils ne sont pas les mêmes, puisqu'il suffit alors qu'un marqueur soit différent.

96 Les prélèvements d'ADN sont faciles à effectuer, étant donné que l'ADN est présent dans toutes les cellules du corps humain. Lorsque le « donneur » est consentant, un frottis de la muqueuse jugale[136] ou une prise de sang sont généralement privilégiés. Si le consentement du « donneur » ne peut pas être recueilli (notamment sur une scène de crime où l'auteur n'attend en principe pas l'arrivée des enquêteurs), on recherchera avant tout des traces de sang, de sperme ou de salive, des cheveux et des poils[137]. Un individu laisse environ 50 000 traces chaque jour[138]. L'ADN est ensuite extrait de cette trace, multiplié et analysé. L'ADN ou le profil établi peuvent être stockés pour un usage ultérieur[139].

97 Une autre particularité des données génétiques réside dans le fait que lors d'une comparaison de traces inconnues avec une base de données de profils enregistrés, il est possible que le résultat ne soit pas identique mais très proche d'un profil connu. On peut dans ce cas déduire que les traces inconnues appartiennent à un parent proche du profil connu, bien que le profil exact de la personne recherchée ne soit pas enregistré[140].

98 Les données génétiques figurent très certainement parmi les méthodes d'identification les plus fiables. Une certaine prudence est toutefois de mise,

[134] COQUOZ, *Profils ADN*, p. 166.

[135] Pour une analyse critique et scientifique des probabilités en matière d'ADN, voir notamment TARONI / AITKEN, *Probabilités et preuve par l'ADN*; TARONI / MANGIN, *La preuve ADN, les probabilités, les experts et les juristes*.

[136] Frottement effectué au moyen d'un bâtonnet d'ouate sur la paroi interne de la joue.

[137] Pour une liste de traces utilisables : COQUOZ, *Profils ADN*, pp 165-166.

[138] BUSCH, *DNA-Profile*, pp 13-14.

[139] Sur le traitement des données dans le cadre d'analyses d'ADN : PFPDT, *16ème rapport*, pp 46-48.

[140] TARONI / CASTELLA / RIBAUX, *et al.*, *Partial DNA profiles and familial searching*, p. 10.

alors que d'aucuns considèrent aujourd'hui l'analyse ADN comme la reine des preuves. En effet, quand bien même le propriétaire d'un cheveu retrouvé sur une scène de crime serait identifié, cela ne fait pas encore de lui l'auteur du crime.

Par ailleurs, le résultat chiffré d'une probabilité peut également être trompeur et varier grandement selon la méthode utilisée, alors qu'il est retenu généralement comme une vérité absolue plutôt que comme une interprétation du résultat. Il ressort d'un rapport du Fonds national de la recherche scientifique que les experts n'évaluent pas la complexité d'un lien dans les affaires criminelles, qu'ils n'abordent pas toujours correctement les statistiques à la base des calculs de paternité, qu'ils n'exploitent pas tout à fait correctement l'argument probabiliste et que l'argument statistique n'est pas correctement compris par les étudiants en droit qui sont enclins à accepter des argumentations fallacieuses[141]. Même si ces critiques concernent les analyses génétiques, elles sont également pertinentes pour toutes les autres données biométriques, voire d'autres résultats exprimés sous forme de probabilité. 99

d) La reconnaissance faciale

La reconnaissance faciale se base sur la structure géométrique du visage d'une personne (distance entre les yeux, avec le nez, le menton, les os de la joue, la forme des yeux, du nez, etc.)[142]. 100

La ville de Newham, dans la banlieue de Londres, est équipée depuis 1998 d'un système de vidéosurveillance couplé à un logiciel de reconnaissance automatique des visages (Mandrake) qui permet d'alerter la police lorsqu'une personne présente dans ses fichiers passe devant une de ses caméras. En Suisse, l'aéroport de Zurich utilise depuis 2003 un système de vidéosurveillance et de reconnaissance des visages à la porte de débarquement de certaines lignes pour lutter contre l'immigration illégale[143]. Lors du Super Bowl organisé en janvier 2001 à Tampa en Floride, les spectateurs entrant dans le stade ont été filmés par des caméras de vidéosurveillance et les images étaient couplées, en temps réel, à un système informatique reposant sur la reconnaissance de 128 traits caractéristiques du visage. Les visages des spectateurs ont ainsi été numérisés et 101

[141] TARONI / MANGIN, *La preuve ADN, les probabilités, les experts et les juristes*, p. 109.
[142] CAI, *La biométrie*, pp 13-14.
[143] DFJP, *Rapport sur la vidéosurveillance*, p. 17.

comparés à une base de données. L'opération de comparaison prenait moins d'une seconde, mais le résultat final était plutôt décevant. Lors d'élections présidentielles en 2001 en Ouganda, chacun des 10 millions d'électeurs a reçu une carte d'électeur à puce comportant le gabarit de leur visage. Lors du vote, le visage de l'électeur était comparé en temps réel par logiciel à celui enregistré dans la carte présentée, afin d'empêcher une personne de voter à la place d'une autre[144]. Des projets sont en cours de mise au point en Grande-Bretagne pour utiliser les caméras de vidéosurveillance du réseau routier afin de reconnaître les conducteurs et passagers des véhicules.

e) L'iris et la rétine

102 La reconnaissance de l'iris ou de la rétine est encore peu présente, bien que ces techniques soient efficaces. La reconnaissance de l'iris est utilisée dans certains aéroports américains pour contrôler l'accès du personnel sur le tarmac. Quant à la reconnaissance de la rétine, elle est utilisée pour une partie du personnel du FBI, ainsi que des militaires américains, suisses, espagnols et suédois[145].

103 La reconnaissance de l'iris consiste à scanner l'iris de l'œil, plus précisément la structure de l'anneau à couleur autour de la pupille, alors que la reconnaissance rétinienne se fait par le balayage des vaisseaux sanguins de la rétine à l'aide d'un laser traversant la pupille. L'iris contient entre 50 et 250 points caractéristiques et la rétine environ 400, qui ne varient pas au cours de la vie. L'iris et la rétine de chaque œil sont différents et des jumeaux ont également des iris et rétines différents. Pour procéder à la reconnaissance, il est nécessaire d'avoir un éclairage restreint et de se trouver à proximité du capteur, soit à quelques centimètres au maximum pour la rétine, et à 60 cm pour la reconnaissance de l'iris[146].

[144] Pour des exemples d'utilisation de la reconnaissance faciale : CASTEX / ACCARDO, *Encadrement et risques de la biométrie*; CEYHAN, *La biométrie*, p. 70; CNIL, *22ème rapport*, pp 162-163. Le Département fédéral de la défense, de la protection de la population et des sports a autorisé à fin avril 2008 des tests d'identification biométrique afin de repérer les supporters violents interdits de stade ou de périmètre.

[145] Pour des exemples d'utilisation de la reconnaissance de l'iris et de la rétine : CEYHAN, *La biométrie*, p. 70; CNIL, *22ème rapport*, p. 160.

[146] Sur les caractéristiques de la reconnaissance de l'iris et de la rétine : CASTEX / ACCARDO, *Encadrement et risques de la biométrie*; CAI, *La biométrie*, pp 14-16; CNIL, *22ème rapport*,

Cette technique est sûre et précise, mais a un coût élevé. Elle est en outre inadaptée pour les aveugles, et les conséquences à long terme pour la santé ne sont pas encore connues. 104

f) La reconnaissance vocale

La voix et son intonation permettent également d'identifier un individu[147]. Le Colombien Pablo Escobar a été retrouvé en 1993 à cause d'un appel téléphonique lors duquel sa voix a été reconnue. La NSA (National Security Agency) a mis sur pied, dans le cadre du système d'écoutes Echelon, un dispositif de reconnaissance des voix et d'écoute des conversations dans le monde entier à partir des caractéristiques vocales propres des individus mis sous surveillance[148]. Une conversation peut être repérée en fonction de certains mots prononcés (contenu) ou de la voix qui s'exprime (auteur), ou encore une combinaison des deux : certains mots prononcés par une voix particulière seulement seront sélectionnés. La technologie n'a pas encore atteint un niveau de maturité permettant son utilisation à large échelle dans les domaines commerciaux ou forensiques, même si les progrès sont importants[149]. D'autres données biométriques plus faciles à appréhender sont souvent préférées. 105

g) Autres

D'autres caractéristiques génétiques peuvent également être envisagées[150]. L'écriture, en comparant deux échantillons ou en analysant le comportement lors de l'écriture (pression, angle du stylo, vitesse, etc.), est peu utilisée en pratique, si ce n'est la comparaison de signatures dont la précision est réduite[151]. Une analyse semblable est possible si la personne écrit avec un clavier : on s'intéressera alors à la dynamique des attaques du clavier (mesure des 106

p. 160; PRIVATIM, *Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données*, p. 16.

147 CAI, *La biométrie*, p. 16; MEUWLY, *Le mythe de "l'empreinte vocale" (I)*; MEUWLY, *Le mythe de "l'empreinte vocale" (II)*; MEUWLY, *Reconnaissance de locuteurs*, pp 5 et 11-28.

148 CEYHAN, *La biométrie*, pp 69-70.

149 MEUWLY, *Reconnaissance de locuteurs*, p. 143.

150 Pour une vue d'ensemble : CAI, *La biométrie*, pp 10-19; PRIVATIM, *Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données*, pp 16-17.

151 CAI, *La biométrie*, p. 17.

hésitations après deux pressions de touches, durée de la pression, position du doigt, etc.)[152]. Ce genre d'analyses reste généralement assez imprécis.

107 Peu connue, l'analyse de la démarche et du mouvement est plus précise que supposée. Elle dépend néanmoins de nombreux facteurs (souliers, habillement, état de la personne, etc.). Ce sont essentiellement la suite des pas, la longueur de ceux-ci et le déroulement du mouvement en général qui sont analysés.

9. Les puces RFID

a) En général

108 Un système d'identification par radiofréquences (RFID[153]) est constitué de deux éléments[154] : un marqueur (également appelé transpondeur ou « tag ») et un lecteur (également appelé interrogateur). Le marqueur RFID contient une petite quantité de mémoire pour la conservation des données. 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.

109 Le marqueur est qualifié de passif, car il n'a pas besoin d'énergie propre pour communiquer avec le lecteur. C'est ce dernier qui émet l'énergie qui sert à alimenter le marqueur et communiquer avec lui, sous la forme d'une onde radio à une fréquence donnée. La distance maximale pour assurer un fonctionnement correct dépend de la fréquence radio utilisée, et de la qualité du matériel. Elle est généralement comprise entre quelques centimètres et quelques mètres, voire jusqu'à plusieurs dizaines de mètres si le marqueur comporte une batterie.

110 La communication se base sur la propagation d'ondes radio, ce qui signifie que marqueur et lecteur n'ont pas besoin de « se voir » (comme pour les codes à barres). Il est donc possible de lire un grand nombre d'objets marqués presque

[152] CAI, *La biométrie*, pp 17-18.

[153] Radio Frequency Identification.

[154] Pour une définition et une description du fonctionnement des puces RFID : HODGES / MCFARLANE, *RFID*, pp 62-65. Pour un aperçu des possibilités d'utilisation des puces RFID et les problèmes soulevés (avec de nombreux liens) : CAI, *La technologie d'identification par radiofréquence*. Pour une approche technique : FINKENZELLER, *RFID-Handbuch*. Pour les questions liées à la protection des données lors de l'utilisatoin de puces RFID : PFPDT, *17ème rapport*, pp 34-36.

simultanément lorsqu'ils passent à proximité d'un lecteur. Mais cela implique également que la transmission peut être détectée par un autre équipement, qu'un lecteur non autorisé peut communiquer avec les marqueurs ou qu'un équipement pourrait générer des interférences et empêcher la communication entre un marqueur et un lecteur.

Actuellement, les marqueurs sont couramment utilisés pour la gestion de stocks (habits, agroalimentaires,…), la gestion de chaînes logistiques, l'enregistrement automatique des livres empruntés et rendus dans les bibliothèques ainsi que le contrôle du classement des ouvrages sur les rayons, les systèmes antivol, le contrôle d'accès à certains bâtiments, le paiement aux cafétérias, l'utilisation de photocopieurs, ordinateurs et autres imprimantes, etc. Une seule et même carte, contenant une puce RFID, peut remplir toutes ces fonctions (prestations multiservices). C'est le cas des cartes fournies par la société Polyright à de nombreuses universités, écoles et entreprises suisses[155]. Dans un avenir proche, les puces RFID devraient également permettre d'éviter de faire la queue à la caisse du supermarché. Elles indiqueront aussi à notre frigidaire que des produits sont périmés, ou qu'il n'y a plus de lait et qu'il est nécessaire d'en racheter. Elles sont également envisagées pour tracer les bagages dans les aéroports[156]. On mentionnera encore que le premier fournisseur mondial de puces RFID est une entreprise suisse, la société fribourgeoise Sokymat[157]. 111

L'Université catholique de Louvain en Belgique est en train de développer un marqueur RFID à placer dans les dents, afin de pouvoir identifier l'individu lorsque son corps est méconnaissable (accident d'avion, incendie, etc.)[158]. Il semble toutefois plus facile de fausser une puce RFID qu'une empreinte dentaire. Quoi qu'il en soit, ce type de marquage est déjà utilisé dans certains hôpitaux ou établissements médico-sociaux, pour éviter de perdre ou mélanger les prothèses dentaires ! 112

[155] Polyright SA est une société suisse membre du Groupe Kudekski et du Groupe Securitas Suisse, http://www.polyright.com.

[156] CHECOLA, *Le scanner corporel*.

[157] http://www.sokymat.com et http://sokymat.aaitg.com.

[158] Emission nouvo du 26 avril 2007, http://www.nouvo.ch/120-3.

113 A l'instar d'autres composants informatiques, et malgré leur petite taille, les puces RFID peuvent contenir des virus ou des vers[159]. Si la place n'est pas suffisante sur la puce, elle pourrait ne contenir qu'un code en JavaScript, qui infecterait les composants web du lecteur et le chargerait alors de compléter les données manquantes par Internet. Comme il n'est pas possible de réécrire sur la puce RFID, un virus ne peut pas y être introduit. Une puce réalisée pour contenir un virus, ou infectée lors de sa fabrication, peut en revanche contaminer les lecteurs et fausser le résultat des données lues, y compris lors de la lecture d'autres puces « saines », par exemple en modifiant la base de données à laquelle correspondent les puces[160].

114 Dans le cadre des mesures de surveillance, les puces RFID interviennent à deux titres. Premièrement, il est possible de déposer un marqueur sur l'objet de la surveillance, et être ainsi immédiatement informé de son passage à un point de contrôle, ou du fait qu'il quitte le champ de lecture. Il suffit ensuite de passer à proximité du marqueur pour retrouver l'objet[161]. Le recours aux marqueurs RFID est particulièrement intéressant en raison de leur faible coût, ce qui n'oblige pas à les récupérer en fin de surveillance. Un marqueur revient actuellement à quelques centimes et un lecteur à quelques centaines de francs, et ces coûts devraient encore baisser[162].

115 Deuxièmement, on peut lire des marqueurs existants et utilisés dans un autre but. On peut ainsi obtenir de précieuses informations commerciales sur un objet, les coordonnées du détenteur d'une carte permettant de faire des photocopies ou encore ses droits accès (tant en termes de locaux que de périphériques informatiques par exemple).

[159] Un groupe de chercheurs hollandais en a fait la démonstration lors d'un congrès à Pise (Italie) en mars 2006 : http://www.rfidvirus.org.

[160] Sur les problèmes de sécurité posés par les puces RFID et des propositions de solutions : LECHNER, *RFID*.

[161] Pour des exemples d'utilisation de puces RFID à l'insu de la personne concernée : APSIS, *RFID and Consumers' Privacy Rights*.

[162] HODGES / MCFARLANE, *RFID*, p. 66.

b) Dans les papiers d'identité

La technologie RFID est enfin utilisée pour les nouveaux papiers d'identité[163]. A la demande des Etats-Unis et sur la recommandation de l'Organisation de l'aviation civile internationale (OACI), les nouveaux papiers d'identité sont munis d'une puce contenant des données biométriques, notamment une photo du titulaire[164]. Les USA et les pays de l'UE ont introduit ce type de permis[165]. C'est aussi le cas des passeports suisses 06 produits depuis septembre 2006 dans le cadre d'un projet pilote[166]. La puce contenait, outre les données qui sont imprimées dans le passeport, une photo numérisée qui est la même que celle figurant dans le passeport. 116

Depuis mars 2010, il n'est plus possible d'obtenir un passeport suisse qui ne contienne pas de données biométriques[167]. Ce nouveau passeport contient une photographie du visage de face (élément biométrique principal) et deux empreintes digitales (élément biométrique secondaire)[168]. Les données peuvent être lues par les appareils de lecture à une courte distance, ce qui permet de comparer électroniquement l'image numérisée du visage et celle de la personne qui présente le passeport. La vérification de l'identité est effectuée de façon automatisée et accélérée, les falsifications de passeports sont plus difficiles, et la vérification de l'identité des voyageurs est accélérée. La protection des données 117

[163] Sur l'identité biométrique et ses risques : GHERNAOUTI-HÉLIE, *La cybercriminalité*, pp 108-114.

[164] Voir à ce sujet le chapitre 8. Les données biométriques, p. 52 ci-dessus.

[165] Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres modifié par le Règlement (CE) n° 44/2009 du Parlement européen et du Conseil du 28 mai 200529.

[166] PFPD, *13ème rapport*, p. 44.

[167] A l'exception du passeport provisoire (appelé aussi passeport d'urgence) qui est une variante du passeport 03. Il n'est toutefois délivré qu'à des conditions particulières et sa validité est en principe limitée à la durée du séjour. La carte d'identité suisse ne contient pas d'éléments biométriques, mais les titres de séjours pour étrangers (Livrets B ou L) seront munis au plus tard en mai 2011 d'une puce contenant une image faciale et deux images d'empreintes digitales : ODM, *Commentaire relatif à l'introduction de données biométriques dans le titre de séjour*.

[168] Art. 14a OLDI (Ordonnance sur les documents d'identité des ressortissants suisses, RS 143.11).

et la sécurité des informations sont en outre garanties grâce à des signatures électroniques et des clés[169].

118 Nous avons vu précédemment ce qu'étaient les données biométriques. Intéressons-nous maintenant aux conséquences de la présence de celles-ci dans un marqueur RFID, puisque contrairement aux informations officielles rassurantes, les voix de nombreux scientifiques s'élèvent contre ces passeports. La Commission d'accès à l'information du Québec se demande d'ailleurs si l'incorporation de puces RFID contenant des renseignements personnels dans des passeports ou permis de conduire, n'aura pas comme effet d'augmenter les risques d'usurpation d'identité[170].

119 Le principal danger que représente la présence d'une puce RFID dans un passeport est la possibilité de la lire à distance. Lorsque l'on sait que le gouvernement américain a pour objectif de pouvoir contrôler les passagers d'un autobus entier depuis l'extérieur de celui-ci, on doit bien admettre que les passeports sont ou seront très prochainement lisibles à une distance qui dépasse quelques dizaines de centimètres. Les premières expériences ont montré qu'avec un matériel bon marché et accessible à tout un chacun, le passeport hollandais par exemple pouvait être lu à une distance de 30 centimètres[171].

120 Les données de la puce RFID ne sont pas librement accessibles. Il faut pour communiquer avec le contenu de la puce avoir une clé d'accès. Cette clé est un nombre obtenu à l'aide des informations figurant sur la zone à lecture optique de la carte, ce qui signifie qu'elle ne peut être connue qu'en connaissant l'algorithme (partie de la clé connue de l'appareil de lecture) et les données figurant sur le passeport (partie de la clé en main du possesseur du passeport).

121 Steve BOGGAN et Adam LAURIE ont réussi en quatre heures seulement à trouver la clé d'un passeport britannique neuf, sans le sortir de son enveloppe et en connaissant seulement le nom et la date de naissance du titulaire[172]. Pour forcer la clé, ils ont recouru à ce que l'on appelle une méthode d'attaque en

[169] *Message du CF concernant le passeport biométrique*, pp 4918-4919.
[170] CAI, *La technologie d'identification par radiofréquence*, p. 7.
[171] BOGGAN, *Cracked it.*
[172] L'auteur de l'article explique en détails son expérience : BOGGAN, *Cracked it.*

force brute, c'est-à-dire en essayant toutes les combinaisons possibles. Aucune mesure n'est prise pour empêcher ces attaques, alors que si l'on procède de la sorte avec le code d'une carte de crédit, elle sera bloquée après trois essais.

En été 2009, Adam LAURIE a réussi à pirater la nouvelle carte d'identité britannique munie d'une puce RFID. A l'aide d'un simple téléphone mobile et d'un ordinateur portable, il a trouvé l'algorithme de sécurité de la puce RFID et copié toutes les données qu'elle contenait, puis cloné la carte d'identité en seulement 12 minutes. Il a également réussi à modifier toutes les données de la nouvelle carte, soit les noms et prénoms, la date de naissance, les caractéristiques physiques et les empreintes digitales de son titulaire, mais également des informations comme le droit aux prestations sociales[173]. 122

Dès le moment où il est possible de lire les données contenues sur la puce, il est également possible de la copier comme l'a démontré Lukas GRUNWALD lors de la conférence Black Hat 2006 à Las Vegas[174]. Un nouveau faux passeport est obtenu, sans que le détenteur de l'original ne puisse le remarquer comme dans le cas d'un vol. Des membres du groupe The Hacker´s Choice auraient réussi à piéger un système de contrôle de passeport RFID dans un aéroport à Amsterdam, après avoir créé un faux passeport biométrique avec l'identité d'Elvis PRESLEY[175]. Pour les deux auteurs précités, les choses seraient plus compliquées en cas de comparaison des empreintes digitales et de reconnaissance faciale, puisque les données contenues sur la puce sont celles du vrai passeport et diffèrent de celles du porteur du faux passeport. Ils soulignent toutefois que les premières peuvent être falsifiées, d'autant plus facilement si le contrôle est automatisé, et que la seconde n'est actuellement pas encore suffisamment au point. Cet argument est renforcé par une étude de l'Université de Westminster qui arrivait à la conclusion que la sécurité n'était pas renforcée par la présence de photos sur les cartes de crédit[176]. De plus, les passeports étant réputés plus sûrs, une confiance plus grande leur sera accordée et la personne chargée de contrôler si la photo contenue sur la puce correspond au visage du 123

[173] BOGGAN, *New ID cards are supposed to be unforgeable*.
[174] SCHNEIER, *Hackers Clone RFID Passports*.
[175] http://freeworld.thc.org/thc-epassport.
[176] Etude citée dans BOGGAN, *Cracked it*.

porteur du passeport sera moins attentive puisque théoriquement ce passeport ne peut pas être un faux et que l'original n'a pas été volé.

124 Nombreux sont ceux qui ont dénoncé le risque que la puce RFID serve de déclencheur pour une bombe, qui n'exploserait qu'au passage de ressortissants d'un pays déterminé. Si dans un premier temps cela ressemblait plus à une rumeur qu'à un fait scientifique avéré, le risque est bien réel, comme l'a démontré la société Flexilis. La lecture des données devrait être protégée par la clé d'accès et le fait que le passeport ne peut pas être lu lorsqu'il est fermé. Toutefois, il suffit que le passeport soit légèrement entrouvert, ce qui est fréquemment le cas dans une poche ou un sac, pour que la puce puisse être lue. Ensuite, même en l'absence de la clé, l'empreinte des données émise permet d'identifier le pays[177]. Il faut dès lors admettre que le risque est bien réel de voir des tiers identifier le pays dont sont ressortissants les porteurs des passeports biométriques et d'utiliser automatiquement et instantanément ces informations.

125 Une autre méthode permettant d'utiliser les données d'un passeport qui n'est pas le sien consiste à détourner le signal radio d'un autre passeport, de sorte que lors d'un contrôle ce ne sont pas les données de la personne contrôlée, mais celles d'une autre puce à proximité qui sont transmises[178]. Si une photographie biométrique est transmise et qu'elle ne correspond pas au visage du porteur du passeport, cette méthode est inutile. En revanche, elle permet de passer sans encombre un contrôle visant à détecter la présence de certaines personnes (liste noire) dans un lieu, un véhicule ou d'autoriser le passage d'une porte.

10. La localisation par satellite

126 Le Système mondial de navigation par satellites (GNNS) s'appuie sur la triangulation tridimensionnelle[179]. Les satellites (six pour le GPS et trois pour Galileo) gravitent autour de la terre sur plusieurs plans orbitaux et émettent des signaux contenant un message d'identification qui indique quel satellite émet le signal, une éphéméride avec la position de tous les satellites exploités et l'heure

[177] FLEXILIS, *RFID e-Passport Vulnerability*. L'étude est illustrée d'une vidéo, disponible à l'adresse http://www.youtube.com/watch?v=-XXaqraF7pI.

[178] SCHNEIER, *RFID Cards and Man-in-the-Middle Attacks*.

[179] Pour une présentation des systèmes de navigation par satellite et leur fonctionnement : OOSTERLINCK, *Localisation par satellite*, pp 88ss.

exacte à laquelle le signal a été émis. Avec ces informations, le récepteur sur terre peut alors calculer la distance le séparant du satellite et déterminer sa position dès qu'il a reçu les signaux d'au moins trois satellites[180].

Le GPS (Global Positioning System) est un système américain d'origine militaire qui donne actuellement un signal crypté et extrêmement précis réservé aux usages militaires, ainsi qu'un signal librement utilisable. Jusqu'au mois d'avril 2000 au moins, des erreurs étaient délibérément introduites pour diminuer la fiabilité du signal en cas d'utilisation non amicale. L'Union soviétique possédait également un système similaire (GLONASS), partiellement repris aujourd'hui par la Russie. Quant au programme européen Galileo, il a pour objectif de créer un GNNS européen autonome extrêmement précis et interopérable avec les autres systèmes existants (GPS et GLONASS). Galileo sera le premier système de navigation par satellite conçu par et pour des besoins civils, ainsi que conçu et exploité sous contrôle public. Le gouvernement indien a annoncé en 2006 qu'il allait développer son propre système de navigation, l'IRNSS (Indian Regional Navigational Satellite System), alors que la Chine développe de son côté le projet Beidou, un autre système de positionnement. 127

Un système de navigation n'a, à l'origine, pas pour but de localiser, mais de permettre à l'utilisateur de connaître sa position. Pour permettre à des tiers de connaître la position ou le déplacement de l'utilisateur, il est nécessaire de combiner le système de localisation avec un système de communication qui sera à même de transmettre la position ainsi définie. 128

Actuellement, l'opérateur téléphonique Sunrise, associé à l'entreprise CPR Groupe, propose en Suisse un service de géolocalisation, appelé geogeny[181]. Il fait appel aux systèmes de communication SMS, GSM et GPRS, et de localisation GPS. Il a été utilisé pour la première fois en 2003 129

[180] En connaissant la distance séparant le récepteur du satellite, on peut déduire que le récepteur se situe quelque part à cette distance du satellite, ce qui représente une sphère. Le point d'interception des trois sphères représente l'emplacement du récepteur. L'horloge du récepteur étant généralement moins précise que celles embarquées dans les satellites, on recourt au signal d'un quatrième satellite pour compenser l'éventuel décalage de temps.

[181] http://www.geogeny.ch.

dans le cadre de l'opération « Nez Rouge »[182]. Quant à la police cantonale neuchâteloise, elle a développé en collaboration avec la haute école ARC ingénierie du Locle un système de géopositionnement individuel des policiers au travers de leur téléphone portable GPS[183]. Certaines entreprises utilisent également un système de localisation par satellite de leurs véhicules d'entreprise[184]. Les projets visant à taxer l'automobiliste en fonction des trajets réalisés reposent sur les mêmes méthodes techniques[185].

130 Une nouvelle utilisation est apparue en Suisse il y a quelques années. Il s'agit de « boîtes noires » installées par certains assureurs sur les véhicules de leurs clients. Ces boîtiers permettent de connaître les déplacements effectués, le type de conduite, la durée de freinage, etc., soit en consultant physiquement l'appareil, soit directement à distance et en temps réel[186]. D'autres modèles incluent également le lieu et la vitesse du véhicule.

11. Les autres méthodes de localisation

131 De la même manière qu'il est possible de surveiller un téléphone mobile, il est possible de connaître l'ensemble des communications transitant ou ayant transité à un moment donné par une antenne de téléphonie[187]. Le téléphone est alors localisé dans le champ de portée de l'antenne, qui peut varier de 50 mètres dans

[182] Communiqué de presse SUNRISE du 17 décembre 2003, http://www.geogeny.ch/pdf/sunrise_171203_fr.pdf.

[183] Communiqué de presse de la police cantonale neuchâteloise du 6 mars 2008, http://www.ne.ch/neat/documents/securite/police_canton/RelationsMedias_1523/Comm_PCNE_6012/Defisetmutations.pdf.

[184] Un tel système de surveillance est admissible s'il est justifié par des impératifs de sécurité ou des motifs tenant à l'organisation et à la planification du travail. Il est en revanche interdit par l'art. 26 OLT 3 s'il vise uniquement ou essentiellement à surveiller le comportement des travailleurs : BGE 130 II 425, 438, X., du 13 juillet 2004.

[185] GRIMM, *Pay as you drive*.

[186] Emission nouvo du 7 juin 2007, disponible à l'adresse http://www.nouvo.ch/123-1, et VOGGENAUER-VON BOTHMER, *Welche Daten*. Sur les données électroniques enregistrées dans les véhicules : GARSTKA, *Der "nackte" Automobilist*. De telles boîtes noires pourraient être imposées judiciairement dans le cas de graves infractions routières, par exemple sous la forme d'une règle de conduite conditionnant l'octroi du sursis.

[187] STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 106. Sur les différentes méthodes de localiser un téléphone portable et leur fonctionnement : CARTIER, *Localisation des téléphones portables*.

les zones urbaines à plusieurs kilomètres dans les régions rurales[188]. Pour définir une zone plus précise, il faut que le téléphone active une autre antenne. Cela arrive notamment lorsque le téléphone est déplacé, ou si plusieurs antennes couvrent un même espace. Différentes antennes activées successivement permettent alors de suivre le parcours effectué. C'est ainsi que les autorités françaises ont retrouvé Yvan COLONNA en 2003 dans une bergerie corse, alors qu'il était recherché depuis plus de quatre ans dans le cadre de l'enquête sur le meurtre du préfet ERIGNAC[189].

En cas d'appel en Suisse depuis un téléphone mobile vers les numéros d'urgence, les réseaux mobiles transmettent à une banque de données nationale centralisée des informations sur la zone où se trouve l'appelant[190]. Depuis juillet 2008, Swisscom transmet à un partenaire localisé aux Pays-Bas les données anonymisées concernant la position de ses clients sur les routes suisses, ainsi que leur vitesse de déplacement, dans le but d'établir des cartes de trafic en temps réel[191]. 132

Mais il n'est pas uniquement possible de savoir si un numéro précis était présent à proximité d'une antenne. La liste de tous les téléphones ayant activé cette antenne ou ayant émis ou reçu un appel transitant par cette antenne peut aussi être éditée. Cela veut dire que l'on peut vérifier si un numéro donné était présent à cet endroit à un moment précis, mais aussi que l'on peut savoir qui était présent à cet endroit et à ce moment, sans connaître *a priori* le numéro de la personne que l'on recherche. A la suite d'un hold-up à Lausanne, un juge d'instruction avait demandé le relevé des 1000 numéros de téléphone qui avaient transité par une antenne précise, car il soupçonnait l'auteur du hold-up d'avoir utilisé un téléphone français, dont le numéro aurait pu être facilement isolé des numéros locaux[192]. 133

[188] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 119.
[189] SIGRIST, *Reflex*, p. 35.
[190] Communiqué de presse de l'OFCOM du 18 septembre 2006.
[191] PLATTNER, *L'œil de Swisscom*.
[192] SIGRIST, *Reflex*, p. 37.

134 Le Massachusetts Institute of Technology (MIT) a développé un système de comptage et de localisation de grande envergure[193]. En s'appuyant sur les signaux émis par les téléphones portables et transmis par les opérateurs téléphoniques, le MIT a été capable de dresser en temps réel des cartes de quartiers entiers de Rome où étaient représentés les mouvements de population, les lieux les plus fréquentés, les embouteillages, etc. Ces techniques sont peu à peu mises à disposition du public. Il est désormais possible en France, par exemple, de localiser son portable ou celui de ses enfants sur Internet ou sa position directement sur une carte au moyen d'un téléphone portable[194].

135 Une des méthodes fréquemment utilisées pour localiser un téléphone portable est l'utilisation de messages fantômes[195]. Des SMS sont envoyés à intervalles réguliers, par exemple toutes les 30 secondes, mais ils n'apparaissent pas sur le téléphone du destinataire. L'expéditeur peut ainsi d'une part savoir si le téléphone est actif, respectivement quand est-ce qu'il est remis en activité si le message est reçu ultérieurement, et quelle antenne est activée[196].

136 La localisation d'un objet, le plus souvent d'un véhicule, peut aussi se faire à l'aide d'une balise préalablement installée et émettant des ondes radio. Il est alors possible de localiser l'objet à l'aide d'un récepteur, pour autant que la distance ne soit pas trop grande[197].

12. Les banques de données

137 La recherche informatique par recoupement de bases de données (*Rasterfahndung*) n'est pas récente. L'exemple le plus fameux est

[193] BRAFMAN, *Nous savons combien vous êtes !* Ce projet de 2006 est présenté de manière plus complète sur le site du MIT : http://senseable.mit.edu/realtimerome/. Une expérience similaire a été faite à Copenhague en 2008 : http://senseable.mit.edu/realtimecopenhagen/.

[194] CHARLES, *Votre portable vous espionne*.

[195] Aussi appelé ping, blind sms ou sms-blaster.

[196] Sur cette question: HANSJAKOB, *Die ersten Erfahrungen mit dem BÜPF*, pp 269-270. Contrairement à l'avis de cet auteur, l'envoi de sms fantômes devrait être considéré comme une mesure de surveillance de la correspondance par télécommunication même si le seul but poursuivi est de savoir si le téléphone est actif. A la différence d'un appel téléphonique, l'envoi de sms fantômes a pour vocation de ne pas être connu du destinataire et revêt donc un caractère secret, d'où une atteinte plus importante.

[197] ARZT, *Polizeiliche Überwachungsmassnahmen in den USA*, pp 46-48.

probablement l'arrestation le 9 juin 1979 de l'Allemand Rolf HEISSLER, membre de la fracion armée rouge RAF[198].

Tous les résultats des techniques présentées auparavant peuvent être conservés sous la forme de fichiers ou de banques de données. On trouve également d'autres banques de données d'apparence anodine et utilisées dans la vie courante. Presque tous les programmes de fidélité (M-Cumulus, Supercard, MyOne, Qualiflyer,…) débouchent sur une banque de données. Il en va de même des concours, abonnements en tous genres, annuaires, participations à une société ou association, etc. 138

Les banques de données ne sont pas toujours aussi fiables qu'on le croit. Toute inscription peut être erronée : un nom mal orthographié, un numéro mal donné ou mal saisi, etc. En plus des données incorrectes, le risque existe de saisir les données dans le dossier de la mauvaise personne. Les vérifications de la validité des informations contenues dans les bases de données de la police, et plus rarement des services de renseignement, révèlent une proportion très élevé d'erreurs, de l'ordre de 40 % selon des audits effectués aux Etats-Unis et au Canada. Des études faites auprès de certains organismes de crédit américains affichent des taux d'erreurs de 19 %, 43 %, voire 48 %[199]. En France, la CNIL a contrôlé le « système de traitement des infractions constatées » (STIC)[200]. Parmi les investigations effectuées dans le cadre du droit d'accès indirect à la demande de particuliers entre janvier et octobre 2008, la CNIL a constaté que seules 17 % des fiches de personnes mises en cause étaient exactes (66 % ont fait l'objet d'une correction et 17 % ont été purement et simplement supprimées). 30 % des procédures enregistrées dans le STIC étaient exactes, alors que 51 % ont dû être corrigées et 19 % supprimées[201]. 139r

198 RUDIN, *Auf der Suche nach dem "Bodensatz"*, p. 276.

199 Sur la fiabilité des données et quelques exemples d'études américaines : ETZIONI, *Big Brother*, pp 49-51.

200 Le STIC est un fichier national français destiné à enregistrer les informations recueillies à partir des procédures établies par les services de la police nationale dans le cadre de leurs missions de police judiciaire et relatives aux crimes, aux délits et à certaines contraventions. Il est également utilisé comme instrument d'enquête administrative. Pour plus de détails, voir notamment : CNIL, *Conclusions du contrôle du STIC*, pp 4-5.

201 CNIL, *Conclusions du contrôle du STIC*, p. 26.

140 On peut aussi signaler les bases de données alimentées par les utilisateurs eux-mêmes sur Internet, tel que les blogs ou les réseaux sociaux (MySpace[202], FaceBook[203], LinkedIn[204], Xing[205])[206]. Ces sites peuvent être ouverts à tous les utilisateurs ou à un cercle limité de personnes. Ils regorgent cependant de données, pour la plupart personnelles, et sur lesquelles l'utilisateur perd peu à peu la maîtrise. Les conditions générales prévoient très souvent que l'ensemble des données introduites deviennent la propriété du gestionnaire du site.

141 Les banques de données peuvent également être utilisées pour effectuer une surveillance en direct. C'est le cas notamment en matière de surveillance des relations bancaires. On peut alors être informé, par exemple, de chaque transaction financière effectuée en temps réel, mais également du lieu d'utilisation d'une carte de crédit, du montant débité et de l'objet de la contre-prestation, etc. Le même principe s'applique à l'utilisation de n'importe quelle carte liée à une base de données mise à jour en temps réel (carte fidélité, de paiement, d'entrée, etc.)[207]. Et finalement, il y a les bases de données créées par les autorités, policières notamment[208]. L'ensemble de ces données peut ensuite être trié, recoupé, analysé, etc.[209].

[202] http://www.myspace.com.

[203] http://www.facebook.com.

[204] http://www.linkedin.com.

[205] http://www.xing.com.

[206] Sur le fonctionnement et les dangers potentiels des sites de réseautage social : PFPDT, *16ème rapport*, pp 115-122.

[207] La dématérialisation croissante de moyens d'identification implique qu'une telle surveillance n'est plus limitée aux porteurs de cartes. Elle s'applique également aux puces RFID voire à de simples caractéristiques biométriques préalablement enregistrées.

[208] Sur la situation actuelle et future des banques de données policières en Suisse : BRÖNNIMANN, *Datenbanken*; *Message du CF relatif aux systèmes d'information de police*.

[209] Pour des exemples d'analyses : RIBAUX, *Les outils informatisés du renseignement criminel*.

B. Les possibilités de regroupement des différentes techniques

1. En fonction de la technique utilisée

a) Les catégories juridiques habituelles

Toutes les techniques de surveillance décrites précédemment ont de nombreux points communs, ce qui évite au législateur de les appréhender séparément. Certains regroupements sont nécessaires également pour pouvoir inclure les nouvelles techniques qui apparaîtront. Traditionnellement, le législateur distingue trois catégories : la surveillance de la correspondance postale, la surveillance des télécommunications et l'utilisation d'(autres) appareils techniques de surveillance[210]. C'est dans cette dernière catégorie qu'entrent généralement les techniques qui ne sont pas à proprement parler de surveillance, mais qui aboutissent à un résultat pouvant être utilisé dans le cadre d'une surveillance, ainsi que celles que le législateur ne connaissait pas au moment de l'adoption de la loi. Jusqu'à l'introduction du Code de procédure pénale unifié, la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication[211] règle les deux premières catégories, la troisième revenant au droit cantonal (généralement les codes de procédure pénale cantonaux). 142

Ni la LSCPT, ni le CPP ne contiennent de définition de la notion de correspondance. Selon le message accompagnant le projet de LSCPT, la notion de correspondance postale et de télécommunications comprend toutes les prestations et toutes les transmissions au moyen de techniques de télécommunication qui tombent dans le champ d'application de la Loi du 30 avril 1997 sur la poste (LPO) et de la Loi du 30 avril 1997 sur les télécommunications (LTC)[212]. La surveillance de la correspondance postale a 143

[210] Notamment HAUSER / SCHWERI / HARTMANN, *Schweizerisches Strafprozessrecht*, pp 357-358 et 367; PIQUEREZ, *Traité*, pp 615-618 et 628; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 95-117; VON BENTIVEGNI, *Les mesures officielles de surveillance*, pp 33-34.

[211] LSCPT, RS 780.1

[212] *Message du CF concernant la LSCPT*, pp 3703-3704.

été présentée ci-dessus et n'appelle pas de commentaires particuliers[213]. Pour la surveillance des télécommunications, nous retiendrons qu'elle concerne toutes les informations émises ou reçues, sur des lignes ou par ondes hertziennes, au moyen de signaux électriques, magnétiques ou optiques ou d'autres signaux électromagnétiques[214]. Cela regroupe les écoutes téléphoniques, mais aussi la surveillance du courrier électronique et l'interception de données électroniques, ainsi que partiellement l'interception des données électroniques sur l'ordinateur ou le serveur et l'interception de champs électromagnétiques et d'ondes hertziennes. Ces dernières peuvent également, selon les cas, appartenir à la troisième catégorie : les autres appareils techniques de surveillance. On y trouve tout ce qui n'est pas dans les deux premières catégories, notamment la vidéosurveillance, la prise de photographies, les enregistrements à l'aide de micros, la surveillance au moyen d'identifiants biométriques, la localisation, l'utilisation de bases de données, etc.

b) La surveillance simple ou informatisée

144 Cette distinction est surtout utilisée dans le cas de la vidéosurveillance, mais rien n'empêche de l'utiliser de manière plus globale. On parle de surveillance simple lorsqu'il n'y a pas d'enregistrement ou de traitement automatisé des données. La situation est un peu la même que si l'observation se faisait directement sur place, si ce n'est que la même personne peut procéder simultanément à plusieurs observations différentes.

145 Par opposition, la surveillance dite informatisée permet l'enregistrement, la conservation et le traitement des données[215]. Ces opérations peuvent être effectuées de manière automatique, sans nécessiter une intervention humaine.

2. En fonction de la période visée par la surveillance

146 Un autre critère, qui peut être utilisé en plus des distinctions précédentes, consiste à différencier la surveillance en temps réel de la surveillance rétroactive[216].

[213] Voir à ce sujet le chapitre 1. La surveillance du courrier postal, p. 36 ci-dessus.
[214] Art. 3 lit. c de la Loi sur les télécommunications (LTC, RS 784.10).
[215] FLÜCKIGER / AUER, *La vidéosurveillance dans l'œil de la constitution*, p. 925.

La surveillance en temps réel est la forme classique, prospective, de la surveillance comme on la conçoit intuitivement. Elle consiste dans l'observation de ce qui se produit actuellement, ou du résultat actuellement visible. 147

La surveillance rétroactive porte sur des données recueillies précédemment, mais qui ont été conservées et qui sont encore disponibles. Il s'agit le plus souvent d'enregistrements audio ou vidéo, de données commerciales, etc. 148

3. En fonction de l'objet de la surveillance

a) Les mesures personnelles et les mesures réelles

On peut ensuite distinguer les mesures de surveillance personnelles, soit celles qui visent un individu déterminé, des mesures de surveillance réelles, qui portent sur un lieu, un objet ou encore une adresse[217]. 149

Parmi les mesures personnelles, on trouve toutes celles liées aux données biométriques. Les principales mesures de surveillance réelles sont la surveillance du courrier postal ou électronique (on surveille une adresse), les écoutes téléphoniques (on surveille un numéro ou un appareil), l'interception de données électroniques (on surveille un appareil, une adresse IP ou un compte d'accès). 150

La vidéosurveillance peut être une mesure personnelle ou réelle, selon qu'une personne déterminée est suivie par une ou plusieurs caméras (pour avoir la preuve d'un comportement déterminé par exemple), ou que celles-ci sont dirigées sur un lieu ou un objet (ce qui est généralement le cas). Pour les mêmes raisons, la géolocalisation pourrait théoriquement être une mesure personnelle, mais elle sera dans la quasi-totalité des cas réelle. 151

[216] Pour une définition analogue : PIQUEREZ, *Traité*, pp 615 et 617-618; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 96-99 et 104-107.

[217] La littérature mentionne surtout le caractère réel de la surveillance de la correspondance : PIQUEREZ, *Traité*, pp 615-617; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 96, 103-104 et 116.

b) Le cas particulier de la surveillance de type « Echelon »

152 Le réseau de surveillance Echelon est un système d'écoute qui a la capacité d'exercer une surveillance pour ainsi dire totale à l'échelle planétaire et qui est (notamment) un instrument d'espionnage économique[218]. Il pourrait être assimilé à une mesure de surveillance invasive[219] puisqu'il s'agit d'une mesure de surveillance secrète. La comparaison s'arrête cependant là. Il ne s'agit pas de la surveillance d'une personne ou d'un lieu précis, mais d'une surveillance générale et systématique. La surveillance en tant que telle n'est ainsi plus secrète, seules son étendue et son utilisation le sont.

153 Cette surveillance n'est pas ordonnée dans le cadre d'une procédure judiciaire, mais elle est opérée par les services de renseignement. La plupart du temps, elle ne vise pas les habitants de l'Etat qui l'a mise en place, mais les Etats étrangers et leurs résidents. De fait, ceux-ci sont ainsi privés de toute protection dans leur système juridique interne. Finalement, ce type de surveillance n'est en principe jamais admis par les Etats qui la pratiquent[220], contrairement à la surveillance invasive qui obéit à des exigences légales relativement précises.

c) L'exploitation des résultats d'autres surveillances

154 Si on peut mettre en place une mesure de surveillance particulière à la suite d'un événement précis, il est tout aussi possible d'utiliser une structure existante pour en faire une mesure de surveillance, soit en s'intéressant à des données déjà recueillies dans un autre but, soit en détournant une infrastructure de son usage initial. L'exemple le plus connu est l'analyse de base de données, par exemple celle de l'émetteur d'une carte de crédit, ce qui permet de recenser les dépenses et les déplacements de la personne recherchée. Mais cela peut aussi prendre la forme de l'utilisation d'une caméra de surveillance déjà installée à l'entrée d'un

[218] Pour une description du réseau Echelon et de ses implications : SCHMID, *Rapport Echelon*, pp 11-12. La Suisse dispose d'un système similaire. Le système Onyx se limite toutefois aux questions liées à la sécurité intérieure et extérieure : BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 525-527.

[219] La surveillance est dite invasive lorsqu'elle tend à surveiller secrètement une personne. Voir à ce sujet le chapitre 3. La surveillance invasive, p. 84 ci-dessous.

[220] Pourtant tous les Etats y ont recours. Seuls l'étendue et l'objet de la surveillance (militaire, politique, économique, etc.) varient. Pour quelques exemples historiques de l'activité des services de renseignements étrangers en Suisse : WEISSEN, *Les services de renseignement suisses*, pp 6-9.

immeuble. Celle-ci ne sera plus seulement utilisée pour des mesures de sécurité ou pour rassurer les habitants, mais son usage sera détourné pour contrôler les entrées et sorties de l'immeuble d'un individu en particulier.

4. En fonction de la procédure

a) La surveillance préventive

La surveillance préventive est généralement opérée en dehors de toute procédure judiciaire[221]. C'est notamment celle qui est effectuée par les services de renseignement civils et militaires[222]. Le Service d'analyse et de prévention (SAP) du Département fédéral de la défense, de la protection de la population et des sports (DDPS) est notamment chargé de détecter précocement les dangers liés au terrorisme, au service de renseignement prohibé, à l'extrémisme violent, au commerce illicite d'armes et de substances radioactives et au transfert illégal de technologie[223]. Il collabore avec les autorités cantonales, le Renseignement militaire (RM), le Renseignement des forces aériennes (RFA), les autres organes de renseignement de l'armée, la sécurité miliaire, ainsi qu'avec ses homologues étrangers[224]. Ces activités de surveillance sont réglées par la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI)[225]. Quant au service de renseignement extérieur, il est assumé par le Service de renseignement stratégique (SRS) du Département fédéral de la défense, de la protection de la population et des sports. Depuis le 1er janvier 2010, un nouvel

155

[221] On distingue d'ailleurs généralement le renseignement criminel (judiciaire) du renseignement de sécurité (politique) : LEMAN-LANGLOIS / LEMIEUX, *Renseignement de sécurité et renseignement criminel*, p. 336. Sur l'analyse criminelle : RIBAUX / GITZ / CARTIER, *L'analyse criminelle face à la complexité des données.*

[222] Sur la délimitation des tâches entre le service de renseignement intérieur et les autorités de poursuite pénale : *Rapport du CF relatif à la lutte contre le terrorisme*, pp 5437-5438. Sur l'organisation des services de renseignement suisses et leurs attributions respectives : FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 6-12; WEISSEN, *Les services de renseignement suisses*, pp 24-47. Sur le service de renseignement stratégique en particulier : SRS, *Le service de renseignement stratégique de la Suisse*. Sur la notion de renseignement et les différents buts poursuivis par le renseignement : BRODEUR, *Le renseignement*; CUSSON, *De l'action de sécurité*, p. 48; LEMIEUX, *Vers un renseignement criminel de qualité*, pp 292-295.

[223] Jusqu'à fin 2008, le SAP était rattaché à l'Office fédéral de la police.

[224] *Message du CF relatif à la LMSI II*, pp 4781-4790.

[225] RS 120. Le Code de procédure pénale ne s'applique qu'aux activités de la police en matière de poursuite pénale. Les activités qui relèvent de la sûreté n'y sont pas soumises : *Message du CF relatif à l'unification de la procédure pénale*, p. 1112.

office fédéral appelé Service de renseignement de la Confédération (SRC) regroupe les deux services civils de renseignement de la Suisse, soit le Service d'analyse et de prévention (SAP) et le Service de renseignement stratégique (SRS)[226].

156 On trouve ensuite la surveillance politique et économique, qui peut aussi être effectuée par ou pour un Etat étranger. De tout temps et dans tous les pays, les services de renseignement ont évolué dans une zone relativement grise. Si aujourd'hui les Etats ne nient plus tellement se consacrer à des activités de surveillance et de renseignement, y compris à l'étranger, l'étendue de ces activités et leur contrôle restent méconnus.

157 La surveillance préventive est mise en place lorsqu'il existe un soupçon de menace significative pour la sécurité, alors que la poursuite pénale est engagée lorsqu'il y a une infraction concrète. La sécurité intérieure de la Suisse pouvant être menacée tant par des actes non punissables pénalement que par des actes répréhensibles, les investigations préventives peuvent découler indifféremment de ces deux catégories d'actes[227].

158 Le risque d'atteintes à la sphère privée ou une autre liberté individuelle est au moins aussi important que si la surveillance intervient dans le cadre d'une procédure judiciaire[228]. Le Tribunal fédéral considère d'ailleurs que : « Missbräuche können im präventiven Bereich noch weit mehr als bei der repressiven Überwachung schädliche Folgen für die freiheitliche, demokratische Ordnung haben »[229]. Dans le cas où la surveillance est opérée en l'absence d'un cadre juridique strict et de moyens de contrôle permettant de limiter et sanctionner les éventuels abus, le risque doit être considéré comme supérieur.

[226] SRC, *Rapport annuel 2009*, pp 94-97.

[227] *Message du CF relatif à la LMSI II*, pp 4797-4798.

[228] Il l'est même plus si l'on considère qu'il n'est pas justifié par la commission préalable d'une infraction.

[229] ATF 109 Ia 273, 295, Hans VEST und Demokratische Juristen der Schweiz, du 9 novembre 1983.

b) La surveillance répressive

Les mesures de surveillance répressive interviennent dans le cadre de la procédure pénale, plus précisément au stade de la procédure préliminaire. Une fois que le ministère public a prononcé la clôture de l'instruction, il n'y a en effet plus de place ni de raison de procéder à des mesures de surveillance. La procédure préliminaire est introduite par les investigations de la police ou par l'ouverture d'une instruction par le ministère public (art. 300 CPP). Dès que la police entreprend de telles investigations, la procédure est régie par les dispositions du CPP. Les droits et devoirs des participants à la procédure doivent alors être respectés[230]. 159

Ces investigations policières peuvent être parfois proches de la surveillance opérée par les services de renseignement. La police procède d'ailleurs à des actes d'enquêtes sur délégation du Service d'analyse et de prévention. Il ne s'agit alors pas d'une investigation policière au sens où l'entend le CPP. Lorsque la police agit en tant qu'autorité de renseignement ou se livre à une activité de surveillance préventive, le cadre juridique est le même que celui dans lequel évoluent les services de renseignement. Lorsque l'autorité policière intervient dans le cadre d'une procédure préliminaire, son action est régie par le CPP. 160

Le Tribunal fédéral avait admis que soit prononcée une mesure de surveillance dans le cadre de l'instruction préliminaire. Elle doit cependant reposer sur une base légale et la nature et la gravité des infractions envisagées doivent justifier l'atteinte à la liberté personnelle[231]. Cette question ne se pose plus sous l'empire du CPP, le Conseil national ayant supprimé l'institution des investigations préalables que connaissaient certains cantons[232]. 161

[230] *Message du CF relatif à l'unification de la procédure pénale*, p. 1241.
[231] ATF 112 Ia 18, X., 20-21, du 8 avril 1986.
[232] *Message du CF relatif à l'unification de la procédure pénale*, pp 1247-1248.

c) La surveillance privée

162 Bien qu'elle ne fasse pas partie de l'objet de la présente étude, la surveillance privée mérite d'être brièvement mentionnée ici[233]. Elle n'est pas régie en tant que telle par la procédure pénale[234]. Pour l'essentiel, ce sont les normes de droit civil et de droit pénal qui s'appliqueront, notamment les art. 28ss CC (protection de la personnalité), 186 CP (violation de domicile), 179ss CP (infractions contre le domaine secret ou le domaine privé), 321ter CP (violation du secret des postes et des télécommunications) ou encore la Loi sur la protection des données[235]. D'autres normes juridiques peuvent encore trouver application en fonction de la situation, par exemple celles liées au droit du travail[236], au droit des assurances[237], etc.

5. En fonction de la connaissance de la mesure

163 Une mesure technique de surveillance n'est pas obligatoirement inconnue de la personne surveillée[238]. On peut donc distinguer les mesures techniques de surveillance connues de la personne surveillée de celles qui sont secrètes. C'est cette distinction que semble suivre le Code de procédure pénale[239].

---

[233] Sur la légalité de la surveillance privée et l'éventuelle utilisation de ses résultats dans une procédure pénale : MÉTILLE, *L'utilisation privée de moyens techniques de surveillance*.

[234] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 96. Sur la distinction entre la surveillance opérée par un privé et par une autorité : GAUTHIER, *Enregistrement clandestin*.

[235] Sur la protection offerte par le droit pénal : LEGLER, *Vie privée, image volée*.

[236] Pour une présentation des normes applicables : ORDOLLI, *Les systèmes de surveillance des travailleurs*.

[237] Sur la différence entre la surveillance d'un assuré effectuée dans le cadre de la LCA et soumise au respect de l'art. 28 CC et celle effectuée par la CNA, institution publique agissant dans le cadre de la LAA et soumise au respect des art. 13 et 36 Cst. : ATF 129 V 323, 324-326, F., du 25 février 2003. Une compagnie d'assurance privée agissant au titre de l'assurance accident obligatoire prévue par la LAA est également soumise au respect des art. 13 et 36 Cst. Une mesure de surveillance est admissible si elle est proportionnée et se limite au domaine public : ATF 135 I 169, S., du 15 juin 2009. Voir également AEBI-MÜLLER / EICKER / VERDE, *Verfolgung von Versicherungsmissbrauch mittels Observation*; MEIER / STAEGER, *La surveillance des assurés*.

[238] Voir à ce sujet le chapitre 1. Surveillance technique et exploitation de données, p. 25 ci-dessus.

[239] Le chapitre 8 du titre 5 regroupe les mesures de surveillance dites secrètes : surveillance de la correspondance par poste et télécommunication, autres dispositifs techniques de surveillance, observation, surveillance des relations bancaires et investigation secrète.

Il est toutefois difficile de décider de manière absolue du caractère secret d'une mesure, puisque cela dépend essentiellement du cas d'application. Une mesure de surveillance de la correspondance est en principe secrète, mais elle peut être découverte en cours d'exécution. Un détenu saura par ailleurs *ab initio* que sa correspondance sera surveillée. L'atteinte causée à la personne surveillée est renforcée par le caractère secret de la surveillance, la personne visée ne pouvant se protéger et défendre seule ses droits[240]. 164

C. Les cas d'utilisation de la surveillance

1. La surveillance d'observation

En matière de vidéosurveillance, la littérature distingue généralement la vidéosurveillance d'observation, la vidéosurveillance dissuasive et la vidéosurveillance invasive[241]. Ces distinctions sont également applicables pour les autres moyens de surveillance. 165

On parle de surveillance d'observation lorsqu'elle est utilisée pour surveiller un rayon déterminé accessible au public, afin de constater des mouvements ou des phénomènes objectifs, sans traiter des données personnelles. Ce genre de surveillance n'est pas lié à une activité de police judiciaire, mais elle revêt plutôt un caractère organisationnel ou de gestion de l'espace. La connaissance de l'existence de la surveillance par les personnes observées ne joue aucun rôle. La surveillance n'est pas dirigée sur une personne, mais sur des objets comme une rue ou un bâtiment. L'exemple classique est le contrôle de la fluidité du trafic routier. 166

Les recherches, l'analyse ADN, la saisie de données signalétiques, ainsi que la récolte d'échantillons d'écriture ou de voix figurent dans d'autres chapitres.

[240] WEICHERT, *Überwachung: Einblick in die Praxis*, p. 5.

[241] Notamment BAERISWYL, *Videoüberwachung - im rechtsfreien Raum?*, pp 26-27; DFJP, *Rapport sur la vidéosurveillance*, p. 9; FLÜCKIGER / AUER, *La vidéosurveillance dans l'œil de la constitution*, pp 924-925.

2. La surveillance dissuasive

167 La surveillance dissuasive consiste à surveiller ouvertement un lieu pour tenter d'empêcher les personnes qui s'y trouvent de commettre des infractions. Il s'agit d'une surveillance préventive, utilisée par exemple dans les aéroports ou sur les places publiques. Lorsque la surveillance est mise en place par les pouvoirs publics, elle fait partie de l'activité de la police préventive[242]. La surveillance dissuasive n'a d'effets que si elle est connue et visible, puisque c'est sa présence qui doit dissuader de la commission de l'infraction. C'est pour cette raison qu'il existe parfois des leurres, comme de fausses caméras. L'individu se croyant surveillé, il adaptera son comportement et le but de la surveillance sera atteint.

168 Bien qu'il arrive souvent qu'une surveillance dissuasive soit mise en place à la suite de la commission d'une infraction, elle n'y est pas directement liée. La surveillance dissuasive n'a pas pour objectif de trouver l'auteur de l'infraction commise, mais seulement d'éviter la commission ultérieure d'infractions similaires.

3. La surveillance invasive

169 La surveillance invasive vise à surveiller secrètement une personne. Elle est utilisée notamment lorsqu'une personne a commis une infraction ou qu'elle est soupçonnée d'en commettre une prochainement. La surveillance invasive apporte en principe de meilleurs résultats si elle n'est pas connue de la personne surveillée.

170 Lorsque la surveillance porte sur l'auteur d'une probable infraction future, elle est souvent du domaine de l'activité de la police préventive, voire politique. Dans ces cas-là, la procédure n'appartient plus à l'instruction pénale, mais revient aux services de renseignement.

171 Lorsque la surveillance fait suite à la commission d'une infraction, elle intervient dans le cadre de l'instruction pénale. Elle peut porter sur la surveillance de l'auteur présumé dans le but d'obtenir des preuves de sa

[242] Pour une distinction entre la police préventive, proactive et réactive : KUHN, *Sommes-nous tous des criminels*, pp 25-26. Sur la police en général et ses missions: GISLER, *La coopération policière*, pp 51-68; PIETH, *Schweizerisches Strafprozessrecht*, pp 56-61; RAUBER, *Sicherheitspolizeiliche Aufgaben durch Private*, pp 41-91.

culpabilité, mais également consister à rechercher une personne ou une chose dans des bases de données, afin de vérifier s'il y a un lien avec l'infraction commise. Dans le premier cas, le point de départ est la personne suspectée. Dans le second, il s'agit du délit, puisqu'il n'y a pas encore de suspect.

4. La surveillance sauvage

On retrouve dans cette catégorie toutes les mesures de surveillance non réglementées ou interdites, effectuées par des privés, par des services de renseignement étrangers, ou alors de manière occulte par les autorités policières ou de renseignement internes. 172

IV. Synthèse et critique

A. Des méthodes facilement accessibles

173 L'état actuel de la technique permet de procéder à une surveillance importante et ciblée en recourant à des méthodes très diverses. Des connaissances techniques très pointues ne sont plus obligatoires et le coût de mise en place de ces mesures de surveillance est variable, mais il n'est la plupart du temps plus un obstacle.

174 Du strict point de vue technique, les mesures de surveillance sont parfaitement utilisables par une personne privée, une organisation ou un Etat. Le plus grand obstacle technique n'est pas tant la récolte de l'information, mais plutôt son exploitation : tri, traitement, analyse, etc. Dévier ou « écouter » le flux d'informations circulant à travers un câble ou une fibre optique, surveiller une adresse IP, récolter des traces d'ADN ou encore « attraper » les identifiants de tous les utilisateurs de téléphonie mobile dans un certain rayon sont des opérations facilement réalisables. Il est en revanche beaucoup plus difficile de trouver le bon appel, le bon numéro, le bon courriel, parmi des milliers voire des milliards d'autres.

175 Toutes les possibilités techniques de surveillance ne sont pas autorisées par la législation suisse. Il n'empêche que ces techniques sont disponibles et qu'un Etat étranger, une organisation criminelle ou éventuellement un simple citoyen peuvent en faire usage. Indépendamment de l'arsenal juridique, qui interviendra le plus souvent une fois l'atteinte commise et dans le seul cas où la surveillance a été connue, plusieurs éléments protègent l'individu.

B. Des moyens de se protéger

176 La première limitation aux mesures de surveillance ne dépend ni de la personne surveillée ni du surveillant. Elle repose uniquement sur la masse de données simultanément disponibles et le fait que les données n'ont pas toutes le même format. L'exemple le plus simple est celui de la carte postale envoyée depuis le lieu de ses vacances. Si cette carte postale est techniquement lisible par toute personne qui l'a en main ou à portée de mains, il faut admettre que peu nombreux sont ceux qui la liront. Certains n'auront pas le temps, d'autres ne

comprendront pas la langue, et la plupart ne la remarqueront même pas, cette carte étant finalement cachée au milieu des autres.

Deuxièmement, des mesures de protection le plus souvent élémentaires peuvent être prises par la personne surveillée. On y trouve les mots de passe et les mesures de cryptage, le fait de refermer les portes derrière soi (virtuellement pour des accès numériques et physiquement pour éviter l'accès indu à des locaux) mais également l'utilisation d'infrastructures maintenues à jour et correctement installées ou encore la discrétion voulant que l'on ne donne pas à tout va des informations personnelles. Pour reprendre l'exemple précédent, la carte postale envoyée dans une simple enveloppe ne la rend certes pas indécelable, mais sa lecture en est nettement moins aisée. 177

Le troisième élément est lié au surveillant ou surveillant potentiel. Toute personne qui peut exercer une surveillance ou avoir accès au résultat de mesures de surveillance n'y recourra pas. Tous les employés d'opérateurs téléphoniques, les policiers ou autres fonctionnaires, les informaticiens, etc. ne sont pas systématiquement malhonnêtes. Un risque d'abus de cette position particulière, permettant un accès facilité, existe, mais ces personnes sont également soumises à des directives internes, devoirs de fonction ou autres codes de l'honneur. La grande majorité d'entre elles n'aura d'ailleurs aucun intérêt à profiter de ces informations. 178

C. Une efficacité certaine

Les mesures de surveillance employées à bon escient peuvent apporter d'excellents résultats dans le cadre d'une enquête pénale. Il est toutefois impératif que la surveillance soit suffisamment ciblée pour que les éléments recueillis ne soient pas trop importants et qu'ils puissent être ensuite traités correctement. Pour ce faire, il est nécessaire que celui qui ordonne la mesure de surveillance maîtrise les éléments techniques et choisisse la bonne mesure. Si une personne change par exemple fréquemment de numéro de téléphone mais conserve le même appareil, la surveillance de l'appareil (IMEI) sera efficace. En choisissant de surveiller les numéros, le risque est pris de manquer tous les appels utilisant des numéros qui ne seraient pas connus, mais aussi de surveiller un grand nombre de conversations inutiles effectuées par d'autres personnes qui utiliseraient ultérieurement les numéros surveillés. 179

180 Une collaboration efficace entre celui qui décide de la surveillance et celui qui l'exécute, comme une maîtrise des éléments techniques, sont simplement essentielles.

Deuxième partie :
le cadre juridique

I. Remarques préliminaires

Le cadre technique étant circonscrit, il convient d'examiner quelles sont les normes juridiques qui régissent les possibilités de surveillance. Aux normes protégeant l'individu s'opposent celles qui autorisent la surveillance. Le premier niveau est constitué par les droits fondamentaux. Ces garanties individuelles sont contenues dans plusieurs textes de droit, parmi lesquels la Constitution fédérale et la Convention européenne des droits de l'Homme. Ces normes posent en quelque sorte les limites aux atteintes admissibles et jouent ainsi un rôle protecteur. C'est de ces garanties, et des conditions permettant d'y déroger, que la jurisprudence a déduit les exigences minimales à respecter pour pouvoir utiliser des mesures de surveillance. 181

Les lois mentionnant des possibilités de surveillance sont nombreuses et concernent des domaines variés. Elles contiennent les règles exigées par les garanties mentionnées auparavant, de manière plus ou moins complète. Les lois les plus importantes seront présentées, après avoir examiné la question de la répartition des compétences entre la Confédération et les cantons. 182

II. Les libertés touchées par la surveillance

A. Les droits fondamentaux et les libertés

183 Les droits fondamentaux[243] sont des droits reconnus aux particuliers et qui sont à la base de la détermination de leurs rapports avec la société et l'Etat. Ces droits répondent essentiellement au besoin de liberté et d'égalité des personnes. Ils regroupent les libertés, les garanties de l'Etat de droit, les droits sociaux et les droits politiques[244].

184 Les droits fondamentaux sont généralement définis comme toutes les prétentions subjectives qui visent à obtenir de l'Etat un comportement déterminé, qu'une personne peut faire valoir devant un juge et qui apparaissent soit comme un élément constitutif de la démocratie ou de l'Etat régi par le droit, soit comme une exigence essentielle de l'existence humaine. Ces droits ont pour caractéristique commune d'être dirigés contre l'Etat, alors que l'Etat en est également le garant[245].

185 Les droits fondamentaux se trouvent essentiellement dans les Constitutions fédérale et cantonales, la Convention européenne des droits de l'Homme, les Pactes de l'ONU et quelques autres traités internationaux. Ils peuvent également être consacrés par la jurisprudence : on parle alors de droits constitutionnels non écrits. La révision récente de la Constitution fédérale a fortement réduit la place de ces derniers[246].

---

[243] On parle également de droits de l'Homme, de droits humains ou encore de droits de la personne.

[244] Sur la typologie des droits fondamentaux : HALLER, *The Swiss Constitution*, pp 145-147; KIENER / KÄLIN, *Grundrechte*, pp 25-28.

[245] Pour des définitions analogues : AUBERT / MAHON, *Petit commentaire*, pp 59-63; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 5-16; RHINOW, *Grundzüge*, pp 165-173. Sur la théorie générale des droits fondamentaux : AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*; RHINOW, *Grundzüge*.

[246] Sur les sources en général : AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 33-51; KIENER / KÄLIN, *Grundrechte*, pp 10-21. Sur la question particulière des droits non écrits : AUBERT / MAHON, *Petit commentaire*, pp 63-64; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 35-36.

Nous nous intéresserons d'abord aux principales sources de droits fondamentaux, pour ensuite étudier le contenu et la portée de ces droits. Plusieurs sources consacrent les mêmes droits, et ce qui apparaît parfois comme une seule garantie peut en recouvrir plusieurs. Les droits fondamentaux n'étant pas absolus, nous terminerons ensuite cette partie avec l'examen des conditions auxquelles les libertés peuvent être restreintes et les exigences que posent ces garanties dans le cadre de la surveillance technique. Nous nous concentrerons ici sur les libertés, mais il va de soi que les principes de l'activité de l'Etat régi par le droit (notamment les principes de légalité, proportionnalité, etc.) et les garanties de procédure ont également leur importance[247]. 186

B. Les sources

1. La Constitution fédérale

a) En général

La Constitution fédérale du 18 avril 1999 est entrée en vigueur le 1er janvier 2000[248]. Elle contient un catalogue détaillé des droits fondamentaux (art. 7 à 36). 187

b) La dignité humaine (art. 7)

L'art. 7 Cst. rappelle, dans une formulation laconique, que la dignité humaine doit être respectée et protégée. Cette garantie ne figurait pas explicitement dans la Constitution de 1874. Elle a un caractère subsidiaire et nombre de ses aspects sont concrétisés par d'autres droits fondamentaux. 188

[247] Notamment le droit de ne pas s'auto-incriminer, le droit à un procès équitable et le droit à l'égalité des armes garantis par les art. 29 à 32 Cst. et par l'art. 6 CEDH. Ces principes ne s'opposent pas à l'utilisation de moyens techniques de surveillance durant la procédure préliminaire : GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 47-78 et les réf. cit.

[248] RS 101. Sur les droits touchés par les mesures de surveillance sous l'empire de la Constitution fédérale de 1874 : VON BENTIVEGNI, *Les mesures officielles de surveillance*, pp 6-8.

c) La liberté personnelle (art. 10 al. 2)

189 L'art. 10 al. 2 Cst. dispose que « tout être humain a droit à la liberté personnelle, notamment à l'intégrité physique et psychique et à la liberté de mouvement ». La liberté personnelle était un droit fondamental non écrit sous l'empire de la Constitution de 1874, reconnu par le Tribunal fédéral en 1963 déjà[249]. En tant que garantie générale et subsidiaire, elle protégeait toutes les libertés élémentaires dont l'exercice est indispensable à l'épanouissement de la personne humaine. La liberté personnelle est un droit inaliénable et imprescriptible, tout comme le droit à la vie et l'interdiction de la torture et des peines ou traitements cruels, inhumains ou dégradants[250].

190 L'art. 10 al. 2 Cst. garantit de manière générale la liberté personnelle, et trois aspects en particulier : l'intégrité physique, l'intégrité psychique et la liberté de mouvement.

d) La protection de la sphère privée (art. 13)

191 L'art. 13 Cst. prévoit que « toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et les télécommunications » (al. 1) et que « toute personne a le droit d'être protégée contre l'emploi abusif des données qui la concernent » (al. 2).

192 La protection de la sphère privée a été introduite par le constituant dans la Constitution de 1999. Précédemment, c'était un aspect du droit fondamental non écrit de la liberté personnelle.

e) La liberté de réunion (art. 22)

193 L'art. 22 Cst. garantit la liberté de réunion (al. 1), soit que « toute personne a le droit d'organiser des réunions, d'y prendre part ou non » (al. 2).

[249] ATF 89 I 92, 98, Kind X, du 20 mars 1963.

[250] Pour les diverses formulations et une évolution du contenu de cette garantie : AUBERT / MAHON, *Petit commentaire*, pp 101-103. Le caractère inaliénable et imprescriptible de la liberté personnelle ne signifie pas que des restrictions seraient inadmissibles. Voir à ce sujet le chapitre D. La théorie générale des restrictions des libertés, p. 113 ci-dessous.

La liberté de réunion ne faisait l'objet d'aucune mention dans la Constitution de 1874. Le Tribunal fédéral l'a reconnue en tant que droit constitutionnel non écrit en 1970[251]. 194

f) Les autres libertés

Un certain nombre d'autres libertés garanties par la Constitution fédérale peuvent être touchées par les mesures de surveillance. Il s'agit essentiellement du droit au mariage et à la famille (art. 14 Cst.), de la liberté de conscience et de croyance (art. 15 Cst.), de la liberté d'opinion et d'information (art 16 Cst.), ainsi que la liberté d'association (art. 23 Cst.). 195

2. La CEDH

a) En général

La Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (CEDH) a été conclue à Rome le 4 novembre 1950 sous l'égide du Conseil de l'Europe. Elle est entrée en vigueur pour la Suisse le 28 novembre 1974[252]. 196

b) Le droit au respect de la vie privée et familiale (art. 8)

L'art. 8 CEDH prévoit que « toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ». 197

Cette disposition de la Convention est probablement celle qui a connu le plus grand développement jurisprudentiel ces vingt dernières années. Elle recouvre la protection de la sphère privée au sens strict, mais également le droit d'entretenir des relations avec autrui, le droit à la liberté de la vie sexuelle, le droit à l'image, 198

[251] ATF 96 I 219, 224, *Nöthiger*, du 24 juin 1970.

[252] Convention européenne des droits de l'Homme, RS 0.101. Depuis la ratification jusqu'à fin 2006, 32 arrêts ont été rendus à propos de la Suisse, dont 21 condamnations : HOTTELIER, *Les droits de l'homme et la procédure pénale en Suisse*; HOTTELIER / MOCK / PUECHAVY, *La Suisse devant la CEDH*.

le droit au respect du domicile, la confidentialité des données à caractère personnel, le droit au respect de la correspondance[253].

c) Les autres libertés

199 D'autres libertés expressément garanties par la Convention européenne des droits de l'Homme peuvent être touchées par les mesures de surveillance. Il s'agit notamment de la liberté de pensée, de conscience et de religion (art. 9 CEDH), de la liberté d'expression (art. 10 CEDH), ainsi que de la liberté de réunion et d'association (art. 11 CEDH).

3. La Convention relative au traitement automatisé des données à caractère personnel

200 La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été conclue à Strasbourg le 28 janvier 1981 dans le cadre du Conseil de l'Europe. Elle est entrée en vigueur pour la Suisse le 1er février 1998[254].

201 L'art. 5 exige que les données soient obtenues et traitées loyalement et licitement et qu'elles soient utilisées conformément aux finalités pour lesquelles elles sont enregistrées. Le droit interne doit prévoir des garanties appropriées pour le traitement des données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé, à la vie sexuelle ou concernant des condamnations pénales (art. 6). L'art. 7 exige des mesures de sécurité contre la destruction, l'accès et la modification des données, alors que l'art. 8 dresse une liste des droits garantis à toute personne : droit de connaître l'existence d'un fichier, droit d'obtenir la confirmation de l'existence de données la concernant ainsi que la communication de ces données, droit

[253] Pour une casuistique des droits garantis par l'art. 8 : MOCK, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance.*
[254] RS 0.235.1.

d'obtenir la rectification ou l'effacement des données traitées illégalement, et finalement droit à un recours effectif pour faire respecter les droits précités[255].

4. Les autres sources

Le Pacte international relatif aux droits civils et politiques a été conclu à New York le 16 décembre 1966 dans le cadre de l'Organisation des Nations Unies (ONU)[256]. Il est entré en vigueur pour la Suisse le 18 septembre 1992. L'art. 17 prévoit que nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. Le Pacte II garantit également le droit à la liberté de pensée, de conscience et de religion (art. 18), la liberté d'opinion et d'expression (art. 19), ainsi que la liberté de réunion (art. 21) et d'association (art. 22). 202

On peut encore citer, même si elles n'apportent pas beaucoup de garanties supplémentaires dans la présente étude, la Convention internationale sur l'élimination de toutes les formes de discrimination raciale conclue à New York le 21 décembre 1965 et entrée en vigueur pour la Suisse le 29 décembre 1994[257], la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants conclue à New York le 10 décembre 1984 et entrée en vigueur pour la Suisse le 26 juin 1987[258], la Convention européenne pour la prévention de la torture et des peines ou traitements inhumains ou dégradants conclue à Strasbourg le 26 novembre 1987 et entrée en vigueur pour la Suisse le 1er février 1989[259], la Convention relative aux droits de l'enfant conclue à New York le 20 novembre 1989 et entrée en vigueur pour la Suisse le 26 mars 1997[260], ainsi que la Convention sur l'élimination de toutes les formes de 203

[255] Sur la proportionnalité en droit communautaire de la protection des données et l'influence de la Convention du 28 janvier 1981 : MORNET, *La vidéosurveillance et la preuve*, pp 145-150.
[256] Pacte ONU II ou Pacte II, RS 0.103.2.
[257] RS 0.104.
[258] RS 0.105.
[259] RS 0.106.
[260] RS 0.107.

discrimination à l'égard des femmes conclue à New York le 18 décembre 1979 et entrée en vigueur pour la Suisse le 26 avril 1997[261].

C. La sphère protégée

1. Le droit à la vie

204 Le droit à la vie est garanti par les art. 10 al. 1er Cst., 2 CEDH et 6 al. 1 Pacte ONU II, ainsi que par les Protocoles no 6 et 13 à la CEDH. C'est la plus élémentaire des libertés et la condition indispensable de l'exercice de tous les autres droits. La Constitution va plus loin que le texte de base de la CEDH, puisqu'elle interdit la peine de mort[262]. Aucune restriction ne peut être apportée au droit à la vie, puisqu'elle toucherait directement le noyau intangible du droit à la vie. En revanche, et c'est la seule exception, il existe de rares cas où l'autorité peut et doit prendre des mesures pour protéger et sauver la vie d'une personne menacée par un tiers, même si ces mesures peuvent entraîner la mort de ce dernier. Des conditions strictes, notamment d'absolue nécessité et de proportionnalité, doivent être respectées[263].

205 Le droit à la vie exige non seulement de l'Etat un comportement d'abstention, mais il lui impose aussi de prendre les mesures nécessaires à assurer la protection de la vie des personnes qui se trouvent sous sa juridiction. Par exemple, l'exécution d'une peine privative de liberté est susceptible de violer ce droit lorsqu'il est hautement vraisemblable qu'elle entraînerait la mort ou une maladie grave et durable du condamné[264].

---

[261] RS 0.108.

[262] Cette interdiction est reprise en temps de paix au Protocole no 6 et en tout temps au Protocole no 13.

[263] Pour des définitions analogues : AUBERT / MAHON, *Petit commentaire*, pp 100-107; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 131-142; BIAGGINI, *BV Kommentar*, pp 119-120; HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*, pp 105-116; KIENER / KÄLIN, *Grundrechte*, pp 117-124; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, pp 45-56; RHINOW, *Grundzüge*, pp 211-213; RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*, pp 251-253; SCHEFER, *Grundrechte, Ergänzungsband*, pp 13-18; SCHWEIZER, *Art. 10 BV*, pp 256-261. Sur la question de l'absence de restrictions admissibles, voir le chapitre 6. L'inviolabilité de l'essence des libertés, p. 116.

[264] Pour des exemples, voir AUBERT / MAHON, *Petit commentaire*, p. 105, note n° 33.

2. La dignité humaine

La dignité humaine ressort des art. 7 Cst., 3 CEDH et 7 Pacte ONU II[265]. Elle manifeste une valeur essentielle et inhérente à tout Etat régi par le droit. Elle fonde également l'ensemble des droits fondamentaux, tout en assurant une garantie subsidiaire en protégeant des atteintes à la dignité humaine qui ne tomberaient pas sous le coup d'une garantie spécifique[266]. 206

Le respect de la dignité humaine figure expressément à l'art. 3 du Code de procédure pénale. Il revêt une importance toute particulière dans le cadre de la procédure pénale, domaine dans lequel la collectivité peut recourir aux moyens de contrainte les plus incisifs aux fins d'assurer le respect des objectifs qu'elle poursuit. Le législateur en a déduit un certain nombre d'autres droits, tel que le droit d'être entendu ou l'interdiction de recueillir des preuves selon des méthodes qui sont attentatoires à la dignité humaine[267]. Un mauvais usage de la vidéosurveillance peut ainsi conduire à déshumaniser la personne filmée ou contribuer à l'asservir[268]. 207

Le Code de procédure pénale rappelle l'interdiction d'appliquer des méthodes d'enquête qui seraient incompatibles avec le respect de la dignité humaine (art. 3 al. 2 lit. d CPP). 208

3. La liberté personnelle

La liberté personnelle est un droit inaliénable et imprescriptible garanti par l'art. 10 Cst. Ses trois principales composantes sont l'intégrité physique et l'intégrité psychique, ainsi que la liberté de mouvement. Des garanties similaires figurent aux art. 2 à 5 et 8 CEDH, ainsi qu'aux art. 6 à 12 Pacte ONU II, ainsi 209

[265] La dignité humaine figure dans une vingtaine de traités internationaux, dont certains d'application régionale. Pour une énumération : MORNET, *La vidéosurveillance et la preuve*, p. 68, note n° 198.

[266] Pour des définitions analogues : AUBERT / MAHON, *Petit commentaire*, pp 164-178; BIAGGINI, *BV Kommentar*, pp 95-98; KIENER / KÄLIN, *Grundrechte*, pp 112-116; MASTRONARDI, *Art. 7 BV*, 77-90; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, pp 1-4; RHINOW, *Grundzüge*, 29-33. Pour une approche philosophique : MORNET, *La vidéosurveillance et la preuve*, pp 63-68.

[267] *Message du CF relatif à l'unification de la procédure pénale*, p. 1104. Sur les méthodes interdites, voir le chapitre a) Du point de vue technique, p. 30 ci-dessus.

[268] Pour des exemples : MORNET, *La vidéosurveillance et la preuve*, pp 66-68.

que dans la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants et la Convention européenne pour la prévention de la torture et des peines ou traitements inhumains ou dégradants[269]. L'art. 11 Cst dispose encore que les enfants et les jeunes ont droit à une protection particulière de leur intégrité.

210 La garantie de l'intégrité physique protège l'individu contre toute atteinte injustifiée portée au corps humain, qu'elle soit intentionnelle ou non, grave ou légère, et quels qu'en soient les motifs. Elle est complétée par l'interdiction de la torture et des peines ou traitements inhumains ou dégradants[270]. Aucune restriction ne peut être apportée à l'interdiction de la torture et des peines ou traitements cruels, inhumains ou dégradants[271].

211 La garantie de l'intégrité psychique protège la personne contre les atteintes qui tendraient, par un moyen quelconque, à restreindre ou à supprimer la faculté, qui lui est propre, d'apprécier une situation donnée et de se déterminer d'après cette appréciation.

212 La liberté de mouvement est le troisième aspect de la liberté personnelle. Elle protège le droit d'aller et venir, et représente aussi une protection minimale contre les arrestations et les détentions arbitraires.

---

[269] Pour des définitions analogues sur la liberté personnelle en général et ses trois composantes principales, ainsi qu'une importante casuistique : AUBERT / MAHON, *Petit commentaire*, pp 100-122; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 143-182; BAUM, *Der kriminalpräventive Einsatz von Videoüberwachungsanlagen*; BIAGGINI, *BV Kommentar*, pp 121-125; HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*, pp 105-116; KIENER / KÄLIN, *Grundrechte*, pp 125-145; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, pp 57-87; RHINOW, *Grundzüge*, pp 209-217; RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*, pp 253-256; SCHEFER, *Grundrechte, Ergänzungsband*, pp 10-31; SCHWEIZER, *Art. 10 BV*, pp 261-265.

Sur la notion de torture et de traitements inhumains, cruels et dégradants, avec des exemples : BICHOVSKY, *Guantanamo*, pp 24-31. Sur la notion de torture et de menaces de torture : Arrêt GÄFGEN c. Allemagne [GC], no. 22978/05, §§ 65-68, du 1er juin 2010.

[270] Sur l'interdiction de la torture en droit international et en droit allemand : MÖHLENBECK, *Das absolute Folterverbot*.

[271] Sur la question de l'absence de restrictions admissibles, voir le chapitre 6. L'inviolabilité de l'essence des libertés, p. 116.

Le Tribunal fédéral a développé une importante casuistique des mesures touchant l'intégrité physique : les prises de sang[272], les examens radiographiques[273], les vaccinations obligatoires[274], un frottis de la muqueuse jugale[275], l'obligation pour des élèves de subir un contrôle et éventuellement des soins dentaires obligatoires[276], une hospitalisation de quelques jours en vue d'une expertise[277], un traitement médicamenteux forcé[278], la prise de photographies ou d'empreintes digitales[279], les autopsies[280], l'obligation imposée à un détenu de se raser avant d'être confronté à un témoin[281], un contrôle de sécurité à l'entrée d'une prison[282], etc. 213

La protection de l'intégrité psychique implique aussi l'interdiction des méthodes qui visent à annihiler la personnalité, comme l'utilisation de détecteurs de mensonges, de sérums de vérité ou de narco-analyses, sans quoi le noyau intangible de la liberté personnelle serait touché[283]. Ces techniques sont aussi 214

[272] Pour déterminer la paternité dans une procédure de droit de la famille (ATF 89 I 92, 99, Kind X., du 20 mars 1963), ou le taux d'alcoolémie d'un conducteur (ATF 91 I 31, 34, GRIS, du 31 mars 1965), ou encore pour effectuer une analyse ADN dans le cadre d'une procédure pénale (ATF 124 I 80, 81, X., du 20 mars 1998).

[273] ATF 104 Ia 480, 486, MEYLAN, du 8 février 1978.

[274] ATF 99 Ia 747, 749, ETIENNE, du 7 novembre 1973.

[275] Dans le but d'établir un profil d'ADN : ATF 128 II 259, 268, Z., du 29 mai 2002. Le Tribunal fédéral a retenu qu'un frottis de la muqueuse jugale ou une prise dans sang dans le but d'établir un profil ADN portent atteinte au droit à la sphère intime de l'individu, à l'intégrité corporelle et au droit à l'autodétermination en matière de données personnelles.

[276] ATF 118 Ia 427, 432, C., B., und Ehepaar R., du 26 novembre 1992.

[277] ATF 90 I 29, 39, X., du 25 mars 1964.

[278] ATF 126 I 112, 115, S., du 23 mai 2000 et 127 I 6, 12, P., du 22 mars 2001. Un tel traitement porte également atteinte à la protection de l'intégrité psychique.

[279] ATF 120 Ia 147, 149, B., du 15 juin 1994. Également considéré comme une atteinte à la sphère privée : ATF 109 Ia 146, 155, Comité contre la loi sur la police et Duvanel, du 6 juillet 1983.

[280] ATF 111 Ia 231, 232, HIMMELBERGER, du 18 septembre 1985.

[281] ATF 112 Ia 161, 162, X., du 3 septembre 1986.

[282] Cas d'un avocat rendant visite à son client : ATF 130 I 65, 67, X., du 27 janvier 2004.

[283] ATF 109 Ia 273, 289, Hans VEST, du 9 novembre 1983. Dans un arrêt P051583F du 5 février 2006, la Cour de cassation de Belgique a estimé que le recours au test du polygraphe était conforme aux exigences de procès équitable de l'art. 6 CEDH et à la présomption d'innocence de l'art. 14.3 lit. g Pacte ONU II.

interdites par le respect de la dignité humaine[284]. Le Tribunal fédéral a en outre reconnu comme atteinte à l'intégrité psychique l'ordre donné à un prévenu de s'enivrer pour évaluer son état de responsabilité sous l'influence de l'alcool[285].

215 La liberté de mouvement avait pour origine d'assurer une protection contre les arrestations et détentions arbitraires. Les tribunaux ont d'ailleurs développé une jurisprudence importante en matière de conditions de détention et d'arrestation. Cela ne signifie pas pour autant qu'il n'y a atteinte à la liberté de mouvement qu'en cas d'incarcération, bien au contraire. Le Tribunal fédéral a estimé que l'obligation de servir pour le personnel médical en cas de catastrophe constituait une atteinte[286], de même que l'obligation d'avoir sur soi des papiers d'identité. Des restrictions de circulation ou des contrôles douaniers ou policiers peuvent aussi restreindre cette liberté[287].

4. La protection de la vie privée

216 La protection de la vie privée ressort des art. 13 al. 1 Cst., 8 CEDH et 17 Pacte II. 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. On parle aussi du droit de vivre autant qu'on le désire à l'abri des regards étrangers.

217 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

Nous préciserons cependant que la dignité humaine ou la liberté personnelle n'ont pas été invoquées, et surtout que la personne interrogée a initialement demandé ce mode d'interrogatoire : « l'utilisation de cette méthode spéciale d'interrogatoire ne saurait violer le droit au silence de celui qui s'y soumet volontairement et peut décider à tout moment d'y renoncer ».

[284] BÉNÉDICT, *Le sort des preuves illégales*, pp 107-109; DELESSERT, *Les méthodes techniques de surveillance*, pp 189-191.

[285] ATF 90 I 29, 39, X., du 25 mars 1964.

[286] ATF 115 Ia 277, 287, B., du 3 mai 1989.

[287] ATF 109 Ia 146, 150, Comité contre la loi sur la police et DUVANEL, du 6 juillet 1983 et ATF 136 I 87, 101, Demokratische Juristinnen und Juristen Zürich, du 30 septembre 2009.

matière sexuelle appartiennent au champ de protection de la vie privée. La protection de la vie privée s'applique également aux personnes détenues[288].

La notion de vie privée englobe également les données sur les activités professionnelles ou commerciales d'un individu[289]. La Cour européenne des droits de l'Homme a renoncé à une définition et préfère recourir à une approche casuistique. Elle retient toutefois que la vie privée couvre l'intégrité physique et morale d'une personne et que sa protection est principalement destinée à assurer le développement, sans ingérence, de la personnalité de chaque individu dans ses relations avec ses semblables[290]. En droit interne, l'intégrité physique et l'intégrité morale sont protégées par la liberté personnelle, de même que la protection des données, également rattachée par la Cour à la protection de la sphère privée. 218

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, notamment des données d'identification[291], des données concernant un traitement médical, l'identité sexuelle[292], la participation à une 219

[288] Pour une définition analogue : AUBERT / MAHON, *Petit commentaire*, pp 123-135; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 184-189; BAUM, *Der kriminalpräventive Einsatz von Videoüberwachungsanlagen*; BIAGGINI, *BV Kommentar*, pp 312-134; BONDALLAZ, *Le droit à une télécommunication protégée*, ch. 11-17; BREITENMOSER, *Art. 13 BV*, pp 190-197; DRZEMCZEWSKI, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance*, p. 8; HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*, pp 117-120; KIENER / KÄLIN, *Grundrechte*, pp 148-149; MOCK, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance*, pp 239-240; RHINOW, *Grundzüge*, pp 221-223. Sur le droit à la vie privée « numérique », en particulier le droit à une télécommunication protégée et le droit à l'anonymat : BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 232-307. Pour une comparaison avec le droit allemand et américain : BARTSCH, *Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen*, pp 51-65.

[289] Arrêt AMANN c. Suisse [GC], no 27798/95, § 65, CEDH 2000-II, résumé in JAAC 64.144. La Cour a d'ailleurs 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.

[290] 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.

[291] L'obligation faite à un policier de porter un badge d'identification constitue une atteinte : ATF 124 I 85, 87, Polizeibeamtenverband Basel-Stadt, du 23 avril 1998.

[292] ATF 119 II 264, 268, X., du 3 mars 1993.

association ou encore les dossiers de procédures judiciaires[293]. L'enregistrement d'images de surveillance prises sur des places ou des voies publiques et la conservation de ces enregistrements portent atteinte à la sphère privée, comme la conservation de données signalétiques[294]. Le Tribunal fédéral a annulé la disposition d'une loi sur la police autorisant la surveillance de lieux publics au moyen d'appareils techniques, car ce règlement ne mentionnait pas le but visé par la surveillance. Le Tribunal a considéré qu'il n'est pas possible dans ces circonstances de contrôler s'il y a un intérêt public suffisant justifiant une atteinte aux libertés individuelles, ni si l'atteinte aux libertés est proportionnée[295].

220 Dans un arrêt surprenant et peu convaincant, le Tribunal fédéral a cependant retenu que la surveillance d'un véhicule à l'aide d'une balise GPS ne constituait pas une atteinte de la même intensité que des écoutes téléphoniques, la surveillance de la correspondance, ou encore une surveillance audio ou vidéo de locaux privés[296]. La saisie du journal intime d'une prévenue est également protégée par la liberté individuelle[297].

221 En 1998, la Commission européenne des droits de l'Homme a retenu qu'en l'absence de tout enregistrement, un système de prise de vues installé dans un but de surveillance des lieux publics ne porte pas atteinte à la vie privée : les données visuelles recueillies ne peuvent pas être portées à la connaissance du public et les données qui pourraient être recueillies par une personne se trouvant derrière des écrans de contrôle sont identiques à celles qu'elle aurait pu obtenir

[293] ATF 119 Ia 99, 101, H., du 17 mars 1993.

[294] ATF 136 I 87, 101, Demokratische Juristinnen und Juristen Zürich, du 30 septembre 2009 et ATF 133 I 77, 80, DIGGELMANN, du 14 décembre 2006. Pour une critique de cet arrêt : RUDIN, *Videoüberwachung*.

[295] ATF 136 I 87, 114-116, Demokratische Juristinnen und Juristen Zürich, du 30 septembre 2009.

[296] ATF 1P.51/2007, X., du 24 septembre 2007, consid. 3.5.4. Le Tribunal fédéral a peut-être été tenté de qualifier l'atteinte de très minime pour pouvoir admettre ensuite la preuve recueillie illégalement et essentielle à la condamnation de l'auteur pour vols en bande et par métier, dommages à la propriété, etc.

[297] ATF 1P.519/2006, X., du 19 décembre 2006, consid. 3.2. Le TF a toutefois considéré que la protection n'était pas absolue et qu'il fallait procéder à une pesée d'intérêts. Le droit de ne pas s'auto-incriminer n'empêche pas la saisie de documents. La décision de l'autorité inférieure est publiée dans la *Revue de droit suisse* 2008, Vol. 103 (22), pp 558-562.

par sa présence sur les lieux[298]. Ce raisonnement n'est certainement plus défendable aujourd'hui où l'informatique permet, sans enregistrement, à une seule personne de surveiller de très nombreux écrans et qu'un programme informatique peut assumer seul la détection de certains événements, certaines personnes ou encore assurer le suivi d'un individu donné au travers de caméras différentes. Dans la mesure où il n'est pas possible de voir la personne qui est derrière un écran, contrairement à un policier qui patrouille dans la rue, certains estiment qu'il y a aussi une atteinte au droit à l'autodétermination informationnelle[299]. La Cour européenne des droits de l'Homme a pourtant confirmé sa jurisprudence en 2008, estimant que la simple surveillance des activités d'un individu qui se sont déroulées en public, pendant une brève durée de temps et sans que les autorités enregistrent et mémorisent les données visuelles observées, ne saurait constituer en elle-même une forme d'ingérence dans la vie privée[300]. En 2010, la Cour européenne des droits de l'Homme a pourtant condamné la législation britannique qui permettait à un policier d'interpeller sur rue une personne et de passer ses mains à l'intérieur des poches, du col, des chaussures et des cheveux, et cela en l'absence de tout motif raisonnable de soupçonner une infraction mais dans le but de lutter contre le terrorisme. La Cour a retenu que cette ingérence ne saurait être comparée à une fouille dans un aéroport, car ce passager-là sait qu'il sera fouillé et il peut alors choisir un autre mode de transport[301].

Le Tribunal fédéral a encore retenu que le fait de conserver des données anthropométriques, en l'espèce une photographie, pouvait porter atteinte à la présomption d'innocence et à la protection de la sphère privée, par exemple si l'autorité exprime par là le sentiment que la personne concernée est coupable bien qu'elle ait été acquittée ou que la procédure ait été suspendue[302]. Le 222

[298] Herbecq c. Belgique, décision de la Commission du 14 janvier 1998, Décisions et rapport 92-A, p. 92. La Cour a confirmé cet avis dans l'Arrêt P.G. et J.H. c. Royaume-Uni, N° 44787/98, § 57, CEDH 2001-IX.

[299] Pour un avis similaire : RUEGG / FLÜCKIGER / NOVEMBER, *et al.*, *Vidéosurveillance et risques dans l'espace à usage public*, pp 53-55.

[300] Arrêt CALMANOVICI c. Roumanie, no 42250/02, § 132, du 1er juillet 2008.

[301] Arrêt GILLAN and QUINTON c. Royaume-Uni, n°4158/05, §§ 61-65, du 12 janvier 2010. La comparaison avec l'aéroport ne nous convainc pas tellement, car de fait la possibilité de choisir un autre mode de transport est limitée.

[302] ATF 120 Ia 147, 149-155, B., du 15 juin 1994.

Tribunal fédéral estime qu'une personne ne peut être identifiée de façon sûre par ce moyen et que la conservation de ce matériel exposerait la personne à être mise en cause dans d'autres procédures à cause d'une simple ressemblance. Il en irait différemment d'un prélèvement d'ADN qui permet une identification certaine. Le Tribunal estime cependant que le risque de soupçonner une personne innocente augmente si les données sont conservées longtemps et que les échantillons, comme le résultat de l'analyse, doivent être détruits si la culpabilité de l'intéressé peut être définitivement exclue[303]. Le Tribunal fédéral a précisé ultérieurement que la destruction précitée était justifiée parce que la personne n'avait été suspectée qu'en raison de sa ressemblance avec un portrait-robot. Il en va différemment si la personne a des antécédents et qu'il existe un risque de récidive[304].

223 Dans un arrêt récent, la Cour européenne des droits de l'Homme s'est dite particulièrement préoccupée par le risque de stigmatisation découlant du fait que des personnes qui n'ont été reconnues coupables d'aucune infraction et sont en droit de bénéficier de la présomption d'innocence sont traitées de la même manière que des condamnés, et cela même si la conservation de profils d'ADN n'équivaut pas à l'expression de soupçons. Elle a jugé que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, des échantillons biologiques et des profils d'ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que cette conservation s'analyse en une atteinte disproportionnée au droit au respect de la vie privée et ne peut passer pour nécessaire dans une société démocratique[305].

5. L'autodétermination individuelle

224 Le droit à l'autodétermination individuelle ressort notamment des art. 10 al. 2 et 13 Cst., ainsi que 9 CEDH. Ce droit se recoupe en partie avec la liberté

[303] ATF 124 I 80, 84, X, du 20 mars 1998.

[304] ATF 128 II 259, 276, Z., du 29 mai 2002. Dans l'ATF 1P.362/2006 du 23 novembre 2006, le Tribunal fédéral a confirmé que la destruction des données s'imposait également en cas de retrait des poursuites. Il s'est en partie appuyé sur le droit à l'autodétermination individuelle de l'art. 13 al. 2 Cst.

[305] Arrêt S. et MARPER c. Royaume-Uni, no 30562/04 et 30566/04, §§ 122-125 , du 4 décembre 2008.

personnelle et la protection de la sphère privée, en ce sens qu'il permet à chacun de décider librement des relations qu'il entretient, de l'organisation de ses loisirs, des données personnelles qu'il rend publiques, du sort de sa dépouille après sa mort ou encore de son désir d'avoir des enfants[306].

Le Tribunal fédéral estime que portent atteinte au droit à l'autodétermination individuelle la mise au secret d'un prévenu et l'interdiction faite à celui-ci de communiquer avec des tiers[307], le refus de permettre l'accès à un dossier de police[308], ou encore la publication de l'ensemble des informations d'un candidat à la naturalisation[309]. 225

6. La protection des données personnelles

La protection des données et l'autodétermination informationnelle sont assurées par les art. 13 al. 2 Cst., 8 CEDH et la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concrétisés par la Loi fédérale du 19 juin 1992 sur la protection des données[310]. Ces droits sont un aspect particulier du droit au respect de la sphère privée et de la liberté individuelle. 226

Le droit de toute personne d'être protégée contre l'emploi abusif des données personnelles qui la concernent implique le droit d'être informée de l'existence de telles données et d'obtenir la rectification des données inexactes et la suppression des données inutiles. Par données personnelles, nous entendons toute information sur les caractéristiques physiques, psychiques, sociales ou politiques d'un individu, indépendamment du support utilisé. Les droits garantis concernent les données de base, telles qu'elles sont enregistrées, mais également 227

306 MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, pp 164-182; RHINOW, *Grundzüge*, pp 217-218; RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*, pp 270-273; SCHEFER, *Grundrechte, Ergänzungsband*, pp 32-47; SCHWEIZER, *Art. 10 BV*, pp 265-266. Sur la notion de droit à l'anonymat: RUDIN, *Das Recht auf Anonymität*.

307 ATF 103 Ia 293, 296, BONZI, du 23 février 1977.

308 ATF 113 Ia 1, 5, M., du 28 janvier 1987.

309 ATF 129 I 232, 246, Schweizerische Volkspartei der Stadt Zürich (SVP), MEIER et TUENA, du 9 juillet 2003.

310 LPD, RS 235.1.

celles qui résultent de leur traitement, soit les analyses et appréciations faites sur la base de ces données et consignées dans des dossiers[311].

228 Le Tribunal fédéral a retenu que l'établissement et le traitement d'un profil d'ADN portaient atteinte au droit à la protection contre l'emploi abusif de données personnelles[312]. 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[313]. Le Tribunal fédéral a déclaré proportionnée la conservation de données issues de caméra de vidéosurveillance durant cent jours[314]. Il a récemment confirmé que l'adresse IP est aussi une donnée personnelle protégée par la sphère privée[315].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[316].

7. La protection du domicile

229 Le droit au respect du domicile est garanti par les art. 13 al. 1 Cst., 8 CEDH et 17 Pacte II. Il est concrétisé légalement par l'art. 186 CP qui sanctionne la violation de domicile. Le domicile doit être compris au sens large, soit tout endroit où une personne mène sa vie privée à titre exclusif. Il englobe le lieu d'habitation, l'appartement ou la maison, mais aussi tout espace privé, même

[311] Pour des définitions analogues : AUBERT / MAHON, *Petit commentaire*, pp 130-131; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 187-189; BIAGGINI, *BV Kommentar*, pp 134-136; BREITENMOSER, *Art. 13 BV*, pp 203-210; GRAFFENRIED, *Actes de la police judiciaire*, pp 141-143; HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*, pp 119-120; KIENER / KÄLIN, *Grundrechte*, pp 158-161; RHINOW, *Grundzüge*, pp 227-228. Sur les exigences européennes (applicables à la Suisse en tant que membre du Conseil de l'Europe ou par la reprise de l'acquis lié aux accords de Schengen/Dublin) : RUDIN, *Datenschutzgesetze*.

[312] ATF 128 II 259, 268, Z., du 29 mai 2002.

[313] ATF 122 I 360, 362, B. et consorts, du 28 nombre 1996.

[314] ATF 136 I 87, 101, Demokratische Juristinnen und Juristen Zürich, du 30 septembre 2009. Pour une critique de cet arrêt : RUDIN, *Videoüberwachung*.

[315] Arrêt à paraître dans la cause PFPDT c. Logistep SA, 1C_285/2009, suite à l'audience publique tenue le 8 septembre 2010.

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

ouvert, tels un jardin ou une cour, et provisoire ou temporaire, comme une chambre d'hôtel, une caravane ou une tente. La protection du domicile vaut également pour le domicile professionnel, et la qualité de locataire ou propriétaire est indifférente[317].

Les questions controversées concernent surtout les perquisitions, visites domiciliaires et autres mesures de surveillance. 230

Le Tribunal fédéral n'a apparemment encore jamais dû trancher la question de savoir si un véhicule pouvait bénéficier de la protection du domicile. En 1974, la Commission européenne des droits de l'Homme avait retenu que la fouille d'une voiture privée stationnée sur la voie publique n'était pas considérée comme une perquisition et que les garanties liées à la protection du domicile ne s'appliquaient pas[318]. La doctrine récente considère en revanche que les véhicules doivent aussi bénéficier de la protection constitutionnelle du domicile[319]. 231

8. Le secret de la correspondance et des télécommunications

Le droit au respect de la correspondance, ainsi que des relations établies par la poste et les télécommunications est un autre aspect essentiel de la sphère privée. Il est garanti par les art. 13 al. 1 Cst., 8 CEDH et 17 Pacte II. Légalement, il est concrétisé par les art. 179ss CP (infractions contre le domaine secret ou le 232

[317] Pour des définitions analogues : AUBERT / MAHON, *Petit commentaire*, p. 128; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, p. 196; BREITENMOSER, *Art. 13 BV*, pp 201-202; DRZEMCZEWSKI, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance*, pp 14-15; HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*, p. 119; KIENER / KÄLIN, *Grundrechte*, pp 154-155; MOCK, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance*, p. 243; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, pp 183-200; RHINOW, *Grundzüge*, p. 226; RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*, pp 273-275; SCHEFER, *Grundrechte, Ergänzungsband*, pp 86-91; STEINER, *Das Grundrecht der Unverletzlichkeit der Wohnung*; VON GUNTEN, *Das Grundrecht auf Unverletzlichkeit der Wohnung*.

[318] X. c. Belgique, no 5488/72, décision de la Commission du 30 mai 1974, Décisions et rapports 45, pp 20-22.

[319] GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 20-21 et les références citées. A noter qu'en droit pénal, un véhicule exclusivement destiné au transport n'est pas considéré comme une habitation et n'est pas protégé par l'art. 186 CP sanctionnant la violation de domicile : CORBOZ, *Les infractions en droit suisse I*, p. 704; DELNON / RÜDY, *Art. 186 StrGB*, p. 1077.

domaine privé) et l'art. 321^ter CP (violation du secret des postes et des télécommunications). Il couvre l'ensemble des communications qu'une personne peut établir avec autrui, indépendamment du vecteur utilisé : communication orale, écrite, par voie de poste, télégraphe, téléfax, téléphone, réseau électronique, etc. Les documents déjà parvenus à leur destinataire ne sont en revanche plus couverts par le secret de la correspondance[320].

233 Le Tribunal fédéral a confirmé que le secret des télécommunications vaut aussi pour les communications par courriel au moyen d'Internet, et cela indépendamment du fait que l'infrastructure soit fournie par une organisation étatique comme l'étaient les PTT ou par une entreprise privée[321]. Actuellement, on doit admettre que les communications effectuées par Internet sont couvertes par le secret de la correspondance et des télécommunications, qu'il s'agisse de courriels, de messagerie instantanée, ou de téléphonie[322]. Sont également protégés l'identification de l'utilisateur, de l'interlocuteur et du raccordement téléphonique, le moment et la durée de la conversation, ainsi que les adresses et la période à laquelle un utilisateur a envoyé ou reçu des messages[323]. L'écoute téléphonique des interlocuteurs et des utilisateurs du même raccordement constitue en soi une atteinte grave à leurs droits constitutionnels. Cela d'autant plus que l'écoute effective est irréversible et que l'atteinte est maintenue et

[320] Pour des définitions analogues : AUBERT / MAHON, *Petit commentaire*, pp. 128-129; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 197-200; BIAGGINI, *BV Kommentar*, p. 134; BONDALLAZ, *Le droit à une télécommunication protégée*, ch. 43-46; BREITENMOSER, *Art. 13 BV*, pp 202-203; DRZEMCZEWSKI, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance*, pp 15-16; HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*, p. 119; KIENER / KÄLIN, *Grundrechte*, pp 156-158; MOCK, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance*, pp 243-244; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, pp 201-217; RHINOW, *Grundzüge*, pp 226-227; RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*, pp 275-277; SCHEFER, *Grundrechte, Ergänzungsband*, pp 92-99. Sur les libertés de communication en général : BARRELET, *Une nouvelle liberté*. Voir également pour une approche liée aux mesures de surveillance, bien qu'essentiellement consacrée au droit français : GEORGEL, *Les libertés de communication*.

[321] ATF 126 I 50, 65, Swiss Online, du 5 avril 2000.

[322] Une réserve doit cependant être appliquée pour les conversations tenues sur les forums de discussion ou les chats, le caractère privé de la discussion pouvant faire défaut. Voir également les notes de bas de page 463 et 486 ci-dessous.

[323] ATF 126 I 50, 62-63, Swiss Online AG, du 5 avril 2000, et ATF 130 III 28, 32, A., du 21 octobre 2003.

aggravée par l'établissement de procès-verbaux, leur utilisation et leur éventuelle divulgation[324].

La Cour européenne des droits de l'Homme a pour sa part rappelé à de nombreuses reprises que les écoutes téléphoniques représentent une atteinte grave au respect de la correspondance et qu'en conséquence elles doivent, pour être licites, satisfaire aux exigences du paragraphe 2 de l'article 8 CEDH et, tout spécialement, se fonder sur une loi d'une précision particulière, d'autant que les procédés techniques ne cessent de se perfectionner[325]. 234

9. Les libertés d'opinion et d'information

Les libertés d'opinion et d'information sont garanties par les art. 16 Cst., 9 et 10 CEDH, 19 Pacte II et 13 de la Convention relative aux droits de l'enfant. Le Tribunal fédéral a reconnu la liberté d'opinion et d'expression comme droit fondamental non écrit en 1965 et la liberté d'information en 1978[326]. Les libertés d'opinion et d'information font partie des libertés de communication, au même titre que les libertés des médias, de la science, de l'art, de réunion, d'association, de pétition et les droits politiques. 235

La liberté d'opinion confère à chacun le droit d'avoir une opinion et de la répandre, de ne pas en avoir, ou de ne pas l'exprimer. La liberté d'opinion s'applique à n'importe quel message de la pensée humaine, indépendamment du vecteur utilisé. La liberté d'information se limite, elle, aux seules informations généralement accessibles ou disponibles. Le Tribunal fédéral considère que les libertés d'expression sont une condition de l'exercice de la liberté individuelle et un élément indispensable à l'épanouissement de la personne humaine et qu'elles constituent le fondement de tout Etat démocratique[327]. 236

[324] ATF 125 I 96, 101-102, A.G., B.G., C.G. et D.G, du 28 janvier 1999.

[325] Arrêt KOPP c. Suisse no 23224/94, § 72, CEDH 1998-II, du 25 mars 1998, résumé in JAAC 62.114.

[326] ATF 91 I 480, 485, Association de l'Ecole française de Zurich, du 31 mars 1965, et ATF 104 Ia 88, 93-94, Schweizerische Journalisten-Union, du 8 mars 1978.

[327] Pour des définitions analogues : AUBERT / MAHON, *Petit commentaire*, pp 150-161; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 262-274; BIAGGINI, *BV Kommentar*, pp 145-149; HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*, pp 134-150; KLEY / TOPHINKE, *Art. 16 BV*, pp 366-384; RHINOW, *Grundzüge*, pp 251-259.

237 Le contenu des informations (dans un sens très large) est protégé, mais également les moyens et les modalités de transmission et de réception[328].

10. La liberté de réunion

238 La liberté de réunion est garantie par les art. 22 Cst., 11 CEDH et 21 Pacte ONU II. Elle a été reconnue par le Tribunal fédéral comme droit fondamental non écrit en 1970, en tant que condition de l'exercice des droits politiques et élément indispensable du régime démocratique[329].

239 Cette liberté garantit le droit d'organiser une réunion, de participer à une réunion ou de ne pas y prendre part. Par réunion, on entend généralement tout rassemblement pacifique de plusieurs personnes, de durée limitée, dans un lieu déterminé et dans le but de communiquer et d'échanger des idées ou des opinions. La liberté de réunion s'applique indépendamment du nombre de personnes, de la durée de la réunion, du fait qu'elle a lieu en plein air ou dans un local fermé, sur fond public ou privé. Une réunion peut aussi se concevoir en mouvement, tels un cortège ou une manifestation[330].

240 Lorsque la réunion impose un usage accru du domaine public (on parle alors généralement de manifestation), elle peut être soumise à autorisation préalable. L'autorité ne peut cependant pas refuser une autorisation au motif qu'elle ne partage pas l'opinion des manifestants[331].

[328] ATF 120 Ib 142, 148, Obersee Nachrichten AG, du 11 mars 1994.

[329] ATF 96 I 219, 224, NÖTHIGER, du 24 juin 1970.

[330] Pour des définitions analogues : AUBERT / MAHON, *Petit commentaire*, pp 189-195; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 189-195; BIAGGINI, *BV Kommentar*, pp 167-171; MÜLLER / SCHEFER, *Grundrechte in der Schweiz*, pp 571-593; RHINOW, *Grundzüge*, pp 270-273; ROHNER, *Art. 22 BV*, pp 453-463; SCHEFER, *Grundrechte, Ergänzungsband*, pp 210-216.

[331] ATF 107 Ia 226, 230, Unité jurassienne Corgémont, du 24 juin 1981.

D. La théorie générale des restrictions des libertés

1. Les restrictions admises par la Constitution

L'art. 36 Cst. prévoit que toute restriction d'un droit fondamental doit être 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 est inviolable et les restrictions graves doivent être prévues par une loi[332]. 241

2. L'ingérence admise par l'art. 8 al. 2 CEDH

La CEDH ne contient pas, comme la Constitution, une norme générale fixant les conditions auxquelles une liberté peut être restreinte[333]. Chaque article relatif à une liberté précise les conditions de sa propre restriction et énumère les intérêts publics admissibles. Ainsi l'art. 8 al. 2 CEDH précise qu'une 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. 242

Les art. 10 à 12 CEDH contiennent, dans une formulation légèrement différente, les mêmes conditions, qui sont également semblables à celles de la Constitution. On notera que le Pacte II suit la même méthode que la CEDH. 243

[332] Sur la théorie générale de restrictions des libertés : AUBERT / MAHON, *Petit commentaire*, pp 319-331; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*, pp 79-119; BIAGGINI, *BV Kommentar*, pp 75-109; HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*, pp 90-101; HALLER, *The Swiss Constitution*, pp 157-162; RHINOW, *Grundzüge*, pp 199-206; RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*, pp 237-245; SCHWEIZER, *Art. 36 BV*, pp 727-742. De manière générale et plus particulièrement dans le cas d'une surveillance : BAUM, *Der kriminalpräventive Einsatz von Videoüberwachungsanlagen*; GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 23-42. Dans le cas de l'investigation secrète : VETTERLI, *Verdeckte Ermittlung und Grundrechtsschutz*, pp 370-372.

[333] RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*, p. 246.

3. La base légale

244 L'exigence de la base légale ressort tant de la Constitution que de la CEDH. Les restrictions doivent donc être prévues par une règle de droit, générale et abstraite, qui assure la prévisibilité et la sécurité du droit, ainsi que l'égalité de traitement. La Constitution exige une base légale formelle pour les restrictions graves. Plus une restriction est importante, plus la base légale doit être claire et précise. Le Tribunal fédéral parle d'ailleurs d'une base légale claire et précise[334].

245 Dans le cadre de la CEDH, la base légale peut consister en une loi formelle ou être d'origine jurisprudentielle, mais elle doit être suffisamment accessible et énoncée avec assez de précision pour permettre au citoyen de régler sa conduite[335]. La Cour entend ici la notion de loi au sens matériel et n'exige pas une base légale formelle. Dans les Etats de *common law*, la Cour considère comme loi une création juridictionnelle. Afin de ne pas créer de différences entre Etats, elle a admis que la base légale de l'ingérence puisse aussi être constituée par la jurisprudence interprétant la loi dans les pays continentaux[336]. Dans un domaine couvert par le droit écrit, la loi est alors le texte en vigueur tel que les juridictions compétentes l'ont interprété en ayant égard, au besoin, à des données techniques nouvelles[337].

246 A mesure que l'art. 36 Cst. exige, pour les restrictions graves, une base légale formelle, soit une norme générale et abstraite adoptée par le législateur formellement institué par la Constitution, une pure création jurisprudentielle ne serait vraisemblablement pas suffisante en droit suisse. Une simple précision de la loi par la jurisprudence paraît en revanche plus acceptable.

---

[334] ATF 116 Ia 118, 122, B., du 27 août 1990 et ATF 136 I 87, 91-92, Demokratische Juristinnen und Juristen Zürich, du 30 septembre 2009.

[335] Sunday Times c. Royaume-Uni, arrêt du 26 avril 1979, série A no 30, § 49.

[336] COUSSIRAT-COUSTERE, *art. 8 § 2 CEDH*, pp 334-335.

[337] KRUSLIN c. France, arrêt du 24 avril 1990, série A no 176, § 29. Dans cet arrêt, la Cour a admis qu'une jurisprudence établie depuis de longues années par la Cour de cassation et int122erprétant du droit écrit est une base légale suffisante.

L'examen des lois pouvant servir de base légale en matière de surveillance sera repris ultérieurement[338]. 247

4. L'intérêt public

La restriction à une liberté doit être justifiée par un but d'intérêt public ou par la protection d'un droit fondamental d'autrui. La notion d'intérêt public varie dans le temps et dans l'espace. Certaines composantes de l'intérêt public peuvent justifier des restrictions à certaines libertés, alors qu'elles ne suffiraient pas à justifier une restriction à d'autres. L'intérêt public regroupe notamment l'ordre public (sécurité, santé, tranquillité, moralité publique et bonne foi dans les affaires), les préoccupations de politique sociale, d'équilibre écologique, etc. La CEDH ne parle pas d'intérêt public, mais en énumère les principales composantes : la sécurité nationale, la sûreté publique, le bien-être économique du pays, la défense de l'ordre et la prévention des infractions pénales, la protection de la santé ou de la morale, et finalement la protection des droits et libertés d'autrui. 248

Le Tribunal fédéral estime qu'il y a par principe un intérêt public à élucider des infractions déjà commises et à empêcher de nouvelles infractions au moyen de mesures d'identification[339]. 249

5. La proportionnalité

La Constitution exige que la restriction apportée soit proportionnée au but, ce qui recouvre les critères d'aptitude, de nécessité et de proportionnalité au sens étroit. La restriction doit ainsi être apte à atteindre le but d'intérêt public visé et ne pas être plus rigoureuse que nécessaire. Il doit en outre encore exister un rapport raisonnable entre le but et l'atteinte portée à la liberté[340]. 250

La CEDH parle d'une ingérence nécessaire dans une société démocratique. L'atteinte portée à la liberté doit reposer sur un besoin social impérieux, dont les 251

[338] Voir à ce sujet le chapitre III. Les principales lois traitant de la surveillance technique, p. 122 ci-dessous.
[339] ATF 120 Ia 147, 151, B., du 15 juin 1994.
[340] ATF 136 I 87, 91-92, Demokratische Juristinnen und Juristen Zürich, du 30 septembre 2009.

motifs sont pertinents et suffisants, et respecter un rapport de proportionnalité entre le moyen employé et le but[341].

252 Même si l'Etat jouit d'une certaine marge d'appréciation quant à la nécessité de procéder à une perquisition, il faut que son déroulement soit encadré par des garanties adéquates et suffisantes contre les abus de sorte que les ingérences restent étroitement proportionnées au but légitime recherché[342].

6. L'inviolabilité de l'essence des libertés

253 La Constitution précise encore que l'essence des droits fondamentaux est inviolable, autrement dit qu'il ne peut être porté atteinte au noyau intangible du droit en question. Dans certains cas, le contenu du droit fondamental et le noyau dur se recoupent, par exemple pour le droit à la vie, l'interdiction de la torture et des peines ou traitements cruels, inhumains ou dégradants, ou encore le droit d'obtenir de l'aide dans des situations de détresse[343].

254 La CEDH ne contient pas expressément une telle notion de noyau dur, mais la Cour a parfois relevé que la substance même des droits garantis ne devait pas être atteinte. La protection de l'atteinte au noyau dur se fait aussi, implicitement, lors du contrôle de la nécessité dans une société démocratique. L'art. 3 CEDH ne tolère aucune dérogation, indépendamment du comportement de la personne concernée ou de l'infraction reprochée, et même en cas de danger public menaçant la vie d'un individu ou de la nation[344].

255 Le Tribunal fédéral considère que les écoutes téléphoniques et l'utilisation de dispositifs techniques de surveillance ne portent pas atteinte au noyau dur de la liberté individuelle. Ces méthodes ne font qu'enregistrer l'expression de la

[341] Sur le principe de la proportionnalité dans la vidéosurveillance dans le cadre de l'art. 8 CEDH et en droit communautaire : MORNET, *La vidéosurveillance et la preuve*, pp 125-135.

[342] FUNKE c. France, arrêt du 25 février 1993, série A no 256-A, § 57.

[343] Sur le droit à la vie, ATF 98 Ia 508, 514, GROSS, du 28 juin 1972, et sur la garantie d'un minimum vital au sens de l'art. 12 Cst., ATF 131 I 166, 172, X., du 18 mars 2005 confirmé par l'ATF 135 I 119, 123 et 126, S., du 20 mars 2009.

[344] Arrêt Gäfgen c. Allemagne [GC], no. 22978/05, §§ 86-87 et 107, du 1er juin 2010.

conscience et de la volonté, et les agissements que la personne surveillée aurait également eus en l'absence d'une surveillance[345].

E. Les exigences fondamentales en matière de surveillance

La Cour a admis que la surveillance secrète de la correspondance, des envois postaux et des télécommunications pouvait, devant une situation exceptionnelle, se révéler nécessaire dans une société démocratique à la sécurité nationale, à la défense de l'ordre et à la prévention des infractions pénales. Elle exige cependant des garanties adéquates et suffisantes pour prémunir les individus contre d'éventuels abus des autorités[346]. Dans le cadre d'une perquisition, la Cour a admis que même si l'Etat jouit d'une certaine marge d'appréciation, il faut que son déroulement soit encadré par des garanties adéquates et suffisantes contre les abus de sorte que les ingérences restent étroitement proportionnées au but légitime recherché[347]. On peut donc tirer de la jurisprudence de la Cour européenne des droits de l'Homme un certain nombre de principes applicables à toutes les mesures techniques de surveillance. 256

1. L'interdiction d'une surveillance générale et préventive

L'atteinte portée aux libertés fondamentales par les mesures de surveillance doit respecter strictement le principe de proportionnalité. Elles ne sont admissibles que dans des cas spécifiés dans la loi en vue d'un but légitime d'après la CEDH. 257

[345] ATF 109 Ia 273, 290, Hans VEST, du 9 novembre 1983. Pour un avis un peu plus nuancé : GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 37-42.

[346] Les arrêts KVASNICA c. Slovaquie, no 72094/01, du 9 juin 2009, CALMANOVICI c. Roumanie, no 42250/02, du 1er juillet 2008 et Dumitru POPESCU c. Roumanie (N° 2), no 71525/01, du 26 avril 2007, confirment la jurisprudence rendue précédemment notamment dans les arrêts KLASS c. Allemagne, du 6 septembre 1978, série A no 28, MALONE c. Royaume-Uni, du 2 août 1984, série A no 82, et KRUSLIN c. France et HUVIG c. France, du 24 avril 1990, série A no 176-A et 176-B, Valenzuela CONTRERAS c. Espagne, du 30 juillet 1998, Rec. 1998-V, p. 1910 et P.G. et J.H. c. Royaume-Uni, N° 44787/98, § 57, CEDH 2001-IX. Sur l'influence des arrêts KLASS, MALONE, SCHENK, HUVIG et KRUSLIN : VIENNE, *Les écoutes téléphoniques au regard de la Cour*.

[347] FUNKE c. France, arrêt du 25 février 1993, série A no 256-A, § 57.

Des mesures de surveillance exploratoires ou une surveillance générale et préventive sont dès lors exclues[348].

2. La prévisibilité de la surveillance

258 La base légale 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, et cela d'autant plus que les procédés techniques utilisables ne cessent de se perfectionner.

259 La loi doit contenir la définition des catégories de personnes susceptibles d'être surveillées, la nature des infractions pouvant y donner lieu et la fixation d'une durée limite à l'exécution de la mesure.

260 La prévisibilité permet aussi le respect du principe de finalité : « l'utilisation d'images à d'autres fins que celles pour lesquelles elles ont été recueillies est contraire à l'article 8 de la Convention européenne des droits de l'Homme et donc, l'utilisation d'une vidéo à titre de preuve alors qu'elle n'a pas été constituée pour cela, heurte l'article 8 de la Convention européenne des droits de l'Homme »[349]. Si les mesures de surveillance peuvent confirmer des soupçons déjà existants, elles ne sauraient en revanche les faire naître[350].

3. L'indépendance de l'autorité qui autorise la surveillance

261 La Cour estime que l'autorité qui autorise la surveillance doit être indépendante du pouvoir exécutif. Il est souhaitable qu'elle soit judiciaire. La Cour a cependant admis, dans le cas de l'Allemagne, que la surveillance ordonnée par un fonctionnaire possédant les qualifications requises pour accéder à la magistrature, puis contrôlée par un comité de cinq parlementaires et une commission, respectait les exigences de la Convention, puisque ces deux

[348] COUSSIRAT-COUSTERE, *art. 8 § 2 CEDH*, p. 343.
[349] MORNET, *La vidéosurveillance et la preuve*, p. 177.
[350] BÉNÉDICT, *Le sort des preuves illégales*, p. 210.

derniers organes jouissaient d'une indépendance suffisante pour statuer de manière objective[351].

4. Le contrôle de la surveillance par une autorité judiciaire

La Cour exige que l'individu ait la possibilité d'introduire un recours devant un tribunal[352]. Dans l'arrêt Popescu, la Cour conclut à une violation de l'art. 8 CEDH, notamment parce que l'autorisation du procureur de procéder à l'interception des communications n'était susceptible d'aucun contrôle *a priori* de la part d'un juge ou d'une autre autorité indépendante. La Cour relève l'absence de tout contrôle *a priori* ou *a posteriori* des écoutes par une autorité judiciaire indépendante et impartiale[353]. 262

Ainsi, la possibilité doit être donnée de faire contrôler *a priori* ou *a posteriori* le bien-fondé de la surveillance par une autorité judiciaire indépendante et impartiale. Il ne semble pas nécessaire que les deux contrôles soient assurés par une autorité judiciaire. 263

Pour le Tribunal fédéral, le secret des correspondances téléphoniques exige en revanche un contrôle judiciaire *a priori* et *a posteriori* : un contrôle judiciaire doit avoir lieu lorsque la mesure de surveillance est prononcée, puis l'utilisation du résultat de la surveillance nécessite également un contrôle judiciaire[354]. L'exigence d'un contrôle judiciaire indépendant *a priori* n'implique en revanche pas qu'une voie de recours soit ouverte à ce stade[355]. 264

Un contrôle n'est d'ailleurs possible qu'*a posteriori* pour les interlocuteurs et les autres utilisateurs du raccordement. La personne concernée doit pouvoir 265

[351] Arrêt KLASS c. Allemagne, du 6 septembre 1978, série A n° 28, § 56.
[352] Arrêt KRUSLIN c. France, du 24 avril 1990, série A n° 176-A, § 34.
[353] Arrêt Dumitru POPESCU c. Roumanie (N° 2), no 71525/01, §§ 73 et77, du 26 avril 2007.
[354] ATF 120 Ia 314, 318, G., du 27 décembre 1994 et 122 I 182, 190-191, T., du 2 mai 1996.
[355] ATF 133 IV 182, 185-186, Ministère public de la Confédération, du 15 mars 2007.

demander que le contrôle de la légalité de la surveillance ait lieu déjà au stade de l'instruction, et pas seulement au moment du jugement[356].

5. Le droit de consulter les enregistrements

266 Le Tribunal fédéral considère que le droit de consulter les enregistrements destinés à l'usage ultérieur dans le procès pénal doit être accordé au plus tard lors de la clôture de l'instruction[357]. De manière plus générale, le Tribunal fédéral a également annulé une décision prise en matière de détention provisoire au motif que le juge s'était basé uniquement sur les documents physiques et non sur un CD transmis par le procureur et contenant les transcriptions d'auditions qui n'avaient pas encore été imprimées et jointes au dossier officiel. Le Tribunal a rappelé que le recourant, respectivement son défenseur, doit également avoir accès à ces données, qui pourraient peut être remettre en cause la décision attaquée[358].

6. La conservation des enregistrements intacts jusqu'à la fin du procès pénal

267 La Cour européenne des droits de l'Homme admet que, dans certaines circonstances, il est excessif de transcrire et de verser au dossier d'instruction d'une affaire la totalité des conversations interceptées à partir d'un poste téléphonique. Cela pourrait également aller à l'encontre d'autres droits, tel le droit au respect de la vie privée d'autres personnes qui ont passé des appels à partir du poste mis sous écoute. Dans ce cas, l'intéressé doit néanmoins se voir offrir la possibilité d'écouter les enregistrements ou de contester leur véracité, d'où la nécessité de les garder intacts jusqu'à la fin du procès pénal, et, plus généralement, de verser au dossier d'instruction les pièces qui lui semblent pertinentes pour la défense de ses intérêts. La loi doit d'ailleurs prévoir les précautions à prendre pour communiquer, intacts et complets, les

[356] ATF 122 I 182, 190-193, T., du 2 mai 1996. Cela vaut aussi pour les interlocuteurs et co-utilisateurs des raccordements téléphoniques surveillés : ATF 125 I 96, 102, A.G., B.G., C.G. et D.G, du 28 janvier 1999.

[357] ATF 125 I 96, 103, A.G., B.G., C.G. et D.G, du 28 janvier 1999.

[358] ATF 1B_226/2010, du 23 juillet 2010, consid. 2.3.

enregistrements réalisés, aux fins de contrôle éventuel par le juge et par la défense[359].

La conservation des enregistrements permet également de contrôler la véracité des transcriptions figurant au dossier et éventuellement de faire expertiser l'enregistrement. 268

La Cour a également considéré que le respect des droits de la défense permettait au prévenu d'avoir accès à l'intégralité des enregistrements effectués. Dans des cas particuliers, notamment pour protéger les droits fondamentaux d'un autre individu ou pour sauvegarder un intérêt public important, l'accès peut être limité mais le prévenu doit néanmoins avoir la possibilité de se défendre correctement. Le prévenu a le droit de connaître le contenu des documents qui lui sont interdits d'accès et de demande à une autorité judiciaire de trancher la question[360]. 269

7. La possibilité de faire expertiser les enregistrements

La Cour européenne des droits de l'Homme considère qu'en cas de doute sur la réalité ou la fiabilité d'un enregistrement, il doit y avoir une possibilité claire et effective de le faire expertiser par un centre public ou privé indépendant de celui qui a effectué les écoutes[361]. Cette possibilité devrait aussi exister pour les opérations effectuées sur les enregistrements (traductions, découpages, etc.). 270

8. La mention légale des possibilités de destruction des informations

La loi doit finalement contenir précisément les circonstances dans lesquelles les informations obtenues par une mesure de surveillance peuvent ou doivent être détruites[362]. 271

[359] Arrêt Dumitru POPESCU c. Roumanie (N° 2), no 71525/01, § 78, du 26 avril 2007.
[360] Arrêt NATUNEN c. Finlande, no 21022/04, §§ 39, 42 et 46, du 31 mars 2009.
[361] Arrêt Dumitru POPESCU c. Roumanie (N° 2), no 71525/01, §§ 80-81, du 26 avril 2007.
[362] Arrêt Dumitru POPESCU c. Roumanie (N° 2), no 71525/01, § 79, du 26 avril 2007.

III. Les principales lois traitant de la surveillance technique

A. La compétence législative

272 En Suisse, les cantons jouissent d'une compétence législative générale et la Confédération d'une compétence d'attribution : la Confédération n'est compétente pour légiférer que dans les domaines où la Constitution lui en donne la compétence (art. 3 Cst)[363]. En vertu de la primauté du droit fédéral (art. 49 Cst), l'entrée en vigueur de la législation adoptée par la Confédération dans ses domaines de compétence empêche les cantons d'adopter ou d'appliquer les règles contraires à la législation fédérale[364].

273 La surveillance technique en tant que telle n'est pas l'objet d'une compétence fédérale ou cantonale et il est nécessaire de rechercher dans quel but la surveillance est mise en place[365]. La Confédération est cependant compétente dans les domaines suivants : droit civil et procédure civile (art. 122 al. 1 Cst), droit pénal et procédure pénale (art. 123 al. 1 Cst), services postaux et télécommunications (art. 92 al. 1 Cst), utilisation du patrimoine génétique humain (art. 119 Cst), affaires étrangères (art. 54 Cst), douanes (art. 133 Cst).

274 La sécurité du pays et la protection de la population sont des compétences partagées entre la Confédération et les cantons. La sécurité extérieure revient plutôt à la Confédération, mais elle doit tenir compte des compétences cantonales (art. 54 al. 3 Cst. notamment), alors que la sécurité intérieure est une compétence cantonale puisque les cantons disposent d'un pouvoir primaire de

[363] BENOÎT, *Le partage vertical des compétences*, pp 13-17.

[364] Sauf si la Confédération ne dispose que d'une compétence limitée. Sur les notions de compétences législatives exclusives, concurrentes et limitées : AUBERT / MAHON, *Petit commentaire*, pp 387-388; BENOÎT, *Le partage vertical des compétences*, pp 27-36. Sur la répartition des compétences en général : AUBERT / MAHON, *Petit commentaire*, pp 30-31; AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse I*, pp 341-383; BIAGGINI, *BV Kommentar*; HALLER, *The Swiss Constitution*, pp 56-75; RAUBER, *Sicherheitspolizeiliche Aufgaben durch Private*, pp 127-139; RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*, pp 141-151; SCHWEIZER, *Art. 3 BV*.

[365] MÜLLER / WYSSMANN, *Rechtssetzungszuständigkeit*, pp 530-531 et 552.

police. La Confédération a cependant également des compétences en matière de sécurité intérieure[366]. En matière de violence sportive, la Confédération est compétente pour interdire aux auteurs de violence sportive de se rendre dans un pays et pour constituer une banque de données sur les hooligans. Les cantons sont en revanche compétents pour ce qui concerne l'interdiction de périmètre, la garde à vue et l'obligation de se présenter à la police[367].

En matière de protection des données, la compétence est partagée entre la Confédération et les cantons. La Confédération est compétente pour légiférer en droit pénal et en droit civil, ainsi qu'en matière d'organisation des autorités et de l'administration fédérale, alors que les cantons sont compétents en matière d'organisation des autorités et de l'administration cantonale[368]. 275

C'est à cause de cette répartition des compétences que la Loi fédérale sur la protection des données ne concerne que le traitement de données effectué par des particuliers et des organes fédéraux[369]. 276

[366] A propose de cet enchevêtrement de compétences : art. 4ss LMSI, AUBERT / MAHON, *Petit commentaire*, pp 480-482; BICHOVSKY, *Prévention de la violence commise par les spectateurs*, pp 264-268; *Message du CF concernant la LMSI*, pp 1139-1140 et 1202-1203; *Message du CF relatif à la violence lors de manifestations sportives*, pp 5293-5294 et 5310-5312; KELLER, *Die politische Polizei*, pp 169-171 et 466-469; RAUBER, *Sicherheitspolizeiliche Aufgaben durch Private*, pp 53-54; SAUER, *Das Recht der Vollzugspolizeien*, pp 54-76. Pour les compétences de la Confédération en matière de sécurité intérieure : OFJ, *Rapport relatif à la disposition constitutionnelle sur la violence dans le cadre des manifestations sportives*, pp 7-9.

[367] Les deux premières mesures figurent aux art. 24a et 24c LMSI, alors que les trois dernières ressortent du Concordat instituant des mesures contre la violence lors de manifestations sportives adopté par la Conférence des chefs des départements de justice et police le 15 novembre 2007 et entré en vigueur le 1er janvier 2010. Cette solution a été préférée à l'adoption du projet d'art. 68 al. 4 Cst, afin de préserver la souveraineté des cantons en matière de sécurité intérieure : BICHOVSKY, *Prévention de la violence commise par les spectateurs*, pp 266-268. La compétence législative était déjà donnée pour l'établissement de la banque de données HOOGAN par l'art. 57 al. 2 Cst. : BICHOVSKY, *Prévention de la violence commise par les spectateurs*, p. 266.

[368] *Message du CF concernant la LPD*, pp 432-433.

[369] FLÜCKIGER / AUER, *La vidéosurveillance dans l'œil de la constitution*, p. 925.

277 Les cantons sont donc compétents pour légiférer en matière de surveillance sur le domaine public et accessible au public lorsqu'elle ne tombe pas sous le champ d'une compétence fédérale[370]. Ainsi, l'installation de vidéosurveillance d'un grand magasin est réglée par le droit fédéral (droit civil), alors que celle qui est dans la rue menant à ce magasin est soumise au droit public cantonal.

278 Une délégation de la compétence législative est admissible. La Confédération peut confier des tâches spécifiques aux cantons, voire l'exécution de certaines lois fédérales. De même, un canton peut déléguer certaines compétences aux communes[371]. C'est particulièrement le cas pour les tâches policières, réparties entre le canton et les communes[372].

B. Les lois fédérales

1. Le Code fédéral de procédure pénale

279 L'unification de la procédure pénale a débuté en mai 1994 et a conduit à l'adoption du Code de procédure pénale suisse le 5 octobre 2007, dont l'entrée en vigueur est prévue le 1er janvier 2011[373]. Les 26 codes de procédure pénale cantonaux et la Loi sur la procédure pénale fédérale seront abrogés à cette date[374]. Subsisteront en revanche la Procédure pénale militaire du 23 mars 1979[375], la Loi fédérale sur le droit pénal administratif du 22 mars 1974[376], ainsi

[370] Notamment la vidéosurveillance si elle n'est pas installée dans le cadre d'une instruction pénale : FLÜCKIGER / AUER, *La vidéosurveillance dans l'œil de la constitution*, p. 926; RUEGG / FLÜCKIGER / NOVEMBER, *et al.*, *Vidéosurveillance et risques dans l'espace à usage public*, p. 47.

[371] Sur la délégation de compétence verticale en général : AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse I*, pp 361-363.

[372] RAUBER, *Sicherheitspolizeiliche Aufgaben durch Private*, pp 53-65.

[373] Code de procédure pénale (CPP).

[374] PPF, RO 50 709.

[375] PPM, RS 322.1.

[376] DPA, RS 313.0.

que les lois cantonales d'exécution du CPP et les lois d'organisation judiciaire cantonales et fédérales[377].

De nombreuses dispositions qui figuraient auparavant dans diverses lois ont été intégrées dans le CPP, notamment des dispositions du Concordat sur l'entraide judiciaire et la coopération intercantonale en matière pénale du 5 novembre 1992[378], de la Loi fédérale sur l'aide aux victimes d'infractions du 4 octobre 1991[379], de la Loi fédérale sur l'investigation secrète du 20 juin 2003[380], de la Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication[381], de la Loi fédérale sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues du 20 juin 2003 [382] ou encore du Code pénal[383]. 280

Les mesures techniques de surveillance obéissent désormais aux mêmes règles dans l'ensemble de la Suisse, ce qui n'était le cas précédemment que pour les mesures tombant sous le coup d'une loi fédérale comme la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT). Les autres mesures figuraient dans les codes cantonaux et étaient soumises à des règles parfois assez différentes. 281

Le CPP traite désormais de l'observation (art. 282 et 283), de la récolte des données signalétiques, des échantillons d'écriture ou de voix (art. 260 à 262), de l'analyse d'ADN (art. 255 à 259), de la surveillance de la correspondance par poste et télécommunication (art. 269 à 279), de la surveillance des relations bancaires (art. 284 et 285) et des autres dispositifs techniques de surveillance (art. 280 et 281). 282

[377] Sur les raisons qui ont conduit au maintien du CPM et du DPA : *Message du CF relatif à l'unification de la procédure pénale*, p. 1069. Les lois d'organisations judiciaires ont été entièrement révisées.
[378] RO 1993 2876.
[379] LAVI, RS 312.5.
[380] LFIS, RS 312.8.
[381] LSCPT, RS 780.1.
[382] Loi sur les profils d'ADN (LADN, RS 363).
[383] CP, RS 311.0.

2. La Loi fédérale sur la surveillance de la correspondance

283 La Loi fédérale sur la surveillance de la correspondance par poste et télécommunication du 6 octobre 2000 est entrée en vigueur le 1er janvier 2002[384]. Avec l'entrée en vigueur du CPP, les conditions auxquelles une surveillance peut être ordonnée ne figurent plus dans cette loi, mais dans le CPP, la Procédure pénale militaire[385] et la Loi sur l'entraide pénale internationale[386]. Pour les procédures précitées, la LSCPT régit l'exécution de la surveillance, plus particulièrement les tâches des opérateurs proposant des services postaux et des services de télécommunication, ainsi que le contrôle du service de surveillance de la correspondance par poste et télécommunication géré par la Confédération (Service SCPT rattaché administrativement au Centre de services informatiques du Département fédéral de justice et police CSI-DFJP).

284 Le Conseil fédéral a mis en consultation durant l'été 2010 un avant-projet de révision complète de la LSCPT, qui modifie également le CPP[387]. Si plusieurs adaptations sont bienvenues, il est regrettable que ces modifications n'aient pas eu lieu en même temps que la rédaction du CPP. L'avant-projet (AP LSCPT) prévoit une modification complète de la LSCPT au niveau formel puisque la numérotation des articles et la structure de la loi sont complètement revues. Sur le fond, il règle les communications par Internet, y compris la téléphonie en ligne. Il précise le cercle des personnes soumises à la LSCPT et leurs obligations, augmente le délai de conservation des données accessoires à 12 mois et prévoit un nouveau système de transmission électronique des résultats de surveillance. Finalement, cet avant-projet apporte quelques modifications au CPP par l'introduction de dispositions autorisant l'utilisation d'un logiciel

[384] LSCPT, RS 780.1. Avant l'introduction de la LSCPT, la surveillance de la correspondance téléphonique et postale était réglée par la Loi fédérale du 23 mars 1979 sur la protection de la vie privée (RO 1979 1170). Voir à ce sujet : VON BENTIVEGNI, *Les mesures officielles de surveillance*. Sur le développement de la réglementation en matière de surveillance téléphonique depuis 1922 : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 1-18. Sur la procédure d'adoption de la LSCPT, voir notamment : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 25-37; JEAN-RICHARD-DIT-BRESSEL, *Ist ein Millionendiebstahl ein Bagatelldelikt*, pp 41-43.

[385] PPM, RS 322.1.

[386] Loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP, RS 351.1).

[387] *AP LSCPT*; *Rapport du CF relatif à l'AP LSCPT*.

espion dans un ordinateur objet de la surveillance ou de l'IMSI-Catcher[388]. L'AP LSCPT prévoit de s'appliquer également aux surveillances en cours à son entrée en vigueur, ce qui est évidemment contraire aux exigences de la CEDH et de la Constitution en matière de base légale et de prévisibilité[389].

D'autre part, le projet de Loi fédérale sur le programme de consolidation 2011-2013 (LPCO) mis en consultation en avril 2010 par le Conseil fédéral prévoit la suppression de l'indemnisation des personnes qui exécutent des surveillances en vertu de la LSCPT (abrogation de l'actuel art. 16 LSCPT)[390]. Les arguments mentionnés (intérêts des fournisseurs de service à ce qu'aucune infraction ne soit commise et devoir d'édition) ne résistent pas à un examen sérieux et semblent bien plus répondre à une volonté de réaliser des économies qu'à une motivation juridique. Au contraire, il paraît juste que celui qui doit produire des documents ou mettre en place une surveillance soit indemnisé, comme doit également l'être un témoin ou un expert. L'art. 434 CPP prévoit expressément l'indemnisation des tiers qui ont subi un dommage du fait de l'aide apportée aux autorités pénales. Ces frais font partie des frais de procédure, qui seront *in fine* à charge du condamné (art. 422ss CPP). 285

3. La Loi sur les profils d'ADN

La Loi fédérale sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues du 20 juin 2003 est entrée en vigueur le 1er janvier 2005[391]. Elle a remplacé l'Ordonnance du Conseil fédéral sur le système d'information fondé sur les profils d'ADN[392]. 286

[388] Art. 270bis et 270ter CPP. Ces modifications seront mentionnées lorsque ces méthodes sont abordées plus loin.

[389] Art. 37 AP LSCPT et *Rapport du CF relatif à l'AP LSCPT*, p. 48. Sur la prévisibilité de la surveillance, voir le chapitre 2. La prévisibilité de la surveillance, p. 118 ci-dessus.

[390] *Rapport du CF relatif à l'AP LSCPT*, pp 11-11 et 37-38; *Rapport du CF sur le programme de consolidation 2011-2013 des finances fédérales*, pp 124-125. Les prestations offertes par le Service chargé de la surveillance de la correspondance par poste et télécommunication (en l'occurrence le CSI-DFJP) ne sont pas concernées et continueraient d'être facturées aux cantons.

[391] Loi sur les profils d'ADN (LADN, RS 363).

[392] Ordonnance ADNS, RO 2000 1715.

287 La Loi sur les profils d'ADN règle de manière générale l'organisation des analyses et les modalités concernant la saisie des profils. C'est également cette loi qui précise les conditions auxquelles des profils d'ADN peuvent être établis dans le cadre de procédures pénales militaires, de procédures pénales administratives et en dehors de procédures pénales, lorsqu'il s'agit d'identifier par le recours à la comparaison de profils d'ADN des personnes inconnues, disparues ou décédées[393].

4. La Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI)

288 La Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure du 21 mars 1997 est entrée en vigueur le 1er juillet 1998[394]. Elle est complétée par la Loi fédérale du 3 octobre 2008 sur le renseignement civil entrée en vigueur le 1er janvier 2010[395] et plusieurs ordonnances du Conseil fédéral, parmi lesquelles l'Ordonnance du 4 décembre 2009 sur le Service de renseignement de la Confédération[396], l'Ordonnance du 19 décembre 2001 sur les contrôles de sécurité relatifs aux personnes[397], et l'Ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale[398].

289 La LMSI donne mandat à la Confédération de prendre les mesures préventives nécessaires pour détecter précocement les dangers liés à la sécurité intérieure et extérieure. Elle permet notamment la recherche d'information. Un projet de révision de la loi a été renvoyé au Conseil fédéral par le parlement au printemps 2009[399]. D'ici quelques années, la LMSI devrait être remplacée par la Loi sur le service de renseignement de la Confédération (Loi sur le SRC) dont les premiers projets semblent être en cours d'élaboration au sein de l'administration.

[393] *Message du CF relatif à l'unification de la procédure pénale*, pp 1328-1329.
[394] LMSI, RS 120. Sur l'évolution historique de la sûreté intérieure en Suisse : MÜLLER, *Innere Sicherheit Schweiz.*
[395] LFRC, RS 121.
[396] OSRC, RS 121.1.
[397] OCSP, RS 120.4.
[398] OSF, RS 120.72.
[399] BO 2009 N 672-676.

5. La Loi sur les systèmes d'information et de police

La Loi fédérale sur les systèmes d'information de police de la Confédération du 13 juin 2008 est entrée en vigueur le 5 décembre 2008[400]. C'est la base légale des systèmes policiers RIPOL (recherches informatisées de police), IPAS (données relatives aux personnes ayant fait l'objet d'un traitement signalétique ou d'une communication Interpol) et JANUS (données de la Police judiciaire fédérale traitées dans le cadre de procédures d'enquêtes ou d'investigations préliminaires en tant qu'Offices centraux de police criminelle), ainsi que de l'index national de police (répertoire qui rassemble les noms des personnes enregistrées dans les diverses bases de données de police)[401]. 290

6. Le Code pénal

Le Code pénal suisse est entré en vigueur le 1er janvier 1942[402]. Les art. 179ss CP, introduits le 1er mai 1969, visent les infractions contre le domaine secret ou le domaine privé. Quant à l'art. 321ter CP, il sanctionne la violation du secret des postes et des télécommunications. L'art. 179octies CP déclare non punissable l'auteur d'une violation du secret de fonction (par renvoi de l'art. 321ter al. 5 CP) ou d'une infraction contre le domaine secret ou privé, si l'autorisation du juge compétent a été demandée[403]. C'est donc bien un cas particulier d'acte licite au sens de l'art. 14 CP, mais en aucun cas une base légale suffisante telle qu'exigée par la Constitution et la CEDH pour restreindre des libertés fondamentales. Le fait que l'auteur de la surveillance ne puisse être puni pénalement est à distinguer de la légalité de la surveillance et de la légalité de l'utilisation des résultats obtenus[404]. 291

[400] LSIP, RS 361.

[401] *Message du CF relatif aux systèmes d'information de police*.

[402] CP, RS 311.0.

[403] Le second alinéa renvoie aux conditions et à la procédure prévues par la LSCPT. Si cela est conforme jusqu'à l'entrée en vigueur du CPP, cet article devrait être modifié puisque la LSCPT ne concernera plus que l'exécution de la surveillance. Le juge appelé à appliquer cette disposition considérera vraisemblablement qu'il s'agit d'une lacune et remplacera les dispositions (abrogées) de la LSCPT auxquelles il est renvoyé par celles (nouvelles) du CPP.

[404] Sur les art. 179ss CP : AEBI-MÜLLER / EICKER / VERDE, *Verfolgung von Versicherungsmissbrauch mittels Observation*, ch. 84-110; BAUM, *Der kriminalpräventive Einsatz von Videoüberwachungsanlagen*; CORBOZ, *Les infractions en droit suisse I*, pp 588-641; DUBUIS, *Note sur les mesures de surveillance optique par caméra*, pp 207-208;

7. La Loi fédérale sur la protection des données

292 La Loi fédérale sur la protection des données du 19 juin 1992 est entrée en vigueur le 1er janvier 1993[405]. Elle concrétise la protection constitutionnelle de l'art. 13 al. 2 Cst.[406]. Elle est parfois complétée par des directives ou recommandations du Préposé fédéral à la protection des données et à la transparence (PFPDT)[407]. Les recommandations concernent un cas d'espèce[408], alors que les directives sont plus générales. Elles sont établies sous la forme de brochures[409] ou de feuillets thématiques[410]. L'art. 2 al. 2 lit. c prévoit qu'elle ne s'applique pas aux procédures pendantes civiles, pénales, d'entraide judiciaire internationale ainsi que de droit public et de droit administratif, à l'exception des procédures administratives de première instance. Si les activités de la police et de la justice durant une procédure pénale sont exclues du champ d'application de la LPD, il n'en va pas de même des recherches que la police ferait de manière préventive, avant même l'ouverture de la procédure pénale[411].

GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 12-18 et 79-84; LEGLER, *Vie privée, image volée*, pp 212-223; MÉTILLE, *L'utilisation privée de moyens techniques de surveillance*; RUEGG / FLÜCKIGER / NOVEMBER, *et al.*, *Vidéosurveillance et risques dans l'espace à usage public*, pp 41-46; VON BENTIVEGNI, *Les mesures officielles de surveillance*, pp 12-13.

405 LPD, RS 235.1.

406 Sur l'application de la LPD en matière de vidéosurveillance : BAUM, *Der kriminalpräventive Einsatz von Videoüberwachungsanlagen*. De manière plus générale : BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 161-170. Sur la protection des données et les informations recueillies par la police : GISLER, *La coopération policière*, pp 79-87.

407 Elles sont consultables sur le site du PFPDT à l'adresse : http://www.edoeb.admin.ch/dokumentation.

408 Par exemple la Recommandation du 18 février 2009 concernant une caméra de surveillance installée dans le chalet SJ.

409 Par exemple : PFPDT, *Surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail*; PFPDT, *Systèmes de reconnaissance biométrique*.

410 PFPDT, *Vidéosurveillance effectuée par des personnes privées*.

411 RUDIN, *Auf der Suche nach dem "Bodensatz"*, p. 278. Sur la notion de procédure pendante de l'art. 2 al. 2 LPD : ATAF A-3144/2008, PFPDT c. Logistep AG, du 27 mai 2009, consid. 3.2 et les réf. citées, ainsi que RHYNER, *Kommentar zu Art. 95-99 StPO*, pp 139-140.

Les art. 95 à 99 CPP ont cependant repris l'essentiel des garanties de la LPD[412]. L'art. 95 al. 2 CPP prévoit en particulier que si des données personnelles sont collectées à l'insu de la personne concernée, celle-ci doit en être informée sans délai. L'autorité peut toutefois renoncer à cette information ou l'ajourner si un intérêt public ou privé prépondérant l'exige. 293

8. La Loi sur les douanes

La Loi sur les douanes du 18 mars 2005 est entrée en vigueur le 1er mai 2007[413]. Son art. 108 permet l'utilisation d'appareils automatiques de prise de vue et de relevé, ainsi que d'autres appareils de surveillance. Les détails sont réglés par l'Ordonnance du Conseil fédéral du 4 avril 2007 régissant l'utilisation d'appareils de prises de vue, de relevé et d'autres appareils de surveillance par l'Administration fédérale des douanes[414]. 294

9. La Loi sur le transport des voyageurs et la Loi sur les chemins de fer

L'Ordonnance du Conseil fédéral du 4 novembre 2009 sur la vidéosurveillance dans les transports publics régit la surveillance par caméra vidéo des véhicules, des ouvrages, des installations et des équipements des entreprises de transports publics[415]. Cette Ordonnance est entrée en vigueur le 1er janvier 2010. Elle est basée sur l'art. 55 de la Loi fédérale sur le transport de voyageurs du 20 mars 2009[416] et l'art. 16b de la Loi fédérale sur les chemins de fer du 20 décembre 1957[417]. 295

[412] RHYNER, *Kommentar zu Art. 95-99 StPO*, pp 149-154. Il s'agit de normes fondamentales devant compléter les prescriptions de détails qui assurent déjà la protection des intérêts des prévenus : *Message du CF relatif à l'unification de la procédure pénale*, pp 1136-1139.

[413] LD, RS 631.0.

[414] RS 631.053. Voir aussi sur la question de la vidéosurveillance des frontières : OFJ, *Avis du 15 juin 1993*.

[415] Ordonnance du 4 novembre 2009 sur la vidéosurveillance dans les transports publics (OVid-TP, RS 742.147.2).

[416] LTV, RS 745.1.

[417] LCdF, RS 742.101.

10. La Loi sur l'aviation

296 La Loi fédérale sur l'aviation du 21 décembre 1948 est entrée en vigueur le 15 juin 1950[418]. Son article 12 al. 1 et les art. 122a ss de l'Ordonnance sur l'aviation du 14 novembre 1973[419] servent de base légale aux mesures de sécurité déployées dans les aéroports. Il s'agit d'une reprise des dispositions de sécurité édictées par l'Organisation de l'aviation civile internationale (OACI). Le détail de ces mesures de sécurité est inscrit dans l'Ordonnance du DETEC sur les mesures de sûreté dans l'aviation du 31 mars 1993[420].

11. La Loi sur les maisons de jeu

297 La Loi fédérale sur les jeux de hasard et les maisons de jeu du 18 décembre 1998 oblige les maisons de jeu à prendre des mesures de sécurité[421]. Le Conseil fédéral a adopté le 24 septembre 2004 une Ordonnance sur les jeux de hasard et les maisons de jeu[422]. Cette ordonnance impose aux maisons de jeu de procéder à des contrôles d'identité, d'enregistrer certaines données et d'installer un système de vidéosurveillance[423].

12. La Loi sur les étrangers

298 La Loi fédérale sur les étrangers du 16 décembre 2005 est entrée en vigueur le 1er janvier 2008[424]. Ses art. 102ss, complétés par les art. 45ss de l'Ordonnance du 22 octobre 2008 sur l'entrée et l'octroi de visas[425] permettent l'utilisation d'un système de reconnaissance biométrique des visages notamment le système FAREC à l'aéroport de Zurich[426].

[418] LA, RS 748.0.
[419] OSAv, RS 748.01.
[420] OMSA, RS 748.122.
[421] Loi sur les maisons de jeu (LMJ, RS 935.52)
[422] Ordonnance sur les maisons de jeu (OLMJ, RS 935.521)
[423] Art. 28 à 36 OLMJ.
[424] LEtr., RS 142.20.
[425] OEV, RS 142.204.
[426] Face Recognition : DFJP, *Rapport sur la vidéosurveillance*, p. 17.

13. Les autres lois fédérales

299 On citera encore la Loi fédérale sur l'investigation secrète du 20 juin 2003, entrée en vigueur le 1er janvier 2005, qui règle les conditions d'engagement des agents infiltrés[427], la Loi fédérale sur l'armée et l'administration militaire du 3 février 1995, entrée en vigueur le 1er janvier 1996, qui vise la recherche d'informations sur l'étranger qui sont importantes pour l'armée[428], ainsi que la Loi fédérale sur les télécommunications du 30 avril 1997, entrée en vigueur le 20 octobre 1997[429]. Cette dernière prévoit une surveillance dans un but de contrôle technique des fréquences (art. 26 LTC), ainsi qu'une compétence du Conseil fédéral d'ordonner la surveillance des télécommunications lors de situations extraordinaires qui nécessitent l'engagement de l'armée, de la protection civile, de la police, des services de protection et de sauvetage ainsi que des états-majors civils de conduite (art. 47s LTC)[430].

C. Les lois cantonales

300 La compétence législative en matière civile et pénale étant donnée à la Confédération, il ne reste guère de place pour une législation cantonale, mis à part les questions de sécurité publique et de protection des données qui n'entrent pas dans le champ de la législation fédérale. La législation cantonale n'a alors pas tellement pour objectif d'imposer un cadre à la surveillance effectuée par les individus, mais bien plus de servir de base légale pour la surveillance publique qui ne remplit pas un des objectifs fixés par une des lois fédérales précitées.

301 En effet, pour les cas de figure qui ne sont pas régis par une loi fédérale, une base légale cantonale est nécessaire pour permettre à l'Etat de mettre en place

[427] LFIS, RS 312.8. Sur ce sujet, voir : BAUMGARTNER, *Zum V-Mann-Einsatz*; BÉNÉDICT, *Le sort des preuves illégales*, pp 157-182; HANSJAKOB, *Das neue BVE*; JOSET / RUCKSTUHL, *V-Mann-Problematik*; PIQUEREZ, *Traité*, pp 629-634; WOHLERS, *Revue de droit suisse*.

[428] LAAM, RS 510.10. Il s'agit en particulier de l'art. 99 et de ses dispositions d'exécution. Sur ce sujet, voir : BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 522-527.

[429] LTC, RS 784.10.

[430] Sur la surveillance en cas de crise : BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, p. 527. Sur la surveillance dans un but de contrôle technique des fréquences et de recherche des perturbations : BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 529-530.

une mesure de surveillance. Jusqu'à l'entrée en vigueur du CPP, les autres mesures de surveillance (soit celles qui n'étaient pas prévues par la LSCPT) doivent avoir une base légale dans le droit de procédure cantonal[431]. Cela n'était souvent pas le cas, mais la question sera désormais résolue par le CPP[432].

302 Les collectivités cantonales et communales ne disposent pas encore toutes d'une base légale formelle permettant de mettre en place des mesures de surveillance, le plus souvent des mesures de vidéosurveillance dissuasive. Les bases légales existantes sont de qualités très inégales, allant d'une simple clause générale contenue dans une loi régissant l'activité de la police ou consacrée à la protection des données, à une réglementation bien plus complète[433]. Pour les autres collectivités ne disposant pas d'une base légale suffisante, les mesures de surveillance installées sont tout bonnement illégales[434].

303 A titre d'exemple[435], on peut citer pour le canton de Neuchâtel l'art. 58 de la Loi sur la police neuchâteloise du 20 février 2007[436], pour le canton de Bâle-Ville l'art. 6a de la Loi sur la protection des données du 18 mars 1992[437], pour le canton de Vaud les art. 22s de la Loi sur la protection des données personnelles

[431] Pour un exemple de la répartition des compétences cantonales entre le canton de Berne et les communes bernoises : MÜLLER / WYSSMANN, *Rechtssetzungszuständigkeit*.

[432] Sous l'ancien droit : VON BENTIVEGNI, *Les mesures officielles de surveillance*, pp 18-19.

[433] DFJP, *Rapport sur la vidéosurveillance*, pp 20-21, 26 et 29.

[434] Pour un exemple à Genève : FAVRE / DSIC, *Rapport à l'attention du Conseil administratif*, p. 24; GANI, *Sans cadre légal, 120 caméras surveillent déjà la ville de Genève*. L'art. 42 de la Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD, RSG A 2 08) a été révisé le 1er janvier 2010 et constitue désormais une base légale suffisante. Voir également à Neuchâtel où les systèmes de vidéosurveillance utilisés dans le canton ne reposent pas sur une base légale suffisante. Un projet d'introduction des art. 25a ss dans la Loi cantonale sur la protection des données existe et devrait régulariser la situation s'il est adopté, mais il pourrait aussi être remplacé par une convention intercantonale avec le Jura en matière de protection des données et de surveillance actuellement en discussion. Le législateur relevait alors que « certes, la plupart des autorités qui recourent à la vidéosurveillance s'approchent du président de l'Autorité de surveillance en matière de protection de la personnalité, laquelle leur prodigue aide et conseils, mais cela ne suffit pas à pallier le manque de bases légales formelles que requiert ce type d'installations » : CONSEIL D'ETAT NEUCHÂTELOIS, *Rapport vidéosurveillance*, p. 2.

[435] Pour un panorama plus complet : FLÜCKIGER, *Droits fondamentaux et vidéosurveillance*, note de bas de page n° 83.

[436] LPol, RSN 561.1, qui devrait être complété par les art. 25a ss de la Loi sur la protection des données du 30 septembre 2008 ou une convention intercantonale.

[437] Gesetz über den Schutz von Personendaten, RSBS 153.260.

du 11 septembre 2007[438], les art. 9s du Règlement d'application de la Loi sur la protection des données personnelles du 29 octobre 2008[439] et l'art. 2 al. 1er lit. b de la Loi d'application du concordat instituant des mesures contre la violence lors de manifestations sportives du 17 novembre 2009[440], pour le canton de Berne les art. 51ss de la Loi sur la police du 8 juin 1997[441] et l'Ordonnance du 29 avril 2009 sur l'utilisation d'appareils de vidéosurveillance lors de manifestations de masse et dans les lieux publics[442] et pour le canton de Genève l'art. 42 de la Loi du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles[443] et l'art. 6 al. 4 et 5 de la Loi du 26 juin 2008 sur les manifestations sur le domaine public[444].

D. Les standards ETSI et les normes techniques

304 Les aspects techniques en matière de surveillance des télécommunications sont réglés au niveau international par les standards ETSI[445] et en Suisse par des normes techniques (Operational and Administrative Requirements OAR et Technical Requirements TR) éditées par le Département fédéral de justice et police[446]. L'autorité suisse reprend de plus en plus les standards ETSI, ce qui facilite également la tâche des opérateurs téléphoniques qui n'ont plus à développer des applications particulières pour la Suisse.

[438] LPr, RSVD 172.65.

[439] RSVD 172.65.1.

[440] RSVD 125.15.

[441] Lpol, RSB 551.1.

[442] OVid, RSB 551.332.

[443] LIPAD, RSG A 2 08.

[444] LMDPu RSG F 3 10.

[445] L'Institut européen des normes de télécommunication (European Telecommunications Standards Institute, ETSI) est un organisme de normalisation reconnu par l'Union européenne dans le domaine des télécommunications.

[446] Alors que les normes suisses ne sont pas publiques, les standards ETSI sont librement accessibles sur le site de l'Institut : http://www.etsi.org/WebSite/Standards/Standard.aspx. Microsoft a présenté de manière claire les informations que cette société est à même de livrer sur demande judiciaire dans un document intitulé « Microsoft® Online Services Global Criminal Compliance Handbook » : http://cryptome.org/isp-spy/microsoft-spy.zip ou http://www.scribd.com/doc/27394899/Microsoft-Spy. La Loi fédérale sur le principe de la transparence dans l'administration, et l'exigence posée par la CEDH d'une loi accessible, permettent d'obtenir les normes suisses OAR et TR. Il faut toutefois déposer une requête, dont l'expérience a montré qu'elle risque d'être rejetée si elle n'est pas motivée (alors même que la loi n'exige pas de motivation à la requête).

IV. Synthèse et critique

A. Les libertés

305 Les garanties offertes par les droits fondamentaux en général et les libertés individuelles en particulier sont suffisantes pour les situations envisagées dans la présente étude. Énoncées en termes généraux, ces normes permettent de couvrir tous les cas de figure et sont judicieusement complétées par la jurisprudence et les lois nationales. La Convention européenne des droits de l'Homme (CEDH) apporte quelques éléments supplémentaires aux garanties offertes par la Constitution fédérale. Il faut souligner que la jurisprudence de la Cour européenne des droits de l'Homme se distingue souvent par une interprétation autonome et dynamique des notions qu'elle protège. L'application de la CEDH pouvant être contrôlée par un organe supérieur et international, son application en Suisse, voire celle de la Constitution[447], sont évidemment influencées par la jurisprudence de Strasbourg. D'autre part, la Cour ayant à traiter des affaires émanant de l'ensemble des pays membres, sa jurisprudence apporte aussi la réponse à des cas qui ne se sont pas encore produits en Suisse, ou qui n'auraient pas été l'objet d'un recours jusque devant le Tribunal fédéral. Lorsque la Cour condamne un pays, cela conduit souvent ce dernier à modifier sa législation interne[448].

306 Les conditions de restrictions aux droits fondamentaux, similaires qu'il s'agisse de la CEDH ou de la Constitution, permettent aussi une adaptation à chaque situation individuelle de manière raisonnable. L'exigence de la base légale permettant de restreindre une liberté fondamentale a conduit à l'élaboration de nombreuses lois. Elles ne sont pas seulement la condition formelle pour une atteinte à la Constitution. Elles sont bien plus un moyen pour le législateur de décider ce qu'il accepte ou non (dans le respect toujours des normes supérieures) et de permettre ainsi une véritable discussion lors de l'adoption de

[447] Singulièrement lorsque l'on est hors du champ d'application de la CEDH, mais que la protection offerte par la Constitution est la même. Dans ce cas le Tribunal fédéral reprend spontanément la jurisprudence de la Cour. Pour un exemple : ATF 133 I 100, 104, A. et consorts, du 11 janvier 2007, consid. 4.6.

[448] Pour des exemples en matière d'écoutes téléphoniques : RUEDIN, *Exécution des arrêts de la Cour européenne des droits de l'homme*, pp 294-295.

la loi. Ensuite, cette loi sert de cadre aux opérations policières et judiciaires. Elle permet aussi à l'individu de savoir ce qui est permis et ce qui ne l'est pas, pour ensuite pouvoir défendre ses droits correctement.

307 L'exigence de la base légale est particulièrement bénéfique puisqu'elle oblige le législateur à codifier, sous la forme d'une loi, les restrictions possibles des droits individuels avec une certaine précision. Même si le législateur est conscient des exigences constitutionnelles, il est nécessaire d'avoir des normes précises et directes : le policier, le procureur ou l'individu concerné ne va pas commencer par déduire ses droits et obligations en fonction de normes de droit supérieur, mais en suivant la loi qui s'applique à son domaine dans l'hypothèse à laquelle il est confronté. Dans un deuxième temps, lorsqu'une autorité judiciaire statue par exemple sur un recours, on peut s'attendre à ce que les questions constitutionnelles soient examinées. Mais précédemment, et même si toute autorité ou organe peut, voire doit, effectuer un contrôle concret de la constitutionnalité des règles qu'il applique, il faut rester conscient des possibilités et des limites de chacun. Sans remettre en cause les compétences d'un policier, on peut imaginer que lorsque celui-ci procède sur le terrain à une arrestation ou une perquisition, il va agir dans le respect des prescriptions de service et des dispositions légales qu'il connaît. On ne peut guère exiger de lui qu'il vérifie si les prescriptions de service sont couvertes par des dispositions légales, elles-mêmes conformes aux exigences constitutionnelles et conventionnelles. Cela ne signifie en revanche pas qu'un agent de police doit suivre aveuglément une règle sans se poser la moindre question. Les exigences de remises en cause de la conformité d'une norme qu'il applique sont simplement moins grandes que pour une autorité judiciaire précisément chargée d'un tel contrôle.

308 La surveillance secrète des communications est admise depuis longtemps par les plus hautes autorités judiciaires et l'évolution de la technique y a ajouté de nouvelles mesures de surveillance. Elles ne sont néanmoins admises qu'en présence de garanties suffisantes. Ainsi la procédure et les conditions de surveillance doivent figurer dans une loi et être connues avant le début de la surveillance, de même qu'un contrôle judiciaire doit être prévu. Un droit d'accès suffisant doit aussi être prévu. Finalement, une surveillance générale et préventive est interdite, de même que l'utilisation de mesures de surveillance

dans un but autre que celui pour lequel elles sont initialement prévues et autorisées.

B. Les bases légales

309 Au niveau fédéral, il y a essentiellement deux grandes bases légales permettant des mesures de surveillance : le Code de procédure pénale (CPP) et la Loi instituant des mesures visant au maintien de la sûreté intérieure (LMSI). On trouve encore quelques autres lois fédérales liées à la création et l'exploitation de bases de données. Au niveau cantonal et communal figurent, ou devraient figurer, les bases légales permettant notamment la surveillance dissuasive des espaces publics. Il se justifie de traiter dans des lois différentes ces mesures de surveillance appliquées à des situations différentes. Indépendamment de la question de la compétence législative, la situation de la personne surveillée n'est pas la même par rapport à l'Etat. Le fait qu'il y ait plusieurs textes de lois n'empêche pas non plus, par renvoi par exemple, d'avoir des procédures ou des organes de contrôle semblables ou identiques.

310 Le CPP s'applique à la surveillance utilisée dans le cade de l'instruction pénale. Cette réglementation est assez complète et respecte les exigences de droit supérieur. Le principal reproche qui peut être fait au législateur tient plutôt de la méthode. Comme un code de procédure fédéral devait être complètement rédigé, c'eût été l'occasion de régler de manière claire et uniforme toutes les mesures de surveillance, plutôt que de reprendre pour l'essentiel les règles éparses et diverses qui existaient déjà auparavant, ce qui a conduit à des difficultés sur lesquelles nous reviendrons plus loin. La procédure pénale permettant les mesures de surveillance portant le plus atteinte à la sphère privée et aux autres droits fondamentaux, une réglementation précise s'imposait. Cela permet aussi aux différents intervenants d'agir avec transparence et une bonne compréhension du système, des limites et des droits de chacun.

311 En ce qui concerne la surveillance préventive régie par la LMSI et les bases de données qui en résultent, les choses sont plus opaques. Certes les notions comme celles de sûreté intérieure ne permettent pas de tout divulguer, il n'empêche que les difficultés à obtenir parfois de simples directives ou précisions législatives laissent croire que tout n'est pas avouable. Des décalages semblent aussi exister, au moins dans la terminologie, entre ce que la loi prévoit

et ce qui est réellement utilisé. Les droits d'accès pour la personne concernée sont également bien plus compliqués dans cette matière qu'en cas de surveillance liée à une procédure pénale, sans qu'il y ait toujours de raison à cela. La personne visée par la surveillance n'ayant commis en principe aucun acte pénalement répréhensible, il devrait y avoir à un cadre légal plus strict et transparent que le CPP. La situation reste cependant acceptable, puisque les mesures de surveillance actuellement autorisées sont limitées.

312 Les conditions juridiques permettant une mise sous surveillance étaient initialement extrêmement souples et assez peu encadrées. L'entrée en vigueur de la Loi fédérale du 23 mars 1979 sur la protection de la vie privée, remplacée le 1er janvier 2002 par la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication a marqué un changement. Cette évolution a été confirmée ensuite avec l'adoption du CPP. S'il reprend le système en vigueur en matière de surveillance de la correspondance par poste et télécommunication, il intègre également les autres dispositifs techniques de surveillance dont l'utilisation était réglée au niveau cantonal, souvent de manière assez peu contraignante. Finalement, le CPP soumet également l'observation à certaines conditions et autorisations. Cela constitue donc une clarification, mais également une restriction des conditions de surveillance[449]. Les oppositions rencontrées par le projet LMSI II confirment également cette tendance. Les autorités policières et judiciaires ne sont pas pour autant démunies dans leurs actes quotidiens. Elles doivent simplement respecter un cadre juridique clair, où les droits et libertés du citoyen sont mieux pris en compte.

313 Au niveau de la surveillance dissuasive des espaces publics, qui est de la compétence cantonale ou communale, la situation est inquiétante car très peu de lois sont en vigueur ou simplement appliquées correctement. Qu'il existe un grand nombre de caméras déjà en fonction ne justifie pas de continuer à tolérer une réglementation lacunaire. Au niveau de la surveillance opérée sur le domaine privé, les normes légales existent (en particulier la LPD et le Code pénal), mais c'est ici plutôt la bonne application de la loi et les moyens de contrôle qui sont déficients. Ces problèmes dépassent toutefois largement le cadre de la présente étude.

[449] RIKLIN, *Vollzugsdefizite noch und noch*, p. 18.

Troisième partie :
la surveillance répressive (selon le CPP)

I. Remarques préliminaires

Les mesures de surveillance répressive, soit celles ordonnées dans le cadre de l'instruction pénale, reposent sur le Code de procédure pénale (CPP) et font suite à la commission d'une infraction. Nous examinerons donc quelles mesures peuvent être ordonnées, par quelle autorité et à quelles conditions. 314

Après l'exécution de la surveillance se posent les questions liées à l'information, aux procédures de contrôle et au sort des données obtenues. Les découvertes fortuites et les preuves illégales seront également traitées, ainsi que la question de l'indemnisation en cas de surveillance illégale. 315

II. Exposé de la surveillance prévue par le CPP

A. Les mesures de surveillance

1. En général

316 Le titre 5 du CPP est consacré aux mesures de contrainte[450], soit les actes de procédure des autorités pénales qui portent atteinte aux droits fondamentaux des personnes intéressées, et qui servent à mettre les preuves en sûreté, ou à assurer la présence de certaines personnes durant la procédure ou encore à garantir l'exécution de la décision finale (art. 196 CP)[451].

317 Le chapitre 8 du titre 5 concerne les mesures de surveillance secrètes, soit la surveillance de la correspondance par poste et télécommunication (section 1), les autres dispositifs techniques de surveillance (section 2), l'observation (section 3), la surveillance des relations bancaires (section 4) et l'investigation secrète (section 5)[452].

318 Quelques mesures de surveillance ne font pas partie du titre consacré aux mesures de surveillance secrètes, mais sont régies ailleurs dans le chapitre consacré aux mesures de contrainte. Il s'agit de la recherche de personnes (art. 210), de l'analyse d'ADN (art. 255 à 259), de la récolte de données

[450] Sur les mesures de contrainte en général et le CPP : HANSJAKOB, *Zwangsmassnahmen in der neuen Eidg. StPO*; RIGHETTI, *Kommentar zu Art. 196-240 StPO*, pp 185-188.

[451] La notion de mise en sûreté des preuves doit vraisemblablement être comprise dans un sens très large, puisque les mesures de surveillance techniques, comme l'instruction dans son ensemble, visent également à la découverte de preuves et non seulement à la mise en sûreté de preuves déjà recueillies.

[452] Sur la vidéosurveillance (policière et privée) en droit autrichien : KÖNIG, *Videoüberwachung*. Sur la surveillance en droit allemand : BARTSCH, *Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen*; BAUSCH, *Videoüberwachung*; GEIGER, *Verfassungsfragen zur polizeilichen Video-Überwachung*; LÜTZNER, *Strafprozessuale Zwangs- und Überwachungsmassnahmen*. Sur la surveillance en droit français : BAUSCH, *Videoüberwachung*. Sur la surveillance en droit américain : ARZT, *Polizeiliche Überwachungsmassnahmen in den USA*; BARTSCH, *Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen*; LÜTZNER, *Strafprozessuale Zwangs- und Überwachungsmassnahmen*. Et pour une comparaison entre les droits allemand et américain : SCHWARTZ, *German and U.S. Telecommunications Privacy Law*.

signalétiques (art. 260 à 261), ainsi que de la récolte d'échantillons d'écriture ou de voix (art. 262).

L'élément distinctif de la mesure de contrainte se trouve dans l'atteinte qu'elle porte aux droits fondamentaux[453]. Ainsi, l'art. 197 CPP reprend les conditions de l'art. 36 Cst. et rappelle que des mesures de contrainte ne peuvent être prises que si elles sont prévues par la loi, si des soupçons suffisants laissent présumer une infraction, si les buts poursuivis ne peuvent pas être atteints par des mesures moins sévères et finalement si elles apparaissent justifiées au regard de la gravité de l'infraction. Le second alinéa précise encore que les mesures qui portent atteinte aux droits fondamentaux des personnes qui n'ont pas le statut de prévenu doivent être appliquées avec une retenue particulière. 319

2. Les mesures de surveillance secrètes

a) La surveillance de la correspondance par poste et télécommunication

La surveillance de la correspondance par poste et télécommunication n'est définie ni par la LSCPT, ni par le CPP, qui se contente de mentionner que peuvent faire l'objet d'une surveillance l'adresse postale et le raccordement de télécommunication du prévenu et à certaines conditions d'un tiers, ainsi que les données relatives au trafic et à la facturation. Il s'agit des mesures qui étaient ordonnées précédemment sur la base de la LSCPT. 320

Si la notion d'adresse postale n'appelle pas de commentaire, la notion de correspondance par télécommunication doit être précisée. Il s'agit de l'émission ou la réception d'informations transmises par le truchement d'installations de télécommunication, soit d'appareils, lignes ou équipements destinés à transmettre des informations au moyen de techniques de télécommunication ou utilisés à cette fin. Ces informations peuvent prendre la forme de signes, signaux, caractères d'écriture, images, sons ou de données, transmis entre des installations d'usagers fixes ou mobiles[454]. 321

[453] *Message du CF relatif à l'unification de la procédure pénale*, p. 1196.

[454] Art. 3 de la Loi sur les télécommunications (LTC, RS 784.10), STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 101-102.

322 Le CPP ne se limite cependant plus aux fournisseurs de services postaux soumis à concession[455]. L'art. 1 al. 2 LSCPT n'est formellement pas modifié par le CPP, ce qui signifie que la LSCPT s'applique seulement aux organismes étatiques, aux organismes soumis à concession ou à l'obligation d'annoncer, qui fournissent des services postaux ou de télécommunication ainsi qu'aux fournisseurs d'accès à Internet. Les art. 269ss CPP ne reprennent en revanche pas cette restriction. Seules les obligations des fournisseurs de services postaux (art. 12 LSCPT) ne s'appliquent pas directement aux entreprises qui ne tomberaient pas sous l'art. 1 al. 2 LSCPT. Le Tribunal fédéral a de plus retenu que l'obligation de conserver durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation s'appliquaient également à l'hébergeur d'un site Internet. Il a assimilé l'hébergeur à un fournisseur d'accès[456].

323 L'avant-projet de révision de la LSCPT modifierait le champ d'application de la loi. Elle permettrait d'obtenir des données de personnes qui ne sont actuellement pas soumises à la LSCPT, comme les services libres postaux[457], les fournisseurs d'hébergement sur Internet[458] et les revendeurs de carte SIM ou sans fil à prépaiement[459] exerçant leur activité à titre professionnel, peu importe que ce soit à temps complet ou partiel et contre rémunération ou à titre gratuit (art. 2 al. 1 AP LSCPT)[460]. Les personnes précitées qui n'exercent pas leur activité à titre professionnel devraient néanmoins tolérer une surveillance, comme c'est déjà le cas actuellement pour les réseaux de télécommunication internes et les centraux

[455] Sur la situation avant l'entrée en vigueur du CPP : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 120-124; SCHNEIDER, *Internet Service Provider im Spannungsfeld*, pp 182-184; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 95.

[456] ATF 6B_766/2009 du 8 janvier 2010, consid. 3.4.

[457] Soit les services qui ne sont plus soumis à concession comme le transport de lettres et de colis proposé en sus des prestations du service universel, le transport d'envois en courrier accéléré et d'envois de détail, et les prestations préalables et accessoires connexes telles que l'emballage et l'adressage d'envois postaux, la prise en charge d'envois postaux ou de marchandises et les conseils à la clientèle (art. 10 OPO).

[458] Reprenant ainsi l'extension du champ d'application

[459] *Rapport du CF relatif à l'AP LSCPT*, p. 30.

[460] *Rapport du CF relatif à l'AP LSCPT*, pp 16-18. Les fournisseurs d'accès à Internet seraient considérés comme des fournisseurs de services de télécommunications, de sorte qu'il n'est plus nécessaire de les mentionner séparément dans la loi : *Rapport du CF relatif à l'AP LSCPT*, p. 17.

domestiques[461]. Celui qui laisse à la disposition d'autres utilisateurs l'accès à son réseau sans fil permettant un accès à Internet serait considéré comme un fournisseur d'accès et devrait être en mesure d'identifier ces utilisateurs, respectivement les ordinateurs avec lesquels ils se sont connectés à Internet (art. 22 AP LSCPT)[462].

La surveillance de la correspondance par télécommunication concerne donc les appels téléphoniques et les communications transmises par fax, SMS, MMS, pager, courriels, téléphonie par Internet (VoIP), mais pas les conversations tenues sur une messagerie publique sur Internet (chat)[463]. La surveillance peut également porter sur les appels à destination de la Suisse effectués depuis un numéro étranger[464]. La saisie de matériel téléphonique ou informatique et leur consultation sont en revanche régies par les règles applicables au séquestre (art. 263ss CPP)[465]. 324

L'IMSI-Catcher, qu'il soit utilisé dans le but de rechercher des numéros IMSI ou IMEI, pour écouter des conversations téléphoniques, ou pour localiser un téléphone doit être considéré comme une mesure de surveillance de la correspondance, même si sa mise en œuvre ne dépend pas d'un opérateur téléphonique[466]. Le critère déterminant est l'objet de la surveillance et non le fait de savoir si la police est à même de mettre directement en place la 325

[461] Art. 2 al. 2 AP LSCPT,

[462] Cette identification pourrait avoir lieu par exemple par le biais d'un numéro de téléphone portable : *Rapport du CF relatif à l'AP LSCPT*, p. 33.

[463] Ces conversations sont librement accessibles. La personne intervenant sur une messagerie publique (chat) ou un forum de discussion sera plutôt qualifiée d'agent infiltré : RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, p. 443; RHYNER / STÜSSI, *Kommentar zu Art. 286-298 StPO*, pp 498-499. Voir également les notes de bas de page 322 ci-dessus et 486 ci-dessous.

[464] ATAF A-2335/2008 du 10 mars 2009, consid. 7 (les parties n'ont pas recouru contre cette décision). Etant donné qu'il n'est pas possible de brancher une surveillance directement sur le téléphone à l'étranger, une telle surveillance implique le scannage automatique de tous les appels effectués depuis l'étranger à destination de la Suisse pour repérer les communications qui sont visées par la surveillance. Le TAF a considéré qu'un tel procédé de scannage pouvant être automatisé, seules les données liées aux communications surveillées seront transmises et que cela ne constituait pas une atteinte incompatible avec les droits fondamentaux de tiers (consid. 7 et 8).

[465] RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, pp 443-445.

[466] Sur les possibilités d'utilisation de l'IMSI-Catcher, voir p. 40 ci-dessus et la note de bas de page n° 65.

surveillance ou s'il faut passer par l'intermédiaire d'un opérateur de télécommunication[467]. L'IMSI-Catcher surveille une transmission d'informations par le biais de techniques et d'installations de communication, ce qui en fait une mesure de surveillance de la correspondance[468].

326 L'avant-projet de révision de la LSCPT ajouterait un nouvel art. 270ter CPP (utilisation de systèmes de localisation) permettant d'utiliser l'IMSI-Catcher et des appareils similaires. Cette nouvelle disposition permettrait de localiser un appareil de téléphonie mobile et de déterminer ses données d'identification, mais pas d'écouter le contenu de la conversation. Le législateur a très probablement perdu de vue cette possibilité, ce qui crée une incertitude sur la possibilité d'utiliser également l'IMSI-Catcher dans ce but sur la base de l'art. 270ter CPP, ou s'il faudrait invoquer les art. 269ss CPP[469].

327 L'installation d'un « cheval de Troie » ou « Government-Software » n'a pas été prévue par le CPP, alors qu'il s'agit actuellement de la possibilité la plus simple de procéder à une surveillance des conversations téléphoniques effectuées par Internet[470]. Il est difficile de classer définitivement cette mesure de surveillance comme étant une mesure de surveillance de la correspondance ou un autre dispositif de surveillance. Jusqu'à présent, 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 opérés par les PTT, puis les opérateurs téléphoniques[471].

[467] Pour un avis contraire : DE SAUSSURE, *Le IMSI-Catcher*, ch. 41-44; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 117. La surveillance d'un réseau de téléphonie interne est pourtant clairement un cas de surveillance de la correspondance, quand bien même elle peut avoir lieu sans le concours d'un opérateur de télécommunication.

[468] Y compris pour la localisation d'un téléphone, puisque l'IMSI-Catcher recourt à l'infrastructure téléphonique (en simulant une antenne relais GSM) et au numéro d'identification du téléphone mobile au sein de cette infrastructure.

[469] *Rapport du CF relatif à l'AP LSCPT*, pp 43-44.

[470] Pour les considérations techniques, voir le chapitre 4. L'interception de données électroniques sur Internet, p. 40.

[471] Pour un avis partagé : SCHMID, *Handbuch*, p. 528; SCHMID, *Praxiskommentar*, p. 529.

Lorsqu'un « cheval de Troie » est placé dans un téléphone ou un ordinateur relié à un réseau de communication (Internet par exemple), il s'agit plutôt d'une mesure de surveillance de la correspondance : on surveille la transmission d'informations par le biais d'installations et de techniques de communication[472]. D'autres données que les données transmises peuvent également être surveillées[473]. Si l'ordinateur n'est en revanche pas relié à un réseau, la surveillance portera sur le contenu et l'activité de l'ordinateur, voire l'observation de ce qui se passe dans l'environnement de la machine. Nous le considérerons alors comme un autre dispositif de surveillance au sens de l'art. 280 CPP[474]. 328

La notion d'autre dispositif de surveillance revêt un caractère subsidiaire et il est impossible, en pratique, d'exclure qu'un ordinateur ne soit pas à un moment donné connecté à un réseau. Il serait donc préférable de considérer qu'il s'agit toujours d'un moyen de surveillance de la correspondance plutôt que d'un autre dispositif de surveillance[475]. La seule conséquence est que la mise sous surveillance de l'ordinateur d'un tiers serait possible si le prévenu l'utilise pour recevoir ou envoyer des communications. Hormis le cas très hypothétique d'un ordinateur sur lequel un correspondant viendrait enregistrer physiquement un message que le prévenu viendrait ensuite consulter, l'ordinateur sera connecté à un réseau et l'on sera en présence d'un cas de surveillance de la correspondance. 329

[472] L'ordinateur relié à un réseau (par câble, modem ou autre) est une installation de communication : STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 101-102.

[473] Pour cette raison, l'ordre de surveillance devrait indiquer précisément ce qui est recherché et quelles parties de la machine sont visées (emails, messagerie instantanée, VoIP, images, documents, etc.) pour éviter une surveillance disproportionnée.

[474] Voir à ce sujet le chapitre e) Les autres dispositifs techniques de surveillance, p. 152 ci-dessous.

[475] Dans le même sens : RHYNER / STÜSSI, *Kommentar zu Art. 280-281 StPO*, p. 468. D'autres encore considèrent au contraire en se basant sur une interprétation littérale que le CPP ne permet plus une telle mesure, qui était pourtant connue par certains codes cantonaux : HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 107; HANSJAKOB, *Zwangsmassnahmen in der neuen Eidg. StPO*, pp 110-111. L'avant-projet de révision de la LSCPT prévoit d'introduire un nouvel art. 270bis CPP intitulé « interception et décryptage de données ». Cette disposition servirait de base légale à la mise en place d'un « cheval de Troie » et serait considérée com152me une forme de surveillance comme un moyen de surveillance de la correspondance.

b) La récolte de données relatives au trafic, à la facturation et à l'identification

330 La récolte de données relatives au trafic, à la facturation et à l'identification des usagers est prévue par l'art. 273 CPP[476]. Il s'agit d'un élément de la surveillance de la correspondance qui répond cependant à des conditions légèrement différentes. Lorsqu'il s'agit exclusivement d'obtenir des données rétroactives, la police essaie souvent d'avoir l'accord de la personne concernée afin de ne pas avoir à suivre la procédure d'autorisation[477]. Cela ne peut évidemment concerner que les données auxquelles la personne a directement accès. Bien que cela ne ressorte pas expressément du texte de la loi, la recherche par champ d'antenne, soit la production de la liste des numéros de téléphone qui ont activé une antenne à un moment précis, est également régie par l'art. 273 CPP[478].

c) La surveillance des relations bancaires

331 Le CPP a introduit la base légale à cette mesure qui était précédemment mise en œuvre d'après une circulaire de l'Association suisse des banquiers[479]. Le CPP concrétise désormais 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[480]. Cette disposition mentionne les techniques spéciales, notamment les ordonnances de surveillance de comptes bancaires, l'observation, l'interception de télécommunications, l'accès à des systèmes informatiques et les ordonnances de production de documents déterminés.

[476] Parfois également appelées données secondaires. L'avant-projet de révision de la LSCPT prévoit d'utiliser de manière uniforme la notion de « données indiquant quand et avec quels raccordements la personne surveillée a été ou est en liaison par télécommunication et les données relatives au trafic et à la facturation » pour la correspondance par télécommunication et la notion de « données indiquant quand et avec quelles personnes la personne surveillée a été ou est en liaison par poste et les données relatives au trafic et à la facturation » pour la surveillance de la correspondance par poste (par exemple art. 16 lit. e et 19 al. 1 AP LSCPT) : *Rapport du CF relatif à l'AP LSCPT*, pp 26 et 29.

[477] RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, p. 448. Le prévenu peut par exemple donner le code d'accès à son téléphone ce qui permet de consulter l'historique récent, la liste des contacts, les courriers électroniques voire les sites visités, etc.

[478] RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, p. 455; SCHMID, *Praxiskommentar*, p. 514.

[479] Circulaire N° 1286 du 8.4.1997.

[480] RS 0.311.53.

La surveillance des relations bancaires ne devrait pas concerner la demande d'extraits de comptes bancaires ou le blocage de fonds[481]. De telles réquisitions ne portent que sur des documents existants et sont basées sur les dispositions concernant la perquisition et le séquestre[482]. La surveillance des relations bancaires consiste en une injonction à l'adresse de la banque de fournir à l'autorité pénale des informations et documents qui n'existent pas encore, mais qui existeront dans un avenir proche[483]. Il s'agit dans ce sens d'une surveillance en temps réel, qui peut s'étendre non seulement aux mouvements financiers, mais également aux lieux d'utilisation d'une carte bancaire par exemple. 332

L'obtention d'enregistrements de vidéosurveillance d'un guichet postal ou bancaire, ou d'un distributeur de billets ne tombe en revanche pas sous le coup des dispositions régissant le service des paiements ou la surveillance des relations bancaires[484]. 333

d) L'observation

L'observation est la surveillance systématique d'événements et de personnes sur la voie publique pendant un certain temps et l'enregistrement des résultats en vue de leur utilisation dans le cadre de la poursuite pénale[485]. Le fait de suivre une discussion sur un forum de discussion en ligne en se concentrant de manière ciblée sur certains participants est également considéré par le Tribunal fédéral 334

[481] Sur le blocage de comptes bancaires : EYMANN, *Die strafprozessuale Kontosperre*.

[482] Art. 241ss et 263ss CPP, EYMANN, *Die strafprozessuale Kontosperre*, pp 81-90. Rhyner/Stüssi estiment que la surveillance des relations bancaires concerne les données rétroactives et en temps réel : RHYNER / STÜSSI, *Kommentar zu Art. 284-285 StPO*, p. 484.

[483] *Message du CF relatif à l'unification de la procédure pénale*, p. 1236; JOSITSCH, *Grundriss des schweizerischen Strafprozessrechts*, p. 150; SCHMID, *Praxiskommentar*, p. 538.

[484] HANSJAKOB, *Die ersten Erfahrungen mit dem BÜPF*, p. 268. Ce sera un cas de séquestre (246 CPP), ou un autre dispositif de surveillance s'il est mis en place par l'autorité. Voir à ce sujet la section e) Les autres dispositifs techniques de surveillance, p. 152 ci-dessous.

[485] ALBERTINI, *Tableaux synoptiques des enquêtes de police*, p. 213; *Message du CF relatif à l'unification de la procédure pénale*, p. 1235; GISLER, *La coopération policière*, pp 87-90; RHYNER / STÜSSI, *Kommentar zu Art. 282-283 StPO*, pp 471-474; SCHMID, *Praxiskommentar*, pp 533-535. Pour une définition plus complète : GUÉNIAT / HAINARD, *Art. 282-283 CPP*, n 1 ad art. 282. Sur l'observation tant au niveau préventif que répressif, avant l'entrée en vigueur du CPP : KELLER, *Die politische Polizei*, pp 353-377. Sur l'observation effectuée par la Police judiciaire fédérale en 2009 : FEDPOL, *Rapport 2009*, pp 45-46. Sur l'observation en droit privé, public et pénal : AEBI-MÜLLER / EICKER / VERDE, *Verfolgung von Versicherungsmissbrauch mittels Observation*.

comme une observation[486]. Si l'enregistrement concerne des événements qui n'ont pas lieu sur la voie publique, il s'agit alors de mesures entrant dans la catégorie suivante, soit celle des autres dispositifs techniques de surveillance. Si l'observation et l'investigation secrète visent toutes deux à réunir les preuves d'un acte punissable sans que la personne soupçonnée ne s'en rende compte, elles se distinguent l'une de l'autre car la première s'opère à distance, alors que la seconde implique l'infiltration de fonctionnaires de police désignés pour effectuer cette tâche dans un milieu déterminé[487].

e) Les autres dispositifs techniques de surveillance

335 Les autres dispositifs techniques de surveillance, parfois appelés simplement autres mesures, sont définis par le code de procédure. Il s'agit des 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 (art. 280 CPP)[488]. L'enregistrement audio ou vidéo dans un lieu librement accessible au public est soumis aux dispositions concernant l'observation (art. 282 CPP)[489]. La surveillance vidéo ou la

[486] Si le policier prend part à la conversation ce sera de l'investigation secrète, alors que s'il suit la conversation de manière générale sans se concentrer sur certains participants en particulier, le TF ne voit pas de forme particulière et assimile cela à des policiers patrouillant en civil : ATF 134 IV 266, 278, Oberstaatsanwaltschaft des Kantons Zürich, du 16 juin 2008. Pour une critique de cet arrêt : HANSJAKOB, *Verdeckte Ermittlung*. Le TF n'y voit pas un cas de surveillance des télécommunications. Voir également les notes de bas de page 322 et 463 ci-dessus.

[487] ATF 134 IV 266, 270, Oberstaatsanwaltschaft des Kantons Zürich, du 16 juin 2008. Pour un avis favorable : VETTERLI, *Verdeckte Ermittlung und Grundrechtsschutz*. Pour une critique de la distinction entre observation secrète et investigation sercrète : HANSJAKOB, *Verdeckte Ermittlung*, pp 365-366.

[488] La localisation au moyen d'un téléphone portable est prévue par les art. 269ss CPP : RHYNER / STÜSSI, *Kommentar zu Art. 280-281 StPO*, p. 465. Sur l'utilisation de la vidéosurveillance par la police (en droit allemand) : GEIGER, *Verfassungsfragen zur polizeilichen Video-Überwachung*.

[489] Avant l'entrée en vigueur du CPP, certains admettaient le droit de la police de poser, sans autorisation judiciaire, des caméras dans des lieux faisant partie du domaine public : DUBUIS, *Note sur les mesures de surveillance optique par caméra*, p. 209. La question ne se pose désormais plus, le CPP distinguant la surveillance du domaine privée (soumise à autorisation selon les art. 272 et 281) de la surveillance du domaine public (soumise à autorisation à partir d'un mois selon l'art. 282) : DUBUIS, *Note sur les mesures de surveillance optique par caméra*, p. 211.

photographie d'une cabine téléphonique est considérée comme un autre dispositif technique de surveillance, et non une surveillance de la correspondance[490].

336 L'obtention d'enregistrements de vidéosurveillance d'un guichet postal ou bancaire, ou d'un distributeur de billets ne tombe pas sous le coup des dispositions régissant le service des paiements ou la surveillance des relations bancaires[491]. S'il est mis en place par l'autorité, il s'agit d'un autre dispositif de surveillance. En revanche, si la police se contente de récupérer la séquence vidéo d'une installation déjà en place, on aura à faire à un simple séquestre. L'art. 246 CPP prévoit que les documents écrits, les enregistrements audio, vidéo et d'autre nature, les supports informatiques ainsi que les installations destinées au traitement et à l'enregistrement d'informations peuvent être soumis à une perquisition lorsqu'il y a lieu de présumer qu'ils contiennent des informations susceptibles d'être séquestrées. La légalité des preuves ainsi obtenue devra être contrôlée, notamment si l'installation de surveillance était conforme aux dispositions légales applicables[492]. Il est en effet difficilement admissible que l'autorité utilise une surveillance illégale, pour laquelle elle n'aurait pas pu obtenir d'autorisation si elle avait souhaité la mettre en place elle-même[493]. Si la police souhaite continuer à utiliser l'installation existante, elle devra alors solliciter l'autorisation prévue par le CPP.

337 L'installation d'un « cheval de Troie » doit être considérée comme une mesure particulière de surveillance de la correspondance, sauf éventuellement le cas particulier d'un ordinateur qui ne serait pas relié à un réseau de communication[494]. Dans ce cas, la surveillance portera sur le contenu de l'ordinateur, voire l'observation de son activité et son environnement, ce qui en fait alors un autre dispositif de surveillance au sens de l'art. 280 CPP. L'avant-projet de révision de la LSCPT ajouterait un nouvel art. 270bis CPP permettant

[490] HANSJAKOB, *Die ersten Erfahrungen mit dem BÜPF*, p. 268.

[491] HANSJAKOB, *Die ersten Erfahrungen mit dem BÜPF*, p. 268.

[492] En particulier la LPD et le CP : MÉTILLE, *L'utilisation privée de moyens techniques de surveillance*, pp 195-198.

[493] On serait en présence d'une surveillance générale (elle ne vise pas uniquement le prévenu) et préventive (elle est mise en place avant que l'infraction ne soit éventuellement commise).

[494] Voir à ce sujet le chapitre a) La surveillance de la correspondance par poste et télécommunication, p. 145 ci-dessus.

l'utilisation d'un « cheval de Troie ». L'art. 270bis CPP prévoit toutefois une telle mesure seulement pour remplacer une mesure de surveillance de la correspondance par télécommunication restée sans succès. On reste alors dans le cas d'une surveillance de la correspondance pour un ordinateur ou téléphone potentiellement relié à un réseau de communication.

338 La localisation par un opérateur téléphonique d'un appareil comme la production de la liste des numéros de téléphone qui ont activé une antenne à un moment précis doivent en revanche être considérées comme la récolte de données relatives au trafic, à la facturation et à l'identification des usagers (art. 273 CPP). Ces mesures nécessitent le concours de l'opérateur qui remet des données consécutives à l'utilisation des services de l'opérateur par la personne surveillée. La localisation d'un téléphone dans le cadre d'une surveillance téléphonique se distingue de celle opérée avec un autre dispositif de surveillance, car la première est la conséquence de l'utilisation par la personne surveillée d'un service de télécommunication. Elle nécessite aussi l'accès à des données de l'opérateur téléphonique parmi lesquels figurent d'autres données accessoires couvertes par le secret de la correspondance.

339 La procédure étant la même, la distinction reste théorique. Certains auteurs considéraient, avant l'adoption du CPP, que les autres dispositifs techniques de surveillance étaient définis par les art. 179ss CP, l'art. 179^{octies} CP déclarant non punissable l'utilisation d'appareils de surveillance au sens des art. 179bisss CP si l'autorisation a été demandée au juge compétent[495]. Cette interprétation est trop restrictive, car l'utilisation d'un appareil qui ne constituerait pas une infraction au sens du Code pénal ne dispense pas l'autorité de respecter les exigences constitutionnelles et conventionnelles exigeant notamment une base légale. L'absence d'infraction pénale ne signifie pas qu'il n'y a pas d'atteinte à la sphère privée. Il faut alors retenir la définition de l'art. 280 CPP que l'on interprétera largement.

[495] Par exemple PIQUEREZ, *Traité*, p. 628; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 113-115.

3. Les mesures de contrainte assimilables aux mesures de surveillance

a) La recherche de personnes

L'art. 210 CPP reste vague, puisqu'il mentionne simplement que des recherches peuvent être ordonnées à l'encontre de personnes dont le lieu de séjour est inconnu et dont la présence est nécessaire au déroulement de la procédure, et qu'un avis de recherche peut être lancé à l'encontre du prévenu à certaines conditions. Le message du Conseil fédéral n'est pas d'un grand secours quant aux instruments de recherche admissibles. Il se contente de renvoyer à la législation sur la police et au droit administratif[496]. 340

Lorsqu'un avis de recherche est diffusé, la mesure n'est évidemment pas secrète. Dans les autres cas, et selon les moyens utilisés, la recherche de personnes aurait aussi pu figurer dans les mesures de surveillance secrètes. Même si le but n'est pas tant d'observer le comportement d'une personne, mais de la retrouver, la recherche de personnes peut présenter de nombreux points communs avec la surveillance entendue dans un sens plus classique. 341

b) L'analyse d'ADN

Un prélèvement en vue de l'établissement d'un profil d'ADN peut être effectué, à des conditions différentes, sur le prévenu, sur le condamné, sur d'autres personnes, ainsi que sur du matériel biologique[497]. Le CPP précise que le prélèvement invasif, par exemple par le biais d'une prise de sang, doit être effectué par un médecin ou un par un membre du personnel médical. *A contrario*, un frottis de la muqueuse jugale doit pouvoir être effectué par un policier[498]. 342

[496] *Message du CF relatif à l'unification de la procédure pénale*, p. 1203.

[497] Art. 255ss CPP. SCHMID, *Praxiskommentar*, pp 467-475. Pour un état des lieux dans les pays membres du Conseil de l'Europe : Arrêt S. et MARPER c. Royaume-Uni, no 30562/04 et 30566/04, §§ 45-49, du 4 décembre 2008.

[498] Art. 258 CPP, *Message du CF relatif à l'unification de la procédure pénale*, p. 1224.

343 Comme dans le cas de la recherche de personnes, cette mesure peut également être secrète. On pense ici aux prélèvements sur des objets et éventuellement à un prélèvement effectué à l'insu de la personne concernée.

344 Les prélèvements d'échantillons lors d'enquêtes de grande envergure, soit sur des personnes présentant des caractéristiques spécifiques constatées en rapport avec la commission de l'acte (art. 256 CPP), doivent encore être mentionnés[499]. Non seulement ces prélèvements ont la particularité de concerner un grand nombre de personnes, mais celles qui font l'objet de l'analyse doivent, par leur contribution, lever le vague soupçon qui pèse sur elles, alors que dans la règle c'est à l'Etat qu'il revient d'apporter la preuve de la culpabilité[500].

c) La récolte de données signalétiques

345 La récolte de données signalétiques recouvre les caractéristiques extérieures d'un être humain pouvant être mesurées ou constatées, comme la taille, le type, le poids, les empreintes digitales, les oreilles, ou d'autres parties du corps[501]. La reconnaissance faciale, ainsi que la reconnaissance de l'iris et de la rétine en font également partie. Comme pour la recherche de personnes et l'analyse d'ADN, la récolte de données peut également revêtir un caractère secret.

d) La récolte d'échantillons d'écriture ou de voix

346 Le législateur a choisi de traiter séparément la récolte d'échantillons d'écriture ou de voix en partant du principe que l'intéressé coopère[502]. Ce raisonnement est critiquable, puisqu'à nouveau la récolte peut avoir lieu à l'insu de la personne concernée, par exemple en recourant à des moyens d'enregistrement

[499] Pour une définition de la notion d'enquête de grande envergure : ROHMER, *Les enquêtes de grande envergure*, pp 97-98.

[500] *Message du CF relatif à la Loi fédérale sur l'utilisation de profils d'ADN*, p. 37. C'est pour cette raison notamment que le législateur a prévu qu'elles ne pouvaient être ordonnées que par le tribunal des mesures de contrainte (art. 256 CPP). Un contrôle par ce tribunal nous aurait pourtant paru suffisant. Voir à ce sujet le chapitre 2. Le cas particulier des mesures ordonnées par le tribunal des mesures de contrainte, p. 225 ci-dessous.

[501] Le prélèvement de sang, d'urine ou du bol alimentaire tombe sous le coup des dispositions sur l'examen corporel ou de l'analyse d'ADN, alors que le prélèvement d'éléments étrangers au corps ou séparés du corps relève des dispositions relatives à la fouille de personnes : *Message du CF relatif à l'unification de la procédure pénale*, p. 1225.

[502] *Message du CF relatif à l'unification de la procédure pénale*, p. 1226.

ou d'écoute. La Cour européenne des droits de l'Homme a retenu que l'enregistrement de la voix d'une personne sur un support permanent en vue d'une analyse ultérieure était manifestement de nature, combiné à d'autres données personnelles, à faciliter l'identification de cette personne. Elle a donc jugé que l'enregistrement des voix des requérants en vue d'une telle analyse ultérieure portait atteinte à leur droit au respect de la vie[503]. Les dispositions sur les autres moyens de surveillance devraient alors trouver application, ce qui réduit sensiblement la portée de l'art. 262 CPP. Le CPP rappelle que le prévenu peut refuser de donner un échantillon d'écriture ou de voix, en vertu du droit de ne pas s'auto-incriminer[504].

B. Les procédures de mise sous surveillance

1. En général

La compétence générale pour ordonner des mesures de contrainte est donnée au ministère public, au tribunal (et dans les cas urgents à la direction de la procédure), ainsi que dans les cas prévus par la loi à la police (art. 198 CPP). Pour ce qui est de l'instruction pénale, la compétence d'ordonner des mesures revient donc au ministère public, sous réserve des exceptions mentionnées ci-après[505]. 347

Le CPP prévoit quatre procédures différentes, soit deux procédures simples et deux procédures à deux instances. Pour les procédures simples, la compétence revient soit à la police, soit au ministère public et il n'y a pas de contrôle *a priori*. Pour les procédures à deux instances, dans le premier cas la surveillance est ordonnée par le ministère public puis autorisée par le tribunal des mesures de 348

[503] Arrêt S. et MARPER c. Royaume-Uni, no 30562/04 et 30566/04, § 83, du 4 décembre 2008.

[504] Ce qui n'est pas le cas en matière d'échantillons d'ADN : HANSJAKOB, *Zwangsmassnahmen in der neuen Eidg. StPO*, p. 107.

[505] Pour une liste des compétences pour ordonner des mesures de contrainte (et pas seulement des mesures de surveillance) revenant à la police, au ministère public et au tribunal des mesures de contrainte : JOHNER / VIREDAZ, *Art. 198-200 CPP*, ch. 6 ad art. 198.

contrainte[506]. Dans le deuxième cas, elle est ordonnée par le tribunal des mesures de contrainte sur proposition du ministère public.

349 Si l'octroi de la compétence à la police ou au ministère public, ainsi que l'existence ou non d'un contrôle *a priori* peuvent se comprendre, la distinction entre une décision du ministère public puis une autorisation du tribunal d'une part et une proposition du ministère public puis une décision du tribunal d'autre part, ne paraît pas très judicieuse. Le législateur a considéré que cette distinction était nécessaire, car il s'agit de mesures de contrainte importantes qui peuvent attendre la décision du tribunal des mesures de contrainte pour les secondes mais qui revêtent un caractère urgent pour les premières[507].

2. Les mesures ordonnées par la police

a) Les mesures concernées

350 La police[508] est compétente pour ordonner la saisie de données signalétiques (sauf si la personne s'y oppose !)[509], pour ordonner une observation ne dépassant pas un mois[510], pour ordonner un prélèvement non invasif d'échantillons d'ADN ou l'établissement d'un profil d'ADN à partir de matériel biologique ayant un lien avec l'infraction[511] et pour lancer un avis de recherche en cas d'urgence[512].

[506] Sur les compétences du tribunal des mesures de contrainte et la distinction d'avec les autres tribunaux : COQUOZ, *Le tribunal des mesures de contrainte*, pp 108-118; KUHN, *La procédure pénale suisse selon le futur CPP unifié*, pp 157-160; KUHN, *Procédure pénale unifiée*, pp 45-49; PIETH, *Schweizerisches Strafprozessrecht*, pp 63-64.

[507] Cette justification ne nous convainc pas. Voir à ce sujet le chapitre 2. Le cas particulier des mesures ordonnées par le tribunal des mesures de contrainte, p. 225 ci-dessous.

[508] Ou certains membres du corps de police selon la réglementation cantonale réservée par l'art. 198 al. 2 CPP. Sur les compétences accordées à la police par le CPP : KUHN, *La procédure pénale suisse selon le futur CPP unifié*, pp 142-143.

[509] Art. 260 CPP. Sur les différentes compétences pour ordonner le prélèvement de données signalétiques : ALBERTINI, *Tableaux synoptiques des enquêtes de police*, p. 200.

[510] Art. 282 CPP.

[511] Art. 255 al. 2 CPP. La police peut ordonner un prélèvement d'ADN sur des traces ou sur une personne si le prélèvement n'est pas invasif.

b) La procédure

Les compétences attribuées à la police appartiennent également au ministère public, puisque ce dernier est responsable de la direction de la procédure à ce stade[513]. Le ministère public peut en tout temps donner des directives et confier des mandats à la police ou se saisir d'un cas[514]. La voie du recours est ouverte directement contre ces actes de procédure (art. 393 al. 1 lit. a CPP) [515]. 351

La saisie des données signalétiques fait l'objet d'un mandat écrit, brièvement motivé. En cas d'urgence, elle peut être ordonnée oralement, mais doit être ensuite confirmée par écrit[516]. Aucune décision écrite n'est requise concernant l'observation et les prélèvements d'ADN soumis à la compétence de la police[517], de même qu'en matière de recherches[518]. 352

Elle peut également ordonner l'analyse de l'ADN (établissement d'un profil) sur la base de traces récoltées, mais elle n'est plus compétente pour décider de l'analyse de l'ADN (établissement d'un profil) sur la base du prélèvement effectué sur une personne : ROHMER, *Art. 255-262 CPP*, n. 26 ad art. 255; SCHMID, *Praxiskommentar*, p. 471; VOSER, *Kommentar zu Art. 255-259 StPO*, p. 388.

[512] Art. 210 al. 1 CPP.

[513] Art. 61 lit. a CPP. Le terme «direction de la procédure» désigne les personnes qui sont responsables de la conduite la procédure à un stade donné : *Message du CF relatif à l'unification de la procédure pénale*, p. 1128.

[514] Art. 307 al. 2 CPP. Il bénéficie en outre de la compétence générale d'ordonner des mesures de contrainte de l'art. 198 CPP.

[515] Voir à ce sujet le chapitre G. Le contrôle *a posteriori*, p. 189 ci-dessous.

[516] Art. 260 al. 3 CPP.

[517] Art. 255 et 282 CPP *a contrario*. Une communication écrite *a posteriori* est prévue pour l'observation (art. 283 CPP).

[518] Art. 210 CPP *a contrario*.

3. Les mesures ordonnées par le ministère public seul

a) Les mesures concernées

353 S'agissant des mesures de surveillance[519], le ministère public est compétent, sans autorisation supplémentaire, pour ordonner la saisie de données signalétiques en cas de refus de la personne concernée[520], pour ordonner un prélèvement invasif d'échantillon d'ADN et l'analyse de l'échantillon d'ADN prélevé sur une personne [521], pour autoriser la poursuite d'une observation au-delà d'un mois[522], pour ordonner la recherche d'une personne ou lancer un avis de recherche[523] et pour astreindre une personne à fournir un échantillon d'écriture ou de voix[524].

b) La procédure

354 Ces mesures ne sont soumises à aucune autorisation du tribunal des mesures de contrainte, mais la voie du recours est directement ouverte contre la décision du ministère public ou l'acte de procédure (art. 393 al. 1 lit. a CPP) [525]. Le CPP ne prévoit aucune procédure particulière pour la décision du ministère public. La forme écrite n'est pas exigée, bien que cela paraisse souhaitable[526].

---

[519] Le ministère public dispose bien évidemment aussi de compétences dans d'autres domaines. Voir par exemple CORNU, *Le nouveau ministère public*, pp 59-77; KUHN, *La procédure pénale suisse selon le futur CPP unifié*, pp 143-146; KUHN, *Procédure pénale unifiée*, pp 36-40.

[520] Art. 260 al. 4 CPP.

[521] Art. 255 CPP. Le ministère public est évidemment aussi compétent pour ordonner un prélèvement non invasif : GOLDSCHMID / MAURER / SOLLBERGER, *Kommentierte Textausgabe zur StPO*, pp 241-242; VOSER, *Kommentar zu Art. 255-259 StPO*, p. 388. Avant l'entrée en vigueur du CPP, une autorisation judiciaire était nécessaire : HANSJAKOB, *Zwangsmassnahmen in der neuen Eidg. StPO*, pp 105-106.

[522] Art. 282 CPP.

[523] Art. 210 CPP.

[524] Art. 262 CPP. La compétence du ministère public n'est pas expresse, mais elle ressort de l'art. 198 CPP. On peut toutefois se demander si la compétence de la police en matière de saisie de données signalétiques ne devrait pas être appliquée par analogie. La question reste cependant théorique, puisque dans ce cas la police n'est compétente que si la personne concernée est d'accord.

[525] Voir à ce sujet le chapitre G. Le contrôle *a posteriori*, p. 189 ci-dessous.

[526] Art. 199 CPP *a contrario* (« lorsqu'une mesure de contrainte est ordonnée par écrit »).

4. Les mesures ordonnées par le ministère public puis autorisées par le tribunal

a) Les mesures concernées

Le ministère public peut ordonner une surveillance de la correspondance par poste et télécommunication[527], obtenir les données relatives au trafic, à la facturation et à l'identification des usagers[528], et ordonner l'utilisation d'autres dispositifs techniques de surveillance[529]. Ces mesures devront ensuite être autorisées par le tribunal des mesures de contrainte (art. 274 CPP). 355

L'interception et le décryptage de données (art. 270bis CPP)[530] ainsi que l'utilisation de systèmes de localisation (art. 270ter CPP)[531], prévus par l'avant-projet de révision de la LSCPT, suivraient également cette procédure. 356

b) La procédure

i. La décision du ministère public

La procédure est basée sur celle que prévoyait la LSCPT[532]. Bien qu'il s'agisse d'une décision du ministère public, elle est en pratique suggérée par la police au travers d'un rapport qu'elle lui adresse. Les autorités cantonales avaient jusqu'à présent des pratiques assez variées, certains cantons accordant quasi automatiquement les autorisations de surveillance, alors que d'autres étaient plus restrictifs. L'entrée en vigueur du CPP devrait permettre d'unifier, au moins en partie, les pratiques cantonales. 357

---

[527] Art. 269 CPP.

[528] Art. 273 CPP.

[529] Art. 280 CPP.

[530] « Cheval de Troie »

[531] IMSI-Catcher.

[532] Voir notamment : BIEDERMANN, *BÜPF*; BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 507-522; HANSJAKOB, *BÜPF und VÜPF Kommentar*; HAUSER / SCHWERI / HARTMANN, *Schweizerisches Strafprozessrecht*, pp 358-366; OBERHOLZER, *Grundzüge des Strafprozessrechts*, pp 555-565; PIQUEREZ, *Traité*, pp 621-623; SCHMID, *Praxiskommentar*, pp 501-527; SCHMID, *Strafprozessrecht*, pp 289-290; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 140-153.

358 L'art. 269 CPP ne dit pas sous quelle forme le ministère public ordonne la surveillance. L'Ordonnance du Conseil fédéral sur la surveillance de la correspondance par poste et télécommunication précise le contenu de l'ordre de surveillance[533]. Celui-ci doit notamment mentionner l'autorité qui ordonne la surveillance, celle à qui les résultats sont destinés, l'objet de la surveillance, l'identité (pour autant qu'elle soit connue) de la personne à surveiller, l'infraction poursuivie, le type de surveillance ordonnée et les informations techniques nécessaires. L'ordre précisera encore le début et la fin de la surveillance. En pratique, le ministère public recourt à des formulaires établis par le Service chargé de la surveillance de la correspondance par poste et télécommunication (Service SCPT)[534]. Ces formulaires sont souvent remplis par la police[535].

359 L'ordre de surveillance doit être transmis par écrit. En cas d'urgence, il peut être communiqué oralement, mais les résultats de la surveillance ne seront transmis qu'à réception de l'ordre écrit (art. 5 OSCPT). Il sera adressé au Service SCPT pour ce qui concerne la surveillance de la correspondance par poste et télécommunication et les données relatives au trafic, à la facturation et à l'identification des usagers. En ce qui concerne l'utilisation d'autres dispositifs techniques de surveillance, l'ordre sera transmis à la police judiciaire, ces mesures de surveillance n'étant pas du ressort du Service SCPT [536].

360 L'ordre de surveillance est immédiatement exécutoire. A réception de l'ordre, le Service SCPT vérifie que la surveillance concerne une infraction pouvant faire l'objet d'une telle mesure et qu'elle a été ordonnée par l'autorité compétente. La

[533] Art. 11, 15 et 23 OSCPT, RS 780.11.

[534] Sur le contenu de l'ordre de surveillance : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 403-408, 412-424 et 443-449. Le service chargé de la surveillance de la correspondance par poste et télécommunication (Service SCPT) est rattaché administrativement au Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP) depuis le 1er septembre 2007. Il dépendait auparavant du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) et s'appelait Service des tâches spéciales (STS). L'intitulé du service ne figure dans aucune loi : Modification de l'OSCPT du 22 août 2007 (RO 2007 4029) et ATAF A-2335/2008 du 10 mars 2009, consid. 3.1.2. Sur l'organisation et les tâches du Service SCPT, anciennement STS : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 128-134, 331-338 et 343-350; PIQUEREZ, *Traité*, pp 618 et 623-624; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 154-157.

[535] RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, p. 455.

[536] Art. 2 al. 1 LSCPT *a contrario.*

surveillance est mise en œuvre même si l'ordre de surveillance est manifestement erroné ou qu'il n'est pas motivé. Dans ce cas toutefois, le Service SCPT prend contact avec le tribunal des mesures de contrainte avant que le résultat de la surveillance ne soit transmis au ministère public[537]. Dans le cas de l'utilisation d'autres dispositifs techniques, il est peu probable que la police alerte le tribunal des mesures de contrainte à cause d'un ordre mal rédigé par le ministère public, alors qu'elle lui est directement subordonnée.

La voie du recours est théoriquement ouverte contre la décision du ministère public, mais la personne surveillée n'en a pas connaissance (art. 393 al. 1 lit. a CPP)[538]. Une telle voie de recours n'est guère logique puisque la décision du ministère public doit encore être autorisée, avec effet rétroactif, par le tribunal des mesures de contrainte. La décision du ministère public n'est alors que provisoire et le produit de la surveillance ne peut pas être utilisé si elle n'est pas approuvée ensuite par le tribunal des mesures de contrainte. Ce recours ne serait dirigé que contre la décision initiale ordonnant temporairement la surveillance, mais pas contre celle, définitive, autorisant la surveillance. Cette construction juridique doit être écartée, d'autant plus que l'art. 279 al. 3 CPP prévoit un recours spécial en matière de surveillance, qui ne distingue pas les décisions du ministère public et du tribunal des mesures de contrainte[539]. 361

ii. L'autorisation du tribunal des mesures de contrainte

L'ordre de surveillance est soumis à l'autorisation du tribunal des mesures de contrainte et cela qu'il s'agisse d'une surveillance de la correspondance, de l'obtention de données relatives au trafic, à la facturation et à l'identification des usagers ou de l'utilisation d'autres dispositifs techniques de surveillance (art. 274 CPP). Certains auteurs préféreraient un contrôle différencié en fonction de la gravité de l'atteinte[540]. A notre avis, l'atteinte est dans tous les cas suffisamment importante pour justifier un contrôle et il n'est pas souhaitable que le ministère public ou la police puisse décider que la surveillance ne représente 362

[537] Art. 11 al. 1 let. a LSCPT et STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 154-157.

[538] Voir à ce sujet le chapitre G. Le contrôle *a posteriori*, p. 189 ci-dessous.

[539] BACHER / ZUFFEREY, *Art. 279 CPP*, n. 8 ad art. 279.

[540] Voir notamment : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 239-240.

pas une atteinte suffisamment importante pour nécessiter une autorisation, ou qu'une procédure d'autorisation simplifiée puisse suffire. Admettre le contraire reviendrait à donner à l'autorité qui ordonne la surveillance la possibilité de définir ce qu'elle est d'accord de laisser contrôler au tribunal. Une appréciation en fonction de l'atteinte est au surplus effectuée par le tribunal des mesures de contrainte dans le cadre du contrôle du respect de la proportionnalité.

363 Dans les vingt-quatre heures suivant le début de la surveillance, le ministère public doit transmettre au tribunal des mesures de contrainte l'ordre de surveillance accompagné d'un exposé des motifs et des pièces du dossier qui sont déterminantes pour l'autorisation de surveillance[541].

364 Le tribunal des mesures de contrainte est une institution nouvelle dans la plupart des cantons (art. 18 CPP)[542]. Une spécialisation des juges n'est pas imposée, mais elle serait souhaitable. Les questions à résoudre par cette autorité seront multiples et toucheront toutes à la liberté individuelle des citoyens[543].

365 Cette autorité statue ensuite dans les cinq jours suivant le début de la surveillance[544]. La personne surveillée ne participe pas à la procédure, puisqu'elle n'en est pas informée. Le tribunal se base sur les documents que le ministère public lui a transmis, spontanément ou sur requête. Les premiers résultats de la surveillance ne doivent pas être pris en compte pour autoriser la

[541] Le délai se compte à la minute près, dès la transmission de l'ordre de surveillance au Service SCPT. Les avis sont partagés quant à savoir si la demande d'autorisation doit être expédiée ou reçue dans le délai de 24h. La question demeure théorique, puisqu'il s'agit d'un délai d'ordre dont l'inobservation n'est assortie d'aucune sanction : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 241-243; JEAN-RICHARD-DIT-BRESSEL, *Ist ein Millionendiebstahl ein Bagatelldelikt*, p 51; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 143.

[542] En plus des compétences mentionnées en matière de surveillance, il est compétent pour ordonner la détention provisoire (art. 220 et 225ss CPP) et la détention pour des motifs de sûreté (art. 220 et 229ss CPP), pour décider de mesures de substitution à la détention (art. 237ss CPP), pour approuver la garantie d'anonymat accordée par le ministère public à une personne (art. 149 CPP), pour ordonner l'hospitalisation d'un prévenu à des fins d'expertise (art. 186 CPP), pour statuer sur la levée des scellés posés sur des documents saisis (art. 248 al. 3 CPP), pour statuer sur les séquestres contestés ou réclamés par plusieurs personnes (art. 264 al. 3 et 267 al. 4 CPP), pour autoriser l'engagement d'un agent infiltré (art. 289 CPP) et pour décider d'un cautionnement préventif (art. 373 CPP).

[543] CORNU, *L'enquête selon le CPP*, pp 75-76.

[544] Le délai de cinq jours est également un délai d'ordre.

mesure, puisque le CPP prévoit expressément qu'en cas de refus ils ne peuvent être utilisés. Nous imaginons donc mal que l'on puisse en tenir compte avant l'octroi de l'autorisation pour justifier la mesure, alors qu'en cas de refus ces informations seraient considérées comme inexistantes[545].

366 La décision doit être rendue par écrit et être brièvement motivée en fait et en droit. Le tribunal des mesures de contrainte vérifie avec un plein pouvoir d'examen si la mesure de surveillance est permise pour l'infraction visée, si la prévention s'avère suffisante, si la gravité de l'acte justifie la surveillance et si cette dernière constitue bien une *ultima ratio*[546].

367 Le tribunal des mesures de contrainte peut autoriser la surveillance à titre provisoire, assortir l'autorisation de conditions ou encore demander que le dossier soit complété ou que d'autres éclaircissements soient apportés. L'autorisation doit aussi indiquer si des mesures visant à sauvegarder le secret professionnel doivent être prises et si des branchements directs peuvent être effectués. Le tribunal des mesures de contrainte communique immédiatement sa décision au Service SCPT et au ministère public. La personne surveillée ne peut pas recourir contre cette décision, au cas où elle en aurait connaissance, mais doit attendre la communication qui intervient à la fin de la surveillance (art. 393 al. 1 lit. c CPP). Cela n'est pas satisfaisant[547]. Quant au contrôle effectué par le Service SCPT, il est limité. Le Service SCPT n'a pas de compétence décisionnelle. Il peut tout au plus avertir le tribunal des mesures de contrainte s'il considère que l'ordre de surveillance n'est pas conforme[548].

368 Aucune voie de recours n'est ouverte à ce stade, étant donné qu'un recours ne peut être déposé par le prévenu qu'après la réception de la communication l'informant qu'il a fait l'objet d'une surveillance[549]. Le ministère public peut

[545] Pour un avis plus nuancé dans les cas où l'on aboutirait à un résultat choquant : HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 245.

[546] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 245-247; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 146-147.

[547] Pour les personnes visées par la surveillance, voir le chapitre G. Le contrôle *a posteriori*, p. 189 ci-dessous.

[548] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 332-336 et 344; HAUSER / SCHWERI / HARTMANN, *Schweizerisches Strafprozessrecht*, p. 362.

[549] Voir à ce sujet le chapitre G. Le contrôle *a posteriori*, p. 189 ci-dessous.

toutefois ordonner une nouvelle demande, espérant qu'elle soit mieux accueillie par le tribunal des mesures de contrainte que la précédente.

369 L'autorisation peut être octroyée pour trois mois au plus, et prolongée pour des périodes d'une même durée. Si la prolongation de la surveillance est nécessaire, le ministère public la demande avant l'expiration du délai en en indiquant les motifs. La procédure de prolongation est similaire à celle d'autorisation[550]. Le Service SCPT doit vérifier que la surveillance ne se prolonge pas au-delà de la durée autorisée (art. 11 al. 1 lit. d et 13 al.1 lit. g LSCPT).

370 La surveillance prend déjà effet au moment de la décision du ministère public[551]. Si le tribunal des mesures de contrainte n'autorise finalement pas la surveillance, les documents et enregistrements collectés doivent être immédiatement détruits, et les envois postaux retenus doivent être immédiatement remis à leurs destinataires (art. 277 CPP). Les informations recueillies durant cette surveillance non autorisée ne peuvent être exploitées, que ce soit à titre de preuves ou de moyens d'investigation. Il s'agit d'une interdiction absolue, qui ne laisse pas de place à une pesée d'intérêts[552]. La décision du ministère public est en quelque sorte provisoire.

[550] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 248 et 253-255; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 152.

[551] A la minute près : STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 129.

[552] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 250-253; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 151.

5. Les mesures ordonnées par le tribunal des mesures de contrainte

a) Les mesures concernées

371 Sur proposition du ministère public, le tribunal des mesures de contrainte[553] peut ordonner la surveillance des relations bancaires[554] et le prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure[555].

b) La procédure

372 Pour ce qui est des prélèvements d'ADN lors d'enquêtes de grande envergure, le message indique que cette mesure est subordonnée à l'autorisation préalable du tribunal des mesures de contrainte[556]. Le texte de la loi parle toutefois d'ordonner à la demande du ministère public[557]. Une procédure différente de celle prévue pour la surveillance de la correspondance trouve une justification dans le fait qu'il y a rarement un caractère d'urgence et que ce genre de prélèvement pose des problèmes importants de respect de la proportionnalité. Le fait que ce soit le tribunal des mesures de contrainte qui l'ordonne a cependant l'effet regrettable de soustraire la décision à un recours au sens de l'art. 393 CPP et d'obliger le prévenu à déposer un recours en matière pénale devant le Tribunal fédéral[558].

373 Quant à la surveillance des relations bancaires, le texte français du CPP prévoit que le tribunal des mesures de contrainte peut autoriser une telle surveillance, avant de préciser qu'il donne à la banque des directives écrites sur le type d'informations et de documents à fournir[559]. Les versions allemande et italienne

[553] Le tribunal des mesures de contrainte a également des compétences dans d'autres domaines, notamment en matière de détention provisoire et de détention de sûreté (art. 18 CPP) : KUHN, *Procédure pénale unifiée*, pp 47-49.

[554] Art. 284 CPP. L'avant-projet donnait la compétence au ministère public d'ordonner seul une surveillance des relations bancaires d'une durée d'un mois (art. 318ss AP-CPP). Sans explication, le projet a changé.

[555] Art. 256 CPP.

[556] *Message du CF relatif à l'unification de la procédure pénale*, p. 1224.

[557] Art. 256 CPP.

[558] Voir à ce sujet le chapitre G. Le contrôle *a posteriori*, p. 189 ci-dessous.

[559] Art. 284 et 285 CPP.

de l'art. 284 CPP parlent d'ordonner[560]. Le message souligne que le tribunal des mesures de contrainte ne se contente pas d'ordonner la mesure, mais qu'il en définit aussi les modalités d'exécution en se fondant sur la requête du ministère public[561]. La surveillance des relations bancaires ne débuterait alors qu'avec la décision du tribunal. Aucun délai n'est imparti au tribunal des mesures de contrainte pour statuer sur la proposition du ministère public[562].

374 L'existence d'un régime d'autorisation différent en matière de surveillance des relations bancaires s'explique, pour le Conseil fédéral, par le fait qu'elle ne doit normalement pas être ordonnée dans l'urgence, les informations et documents visés pouvant aussi être obtenus plus tard, au moyen d'une injonction de dépôt ou d'une mesure de séquestre[563]. Ce raisonnement est valable uniquement si aucune surveillance en temps réel n'est envisagée, ce qui semble être l'intention des auteurs du projet de loi, puisqu'ils ont pensé seulement à des extraits de comptes ou de dépôts, des contrats ou des lettres[564]. Le CPP exigerait alors l'autorisation du tribunal des mesures de contrainte pour l'obtention d'extraits de comptes bancaires, contrairement à la pratique en vigueur précédemment, mais laisserait la compétence en matière de perquisition et de séquestre au

[560] En allemand: « Zur Aufklärung von Verbrechen oder Vergehen kann das Zwangsmassnahmengericht auf Antrag der Staatsanwaltschaft die Überwachung der Beziehungen zwischen einer beschuldigten Person und einer Bank oder einem bankähnlichen Institut anordnen ». En italien: « Per far luce su crimini o delitti, il giudice dei provvedimenti coercitivi può, su richiesta del pubblico ministero, disporre la sorveglianza delle relazioni tra l'imputato e una banca o un istituto analogo ». Les termes « anordnen » et « disporre » figurent également à l'art. 256 CPP et sont traduits en français par ordonner.

[561] *Message du CF relatif à l'unification de la procédure pénale*, p. 1237.

[562] 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.

[563] *Message du CF relatif à l'unification de la procédure pénale*, p. 1237. Dans le même sens : GOLDSCHMID, *Geheime Überwachungsmassnahmen*, pp 169-170; WOLTER, *Kommentar zu Art. 269-281 StPO*, p. 275. Pour un avis contraire et justifié : RHYNER / STÜSSI, *Kommentar zu Art. 284-285 StPO*, p. 485.

[564] *Message du CF relatif à l'unification de la procédure pénale*, p. 1237. Egalement en faveur d'une surveillance rétroactive et en temps réel : RHYNER / STÜSSI, *Kommentar zu Art. 284-285 StPO*, p. 484.

ministère public dès qu'il ne s'agit plus d'établissements bancaires[565]. Ceci n'est guère heureux, car la localisation d'un prévenu ou le blocage de fonds à temps serait impossible sur la base de la surveillance des relations bancaires. La surveillance en temps réel devrait alors être régie par les dispositions sur les autres dispositifs techniques de surveillance.

375 En réalité, il faut admettre que le législateur a perdu de vue que la surveillance des relations bancaires ne concernait pas seulement la remise de documents dont l'examen n'a rien d'urgent, mais également des informations en temps réel permettant de connaître le lieu, le but et le contenu d'une transaction financière (y compris l'utilisation d'une carte de crédit ou de débit)[566] voire le lieu, le moment et la manière dont le titulaire du compte contacte la banque[567]. Il a envisagé une surveillance des relations futures du prévenu avec l'établissement bancaire[568], mais pas en temps réel. Le Message du Conseil fédéral fait d'ailleurs expressément référence à la Convention du Conseil de l'Europe relative au blanchiment, au dépistage, à la saisie et à la confiscation des produits du crime et qui vise des techniques spéciales d'enquêtes[569].

376 Dans ces circonstances, il convient d'appliquer par analogie, et malgré la terminologie utilisée, la procédure appliquée pour la surveillance de la correspondance et retenir que le tribunal des mesures de contrainte autorise la surveillance que le ministère public a ordonnée. Elle devrait être effective dès la décision du ministère public, ce qui correspond à la version française. Un tel raisonnement se justifie également 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

[565] Pour une mention du séquestre de documents bancaires et d'une perquisition, ce qui confirme que le séquestre et la perquisition continuent à exister également pour les établissements bancaires : *Message du CF relatif à l'unification de la procédure pénale*, p. 1221.

[566] De telles mesures sont d'ailleurs régulièrement mises en place pour connaître en temps réel l'utilisation d'une carte de crédit, des mouvements de fonds, etc.

[567] SCHMID, *Praxiskommentar*, p. 538.

[568] GOLDSCHMID / MAURER / SOLLBERGER, *Kommentierte Textausgabe zur StPO*, p. 274.

[569] *Message du CF relatif à l'unification de la procédure pénale*, pp 1236-1237.

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[570]. Comme en matière de surveillance de la correspondance, aucune voie de recours n'est ouverte à ce stade. Un recours ne peut être déposé qu'après la réception par le prévenu de la communication l'informant qu'il a fait l'objet d'une surveillance.

C. Les conditions auxquelles une surveillance peut être ordonnée

1. L'objet de la surveillance

377 Le prévenu, ou des lieux et des objets auxquels il a accès, sont évidemment visés par toutes les mesures de surveillance. La surveillance de la correspondance peut cependant également être dirigée contre un tiers, si le prévenu utilise l'adresse postale ou le raccordement de télécommunication du tiers comme s'il s'agissait du sien ou que le tiers joue le rôle d'intermédiaire[571]. Ce sont toutefois toujours le prévenu et ses actes qui sont visés[572]. La surveillance d'un raccordement public ou anonyme doit être traitée comme la surveillance d'un tiers[573]. Ces principes s'appliquent également concernant la récolte des données relatives au trafic et à la facturation et à l'identification des usagers. La surveillance des relations bancaires et l'utilisation d'autres dispositifs de surveillance ne peuvent cependant viser que le prévenu. Le compte bancaire ouvert et utilisé par un tiers mais pour le compte du prévenu échappe ainsi malheureusement à la surveillance.

[570] CASSANI / OURAL, *Art. 284-285 CPP*, n. 21 et 25 ad art. 284.

[571] Art. 270 CPP, *Message du CF relatif à l'unification de la procédure pénale*, p. 1231. Sur la surveillance des tiers : BIEDERMANN, *BÜPF*, pp 84-85; GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 120-128 et 165-201; HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 189-195; OBERHOLZER, *Grundzüge des Strafprozessrechts*, pp 550-552; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 133-139.

[572] A distinguer du tiers qui est surveillé non pas en tant que tel, mais parce qu'il est par exemple le correspondant du surveillé.

[573] BACHER / ZUFFEREY, *Art. 270 CPP*, n. 16-17 ad art. 270.

Les recherches peuvent être ordonnées à l'encontre de toute personne dont le lieu de séjour est inconnu et dont la présence est nécessaire au déroulement de la procédure[574]. L'observation n'est pas limitée à la personne du prévenu, ce qui signifie qu'elle peut être dirigée contre n'importe qui. Il faut toutefois des indices laissant penser qu'un crime ou un délit a été commis. Il n'est pourtant pas exigé que l'auteur présumé de l'infraction soit l'objet principal de l'observation[575]. 378

Le prélèvement d'ADN peut être effectué également sur les victimes ou les personnes habilitées à se rendre sur les lieux de l'infraction si cela est nécessaire pour distinguer leur matériel biologique de celui du prévenu[576]. Dans le cadre d'enquêtes de grande envergure, un prélèvement peut être effectué sur toutes les personnes présentant des caractéristiques spécifiques constatées en lien avec la commission de l'acte[577]. Les profils établis lors d'une enquête de grande envergure ne peuvent toutefois pas être conservés.[578] 379

La saisie de données signalétiques ne semble pas limitée à la personne du prévenu[579]. Les échantillons d'écriture et de voix peuvent être requis du prévenu, d'un témoin et de toute personne appelée à donner des renseignements. Les personnes qui bénéficient d'un droit de refuser de témoigner ou de déposer, de même que le prévenu, ne peuvent pas être sanctionnées si elles refusent de fournir un tel échantillon[580]. 380

2. Les motifs de la surveillance

a) Le soupçon

Des mesures de contrainte ne peuvent être ordonnées que si des soupçons suffisants laissent présumer une infraction (art. 197 al. 1 lit. b CPP). Cette condition est reprise ensuite pour chaque mesure de surveillance. On retrouve 381

[574] Art. 210 CPP. L'avis de recherche ne peut cependant que concerner le prévenu.
[575] Art. 282 CPP.
[576] Art. 255 al. 1 CPP.
[577] Art. 256 CPP.
[578] Art. 11 al. 4 lit. c LADN.
[579] Art. 260 CPP.
[580] Art. 262 CPP.

l'exigence de respect de la proportionnalité et l'interdiction d'une surveillance générale et abstraite. En l'absence de soupçons suffisants, il ne faudrait pas que la surveillance puisse être opérée à un autre titre pour constituer un dossier permettant ensuite d'obtenir l'autorisation requise pour la surveillance pénale[581].

382 Les mesures de surveillance prévues par le CPP ont pour but de rechercher l'auteur de l'infraction ou des preuves liées à l'infraction. Elles ne sont admises que si une infraction a été commise[582]. En ce sens, il s'agit d'une surveillance répressive[583]. Le CPP ne prévoit pas la surveillance à titre préventif et ne peut en aucun cas servir de base légale à une mesure de surveillance qui serait instaurée dans ce but[584]. Il est en revanche admis que la surveillance puisse porter sur les actes futurs dans le cas d'un délit continu, notamment en matière de trafic de stupéfiants, où ce n'est pas tant les délits commis qui sont visés, mais ceux qui sont en cours et le réseau existant[585]. La seule commission d'actes préparatoires n'ouvre pas la voie à des mesures de surveillance, sauf s'il s'agit d'actes préparatoires délictueux au sens de l'art. 260bis CP[586].

[581] Jusqu'à l'entrée en vigueur de la LSCPT le 1er janvier 2002, il n'était pas rare que des mesures de surveillance préventives soient ordonnées dans le seul but de glaner des informations pouvant déboucher sur une enquête pénale. Une fois qu'un nombre suffisant d'informations étaient recueillies, plus rien ne s'opposait à l'ouverture d'une procédure pénale et à la mise en place de mesures de surveillance dans ce cadre. Le recours à la surveillance préventive n'était pourtant pas justifié par une menace pour la sécurité, mais servait essentiellement à s'assurer d'avoir assez d'éléments lors de la demande de l'autorisation judiciaire nécessaire à la surveillance pénale.

[582] De manière générale l'art. 197 al. 1 lit. b CPP et pour des exemples les art. 255, 256, 269, 273, 282 et 284 CPP.

[583] OBERHOLZER, *Grundzüge des Strafprozessrechts*, p. 545; PIQUEREZ, *Traité*, p. 612.

[584] L'observation à titre préventif, notamment celle destinée à écarter un danger, doit être régie par la législation sur la police : *Message du CF relatif à l'unification de la procédure pénale*, p. 1235.

[585] Pour un avis critique : RUCKSTUHL, *Technische Überwachungen*, p. 150.

[586] Constituent des infractions punissables en tant que telles les actes préparatoires en vue des infractions suivantes suivantes : meurtre (art. 111 CP), assassinat (art. 112 CP), lésions corporelles graves (art. 122 CP), brigandage (art. 140 CP), séquestration et enlèvement (art. 183 CP), prise d'otage (art. 185 CP), incendie intentionnel (art. 221 CP), et génocide (art. 264 CP). En matière d'infractions à la LStup, l'art. 19 ch. 1 al. 6 LStup prévoit que les mesures prises en vue du trafic de stupéfiants sont des délits indépendants. Ils incluent aussi bien la tentative que certains actes préparatoires (ATF 121 IV 198, 200, S., du 19 septembre 1995).

L'existence d'un soupçon présuppose ainsi que l'infraction a déjà été commise et une mesure de surveillance ne doit pas servir à créer un soupçon[587]. 383

Pour certaines mesures, la loi parle de soupçons suffisants[588], de graves soupçons[589] et de forts soupçons[590]. Le soupçon exigé pour justifier l'emploi d'une mesure de surveillance doit être plus important que celui qui permet d'ouvrir une procédure préliminaire[591]. Pour le reste, les différentes terminologies n'impliquent à notre sens rien d'autre que l'application générale du respect du principe de proportionnalité[592]. 384

b) Les infractions poursuivies

Les principes de proportionnalité et de prévisibilité impliquent que le justiciable sache à l'avance dans quels cas une mesure de surveillance peut être ordonnée. Comme il n'est évidemment pas possible de dresser la liste de chaque cas d'espèce, on recourt à une norme générale et abstraite, mais suffisamment précise. Plusieurs possibilités s'offrent au législateur. Il peut définir une liste exhaustive d'infractions, les sélectionner uniquement en fonction de la peine minimale encourue, ou se contenter de critères et principes généraux tels que gravité suffisante et proportionnalité. 385

[587] Par exemple : GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, p. 95; HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 145.

[588] En allemand « ein hinreichender Tatverdacht » et en italien « sufficienti indizi ». Pour les mesures de contrainte en général (art. 197 CPP) et pour l'utilisation de données signalétiques d'un prévenu hors du dossier de la procédure (art. 261 CPP).

[589] En allemand « der dringende Verdacht » et en italien « il grave sospetto ». Pour la surveillance de la correspondance et les autres dispositifs techniques de surveillance (art. 269 CPP), et pour l'obtention des données relatives au trafic, à la facturation et à l'identification des usagers (art. 273 CPP).

[590] En matière de recherches, la loi parle de « fortement soupçonné », respectivement « dringend verdächtigt » dans la version allemande et « sussistano motivi » dans la version italienne (art. 210 CPP).

[591] Si tel n'était pas le cas, les mesures de surveillance seraient automatiquement autorisées pour chaque procédure.

[592] Voir sur la notion de graves soupçons : GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 97-103; HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 141-144.

386 Le législateur n'a toutefois pas adopté une méthode uniforme, puisqu'il n'autorise certains moyens de surveillance que lorsqu'il y a soupçon de commission de certaines infractions, alors que d'autres moyens peuvent être utilisés de manière beaucoup plus large.

387 La surveillance de la correspondance par poste et télécommunication, ainsi que les autres mesures techniques de surveillance ne sont permises que lorsque certaines infractions sont poursuivies. Le législateur en a dressé un catalogue exhaustif à l'art. 269 al. 2 CPP[593]. Il renferme des contraventions, des délits et des crimes[594]. Le recours à une liste exhaustive d'infractions, s'il permet une plus grande prévisibilité, n'est pas toujours accueilli favorablement[595].

[593] On y trouve des infractions au CP : art. 111 à 113, 115, 118 ch. 2, 122, 127, 129, 135, 138 à 140, 143, 144 al. 3, 144bis ch. 1 al. 2 et ch. 2 al. 2, 146 à 148, 156, 157 ch. 2, 158 ch. 1 al. 3 et ch. 2, 160, 161, 163 ch. 1, 180, 181 à 185, 187, 188 ch. 1, 189 à 191, 192 al. 1, 195, 197, 221 al. 1 et 2, 223 ch. 1, 224 al. 1, 226, 227 ch. 1 al. 1, 228 ch. 1 al. 1 à 4, 230bis, 231 ch. 1, 232 ch. 1, 233 ch. 1, 234 al. 1, 237 ch. 1, 238 al. 1, 240 al. 1, 242, 244, 251 ch. 1, 258, 259 al. 1, 260bis à 260^{quinquies}, 261bis, 264 à 267, 271, 272 ch. 2, 273, 274 ch. 1 al. 2, 285, 301, 303 ch. 1, 305, 305bis ch. 2, 310, 312, 314, 317 ch.1, 319, 322ter, 322^{quater}, 322^{septies}; mais également au droit pénal accessoire : art. 116 al. 3 et 118 al. 3 LEtr, art. 24 LF-CLaH, art. 33 al. 2, 34 et 35 LFMG, art. 88 al. 1 et 2, 89 al. 1 et 2, et 90 al. 1LENu, art. 19 ch. 1 2^{e} phrase et ch. 2, et art. 20 ch. 1 2^{e} phrase LStup, art. 60 al. 1 let. g à i, m et o LPE, et art. 14 al. 2 LCB. Cette liste correspond aux infractions permettant de mettre en place une investigation secrète au sens de l'art. 286 CPP : RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, p. 447; ZUFFEREY / BACHER, *Art. 269 CPP*, n. 24-35 ad art. 269. L'avant-projet de révision de la LSCPT prévoit d'ajouter l'art. 220 CP : *Rapport du CF relatif à l'AP LSCPT*, pp 40-41.

[594] Cette liste est reprise de l'ancien art. 3 al. 2 LSCPT. Elle comportait quelques lacunes importantes, qui ont été pour l'essentiel comblées (ajout des art. 129, 135, 139, 143, 144 al. 3, 144bis ch. 2 al. 2, 157 ch. 2, 158 ch. 1 al. 3 et ch. 2, 163 ch. 1, 184, 230bis, 242, 261bis, 267, 271, 272 ch. 2, 273, 274 ch. 1 al. 2, 303 ch. 1, 305, 305bis ch. 2, 317 ch.1, 319 CP, ainsi que des art. 24 LF-CLaH et 33 al. 2 LFMG). Nous ne nous prononcerons pas sur le choix de faire figurer ou non certaines infractions dans le catalogue, ces choix relevant parfois plus de considérations politiques que juridiques. Pour une critique du catalogue d'infractions de la LSCPT, voir notamment : *Rapport du CF à la suite des attentats terroristes du 11 septembre 2001*, p. 1732; HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 160-176; JEAN-RICHARD-DIT-BRESSEL, *Ist ein Millionendiebstahl ein Bagatelldelikt*, pp 60-67; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 124-127. Concernant l'élaboration du catalogue : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 154-160.

[595] Certains auteurs sont opposés à une liste d'infractions, ou souhaitent au moins une clause générale en complément. Voir par exemple dans ce sens : KÜNZLI, *Praktische Probleme bei der Umsetzung des BÜPF*, pp 199-201 et 215. En faveur d'une liste d'infractions, par exemple : GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, p. 116.

La récolte des données relatives au trafic, à la facturation et à l'identification des usagers est possible pour tous les délits et crimes, ainsi qu'en cas d'utilisation abusive d'une installation de télécommunications au sens de l'art. 179^septies CP[596]. Le législateur a renoncé à reprendre le catalogue de l'art. 269 CPP, estimant que l'atteinte est moins grande en matière de récolte de données que lors de l'écoute du contenu de la conversation[597]. Le résultat n'est pourtant pas très heureux, puisque les contraventions figurant dans le catalogue de l'art. 269 al. 2 CPP permettent la surveillance de la correspondance par poste et télécommunication ainsi que les autres mesures techniques de surveillance (soit une atteinte théoriquement plus grande), mais pas la récolte des données relatives au trafic, à la facturation et à l'identification des usagers (soit une atteinte théoriquement moins grande). A l'inverse les délits et crimes ne figurant pas dans le catalogue de l'art. 269 al. 2 CPP peuvent donner lieu à la récolte des données relatives au trafic, à la facturation et à l'identification des usagers, mais ne permettent pas la surveillance de la correspondance par poste et télécommunication ainsi que les autres mesures techniques de surveillance. Les conditions permettant de localiser une personne ne sont ainsi pas les mêmes selon que l'on recourt aux données accessoires, à un IMSI-Catcher, ou à une balise GPS[598]. 388

La surveillance des relations bancaires, l'observation, ainsi que le prélèvement d'un échantillon et l'établissement d'un profil d'ADN, sont admis dans le cas d'un délit ou d'un crime, alors que seule la poursuite d'un crime permet le prélèvement d'échantillons lors d'enquêtes de grande envergure[599]. 389

La récolte de données signalétiques, la récolte d'échantillons d'écriture ou de voix, ainsi que les recherches sont possibles pour n'importe quelle infraction[600]. 390

[596] L'art. 179^septies CP sanctionne une contravention, puisque l'infraction n'est passible que d'une amende (art. 103 CP). Les crimes et délits sont toutes les infractions passibles d'une peine privative de liberté ou d'une peine pécuniaire (art. 10 CP).

[597] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 37-38 et 219.

[598] Voir pour les données accessoires et pour l'IMSI-Catcher le chapitre 3. Les écoutes téléphoniques p. 38 ci-dessus et pour la balise GPS le chapitre 10. La localisation par satellite p. 68 ci-dessus.

[599] Art. 255, 256, 282 et 284 CPP.

[600] Art. 210 et 260 CPP.

La diffusion d'un avis de recherche n'est toutefois autorisée que dans le cas de délits ou de crimes, et non de contraventions (art. 210 al. 2 CPP).

c) La proportionnalité

391 Le seul fait qu'il existe un soupçon de commission d'une infraction qui figure, le cas échéant, dans le catalogue ne suffit pas à justifier le prononcé d'une mesure de surveillance. Encore faut-il que celle-ci soit proportionnée. Pour décider du caractère proportionné ou non d'une mesure de surveillance, il faudra tenir compte de la gravité de l'infraction poursuivie, de l'atteinte que représente la mesure, des chances de succès, de la durée et des modalités de la surveillance, etc. En matière de surveillance de la correspondance, de récolte de données relatives au trafic et à la facturation, d'identification des usagers et d'autres dispositifs techniques de surveillance, la loi rappelle qu'il faut non seulement qu'il existe de graves soupçons que l'infraction visée a été commise, mais encore que la mesure se justifie au regard de la gravité de l'infraction (art. 269 al. 1 lit. a et b CPP)[601]. Pour l'observation, des indices concrets laissant présumer que l'infraction a été commise suffisent (art. 282 al. 1 lit. a CPP). La publication d'un avis de recherche exige, quant à elle, un fort soupçon (art. 210 al. 2 CPP).

392 En matière d'analyse d'ADN, le CPP ne rappelle pas la condition de la proportionnalité. Ce principe doit néanmoins être respecté en application des art. 197 CPP et 36 Cst. Il convient d'y être particulièrement attentif, surtout lors d'enquêtes de grande envergure. Le risque est en effet grand dans ce type d'enquêtes d'établir le profil d'ADN de personnes possédant des caractéristiques spécifiques en lien avec l'infraction poursuivie et de ne pas respecter le sous-principe de la nécessité, plutôt que de se limiter aux personnes pour lesquelles il existe des motifs raisonnables de penser qu'elles sont l'auteur de l'infraction[602].

393 Certains auteurs contestent le fait que plus l'infraction poursuivie est grave, moins les soupçons doivent être importants[603]. S'il est vrai que la gravité de l'infraction doit être prise en compte de manière globale dans l'appréciation de

[601] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 147-152; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 128.
[602] Dans le même sens : ROHMER, *Les enquêtes de grande envergure*, pp 99-102.
[603] Dans ce sens : RUCKSTUHL, *Technische Überwachungen*, pp 153-154.

la proportionnalité, et qu'une infraction grave justifie une plus grande atteinte qu'une infraction légère, la gravité de l'infraction reprochée ne doit pas permettre pour autant de se contenter de vagues soupçons. La loi exige des soupçons suffisants, voire de graves soupçons, et cette exigence minimale doit être respectée.

d) La subsidiarité

Certaines mesures de surveillance sont également subsidiaires. Elles ne peuvent être mises en œuvre que si une mesure moins invasive n'est pas envisageable. Le CPP prévoit ainsi que la surveillance de la correspondance, la récolte de données relatives au trafic, à la facturation, et à l'identification des usagers, ainsi que l'utilisation d'autres dispositifs techniques de surveillance ne peuvent être ordonnées que si les mesures prises jusqu'alors sont restées sans succès ou si les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance (art. 269 al. 1 lit. c CPP)[604]. Il en va de même pour l'observation, même si le CPP utilise une terminologie légèrement différente[605]. Il n'est donc pas nécessaire que toutes les autres mesures envisageables aient été utilisées. Il suffit qu'elles ne puissent raisonnablement pas remplacer la mesure de surveillance envisagée. L'avant-projet de révision de la LSCPT prévoit encore une mesure plus subsidiaire : l'interception et le décryptage de données est une mesure subsidiaire aux mesures de surveillance de la correspondance, ce qui constituerait une double subsidiarité[606]. 394

Aucun ordre de priorité n'est imposé par le CPP dans le choix d'une mesure de surveillance plutôt que d'une autre[607]. Il conviendra alors de choisir, en fonction du cas d'espèce, la mesure qui représente l'atteinte la moins grande. 395

[604] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 152-154; SCHMID, *Praxiskommentar*, pp 505-506.

[605] L'art. 282 al. 1 lit b prévoit que l'observation n'est admissible que si d'autres formes d'investigations n'auraient aucune chance d'aboutir ou seraient excessivement difficiles. Il n'est pas question ici de l'échec des mesures ordonnées précédemment, peut-être parce que l'observation est souvent une des premières mesures à être ordonnée.

[606] Art. 270bis CPP introduit par l'AP LSCPT, *Rapport du CF relatif à l'AP LSCPT*, pp 42-43.

[607] L'échec d'une surveillance de la correspondance ou des conditions supplémentaires pour l'utilisation de dispositifs de surveillance ou le cumul d'une surveillance de la correspondance et de dispositifs visuels ou sonores est suggérée par certains auteurs. Voir par exemple : GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 116-117.

e) Les autres conditions

396 En matière de recherches, l'art. 210 CPP pose la double condition que le lieu de séjour de la personne recherchée soit inconnu et que sa présence soit nécessaire au déroulement de la procédure.

397 La récolte de données signalétiques, ainsi que d'échantillons d'écriture ou de voix, n'est soumise à aucune condition particulière. Seule l'utilisation des données signalétiques d'un prévenu hors du dossier de la procédure exige qu'il existe des soupçons suffisants laissant présumer une récidive (art. 261 CPP).

D. Le moment de la surveillance

3. Le début

398 La mesure débute au moment où elle est ordonnée. C'est la décision du ministère public qui est déterminante, respectivement celle de la police si elle est compétente, que la décision soit soumise ou non à l'autorisation du tribunal des mesures de contrainte. Si ce dernier n'autorise pas la surveillance, elle est réputée n'avoir pas existé et aucune information recueillie durant cette surveillance non autorisée ne peut être utilisée.

399 Lorsqu'aucune décision du ministère public n'est exigée, le début de la surveillance correspond au moment où l'avis de recherche est émis ou lorsque la surveillance commence. L'observation ne débute pas au moment où elle est ordonnée, mais à l'instant où elle commence effectivement[608]. Une période de suspension de l'observation, comme des autres mesures de surveillance, n'en prolonge pas d'autant la durée totale autorisée[609].

[608] Le début effectif de l'observation est déterminant, et non d'éventuels préparatifs : RHYNER / STÜSSI, *Kommentar zu Art. 282-283 StPO*, p. 477.

[609] *Message du CF relatif à l'unification de la procédure pénale*, p. 1236; RHYNER / STÜSSI, *Kommentar zu Art. 282-283 StPO*, p. 478 et le résumé des discussions au Conseil National mentionné en note; SCHMID, *Praxiskommentar*, p. 536.

Pour ce qui est de la surveillance des relations bancaires, elle ne devrait débuter qu'avec l'autorisation du tribunal des mesures de contrainte puisqu'il lui revient d'en définir les modalités d'exécution[610]. Comme mentionné précédemment, cette situation n'est pas satisfaisante et l'on devrait plutôt retenir, par analogie avec la surveillance de la correspondance, que la surveillance débute avec la décision du ministère public. En matière de données relatives au trafic, à la facturation et à l'identification des usagers, les données des six derniers mois peuvent être demandées[611]. Le texte clair de la loi ne permet pas d'obtenir des données plus anciennes, même si elles sont disponibles (art. 273 al. 3 CPP). La loi ne prévoit en revanche pas de durée maximale pour les relations bancaires. 400

4. La fin

Une mesure de surveillance prend notamment fin à l'échéance de la durée autorisée, parce que l'autorisation nécessaire n'a pas été obtenue, parce qu'elle n'est techniquement plus réalisable ou parce que le but de la surveillance est atteint et qu'elle n'est plus nécessaire[612]. S'agissant de la surveillance de la correspondance et de l'utilisation d'autres dispositifs de surveillance, le ministère public lève la surveillance et en informe le tribunal des mesures de contrainte (art. 275 CPP). Ce devoir d'information ne crée pas pour autant un devoir, ni même un droit, de surveillance du tribunal des mesures de contrainte. Il serait pourtant judicieux que le tribunal des mesures de contrainte ne se contente pas d'autoriser la surveillance, mais contrôle qu'elle est exécutée fidèlement, notamment quant à ses modalités et sa durée. Il y aurait ainsi une obligation pour le ministère public non seulement de démontrer avant la surveillance que les conditions sont remplies, mais également après, qu'elle a été exécutée correctement. En l'état, la seule sanction possible peut intervenir en cas de recours de la personne surveillée, soit après la fin de la surveillance. 401

[610] *Message du CF relatif à l'unification de la procédure pénale*, p. 1237.

[611] L'avant-projet de révision de la LSCPT veut allonger à 12 mois la durée de conservation des données (art.19 et 23 AP LSCPT) : *Rapport du CF relatif à l'AP LSCPT*, pp 29, 33-34 et 45. Le rapport ne démontre pas que cet allongement est nécessaire et encore moins qu'il est conforme au principe de proportionnalité.

[612] Sur ces différents cas de figure : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 307-310; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 175-176.

402 La police et le Service SCPT doivent également mettre un terme à la surveillance lorsque la durée autorisée est atteinte, sans qu'un ordre du ministère public soit nécessaire (art. 11 al. 1 lit. d LSCPT)[613].

E. L'exécution de la surveillance

403 Les mesures de surveillance sont en principe exécutées par la police, à moins que leur nature ne requière la collaboration de tiers. C'est en particulier le cas pour la surveillance des relations bancaires, où l'établissement bancaire exécute la surveillance selon les directives du tribunal des mesures de contrainte (art. 285 CPP), ou lors de prélèvements d'ADN dont l'exécution peut être confiée au personnel médical.

404 En matière de surveillance de la correspondance également, la surveillance n'est pas opérée directement par la police. L'exécution de la surveillance est réglée par la LSCPT[614]. La Confédération exploite un Service chargé de la surveillance de la correspondance par poste et télécommunication, appelé Service SCPT[615]. Ce service accomplit ses tâches de manière autonome. Il coordonne les mesures de surveillance ordonnées par des autorités d'instruction et les transmet aux fournisseurs de services de poste et de télécommunication[616]. Il est administrativement rattaché au Département fédéral de justice et police (DFJP). Le Service SCPT a aussi les compétences et les moyens techniques pour effectuer directement des mesures de surveillance, par exemple lorsque le fournisseur de services n'est pas à même d'assumer cette prestation[617]. La

613 HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 336.

614 Sur l'exécution de la surveillance de la correspondance par poste et télécommunication : AELLEN / HAINARD, *Secret professionnel et surveillance des télécommunications*; HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 66-68, 179-180 et 409-410; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 154-159.

615 Voir la note de bas de page n° 534 ci-dessus.

616 Sur les obligations des fournisseurs de services postaux : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 339-341; PIQUEREZ, *Traité*, pp 623-624; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 118 et 155-156. Sur les obligations des fournisseurs de services de télécommunications : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 351-371; PIQUEREZ, *Traité*, p 624; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 119 et 158.

617 C'est particulièrement le cas pour les petits fournisseurs d'accès internet ou les réseaux de téléphonie internes.

police peut également utiliser une infrastructure privée déjà existante comme une installation de vidéosurveillance[618].

F. L'information

1. Les différentes formes d'information

L'information préalable, ou le caractère reconnaissable de la surveillance, est une des conditions de sa validité lorsque la surveillance est soumise à la Loi fédérale sur la protection des données (LPD). Les lois cantonales prévoient en principe les mêmes exigences. Cette loi impose que la collecte de données soit reconnaissable, de même qu'elle oblige le maître du fichier à informer la personne concernée lorsque la collecte porte sur des données sensibles (art. 14 LPD)[619]. Les mesures de surveillance concernées par le CPP ne sont pas soumises à la LPD. C'est d'ailleurs souvent parce que la personne surveillée n'a pas connaissance de l'existence de la surveillance que les résultats obtenus sont utiles[620]. 405

Celui qui s'estime surveillé pourrait essayer de demander la confirmation de ses soupçons. Il lui sera bien difficile de trouver à qui s'adresser puisque la procédure pénale ne prévoit pas de service centralisé pour répondre à cette question et l'un ou l'autre juge saisi de la question se réfugiera derrière le secret de l'enquête. Tout au plus la direction de la procédure pourrait rassurer, dans des cas particuliers, une partie à la procédure qu'elle n'est à ce moment précis pas l'objet d'une surveillance ordonnée par elle-même. 406

[618] MÉTILLE, *L'utilisation privée de moyens techniques de surveillance*.

[619] *Message du CF relatif à la révision de la LPD*, p. 1924. Pour être parfaitement conforme au droit européen et aux recommandations du Conseil de l'Europe, le devoir d'information visé à l'art. 14 aurait dû être retenu pour la collecte de toutes les données personnelles (et pas seulement des données sensibles) : *Message du CF relatif à la révision de la LPD*, p. 1937. A noter que la diposition de l'art. 14 figurait à l'art. 7a jusqu'à l'entrée en vigueur de la Loi fédérale du 19 mars 2010 portant mise en œuvre de la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (FF 2010 1933). Un alinéa 5 permettant de différer cette information a été ajoutée à cette occasion.

[620] C'est le contraire en matière de surveillance dissuasive, où l'effet principal est obtenu parce que l'individu adopte un comportement différent parce qu'il a connaissance de la surveillance.

407 Le législateur a prévu une obligation d'informer lorsque la surveillance est basée sur le CPP, appelée communication (art. 279 CPP). Une information spontanée n'existe pas dans le cas d'une surveillance préventive prévue par la LMSI[621].

2. Les mesures concernées

408 Le CPP prévoit l'information de la personne surveillée en cas de surveillance de la correspondance par poste et télécommunication, de récolte de données relatives au trafic, à la facturation et à l'identification des usagers, d'utilisation d'autres dispositifs techniques de surveillance, de la surveillance des relations bancaires et d'observation[622]. Même si cela ne ressort pas directement du texte légal, une telle information devrait aussi avoir lieu pour l'interception et le décryptage de données (art. 270bis CPP) et l'utilisation de systèmes de localisation (art. 270ter CPP), prévus par l'avant-projet de révision de la LSCPT[623].

409 La communication de mesures restées jusqu'alors secrètes est nécessaire pour permettre un recours effectif au sens de l'art. 13 CEDH[624]. La communication doit intervenir dans tous les cas, c'est-à-dire indépendamment des résultats obtenus par la mesure de surveillance et de leur éventuelle utilisation à titre de preuves[625]. L'information doit permettre de contrôler les conditions de surveillance et elle est d'autant plus nécessaire que les atteintes portées aux libertés individuelles ne sont le plus souvent pas connues durant la surveillance. Le fait que la surveillance n'était pas autorisée, et que les résultats obtenus ne puissent être utilisés ne justifie pas de renoncer à l'information, bien au

[621] Le législateur a dû prévoir une procédure permettant de se renseigner sous la forme d'un droit d'accès indirect étant donné qu'il n'y a ni information spontanée, ni procédure d'autorisation.

[622] Art. 279 et 284 CPP. Sur la situation dans les cantons avant l'entrée en vigueur de la LSCPT : SCHMID, *Die nachträgliche Mitteilung (1)*, p. 38.

[623] Art. 270bis CPP et art. 270ter CPP ajouté par l'AP LSCPT, *Rapport du CF relatif à l'AP LSCPT*, p. 43.

[624] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 310; OBERHOLZER, *Grundzüge des Strafprozessrechts*, p. 563; PIQUEREZ, *Traité*, p. 627. Le Conseil fédéral considère l'obligation de communiquer comme étant de nature constitutionnelle : *Message du CF relatif à la LMSI II*, p. 4838.

[625] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 310.

contraire[626]. Surveiller un individu constitue déjà une atteinte aux droits de l'individu, indépendamment de l'exploitation des résultats de la surveillance[627]. Pour celui qui surveille également, le risque qu'un contrôle *a posteriori* puisse avoir lieu même si les résultats de la surveillance ne sont pas utilisés en tant que preuve le pousse à respecter la procédure dans tous les cas, et non seulement dans l'hypothèse où il serait contraint de déposer au dossier de la cause les éléments qu'il a obtenu par le biais d'une surveillance[628].

A noter qu'aucune information n'est prévue en matière de recherches, de récolte d'échantillons d'écriture, de voix, d'ADN, ou de données signalétiques. Ces mesures n'étant pas secrètes, une information est inutile puisqu'elle a déjà lieu sur le moment. En revanche, si ces récoltes de données devaient se faire à l'insu de la personne concernée, ce qui est techniquement facile à réaliser, il faudrait alors appliquer les art. 280ss CPP et considérer qu'il s'agit d'un autre dispositif technique de surveillance. On retrouverait alors l'obligation d'informer la personne concernée[629]. 410

3. Le moment et la forme de la communication

Le CPP prévoit que le ministère public communique au plus tard lors de la clôture de la procédure préliminaire les motifs, le mode et la durée de la surveillance. Sur le fond, le CPP a repris le contenu de l'ancien art. 10 al. 2 à 6 LSCPT. Cet article prévoyait une communication « au plus tard lors de la clôture de la procédure pénale ou de la suspension de la procédure ». Il se pouvait alors que la personne surveillée n'apprenne l'existence de la mesure de surveillance qu'après la clôture de la phase préliminaire, ce qui n'est désormais plus conforme. Cette communication devrait cependant intervenir avant et non 411

[626] Dans le même sens : SCHMID, *Die nachträgliche Mitteilung (1)*, p. 40. Pour un avis contraire HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 311.

[627] Considérer que la surveillance sans exploitation des résultats ne constitue pas une atteinte permettrait à chacun de surveiller des tiers juste pour le plaisir, à la condition de ne pas exploiter les résultats dans le cadre d'une procédure judiciaire.

[628] On permettrait sinon à la police de mettre en place des mesures de surveillance illégales pour obtenir des informations qui lui permettraient de récolter d'autres preuves qui apparaîtraient comme recueillies légalement, par exemple un aveu. Une telle situation serait choquante.

[629] L'obligation d'informer concerne n'importe quel type de surveillance et vaut quelle que soit la nature de la décision qui met fin à la procédure : PIQUEREZ, *Traité*, p. 627.

pas lors de la clôture de la procédure préliminaire, de sorte que le prévenu puisse prendre encore position sur les résultats de la surveillance dans le cadre de la procédure préliminaire[630].

412 La compétence revient au ministère public, même s'il s'agit d'une observation ordonnée par la police ou d'une surveillance des relations bancaires ordonnée par le tribunal des mesures de contrainte. Le CPP ne précise pas comment cette communication doit avoir lieu. La forme écrite est pourtant souhaitable[631].

413 Le droit d'accès au dossier qui permet aux parties de prendre connaissance de l'autorisation et des résultats de la surveillance n'est pas suffisant[632] . Cette manière de procéder, bien que fréquente, n'est pas conforme et une vraie information au sens de l'art. 279 CPP est nécessaire. L'accès au dossier doit permettre au prévenu de préparer correctement sa défense, alors que la communication de la surveillance sert notamment à vérifier que les conditions de surveillance et les droits de la personne surveillée ont été respectés. La personne surveillée a intérêt à connaître dès que possible qu'elle a été l'objet d'une surveillance. L'accès au dossier, notamment lorsque le prévenu a déjà eu connaissance des pièces du dossier, ne justifie pas toujours une consultation immédiate. Il est dicté par les échéances procédurales. Finalement, le droit d'accès au dossier ne doit pas se transformer en un oreiller de paresse pour le ministère public et une obligation pour le prévenu d'examiner le dossier pour y trouver l'éventuelle trace d'une surveillance. Il ne faut pas perdre de vue que le prévenu n'est pas toujours assisté d'un mandataire professionnel et qu'il ne maîtrise souvent ni le droit ni la langue de la procédure. Le dossier peut en outre être volumineux et les parties ne sont pas informées à chaque fois qu'une nouvelle pièce est ajoutée.

414 Par ailleurs, le fait que le prévenu puisse déduire l'existence d'une surveillance des questions qui lui sont posées lors d'un interrogatoire par la police ou le

[630] Dans le même sens : HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 312.

[631] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 315.

[632] Pas plus l'information donnée lors d'un interrogatoire : ATF 1P.15/2003 du 14 février 2003, consid. 2.

ministère public ne suffit pas à remplacer une information, même si cela arrive souvent souvent en pratique[633].

4. Le contenu de la communication

L'art. 279 CPP n'énumère pas ce qui doit figurer dans la communication[634]. On devrait y trouver la mention de la personne contre laquelle la procédure pénale est dirigée et les infractions présumées, les motifs, le genre et la durée de la surveillance, l'autorisation et les conditions auxquelles elle a été accordée, ainsi qu'une référence aux voies de droit[635]. Le sort réservé aux données recueillies devrait aussi être précisé. 415

Le prévenu surveillé pourra prendre connaissance du dossier de sa cause, en application du droit d'accès au dossier (découlant directement du droit d'être entendu). Il aura ainsi connaissance de la surveillance et tous les éléments servant de preuve y figureront. Cela n'est cependant pas suffisant, puisqu'il devrait avoir également accès aux éléments écartés, voire aux résultats de surveillance qui ne serviront pas de preuve[636]. Il en va de même pour la personne surveillée qui n'aurait pas la qualité de partie à la procédure, puisqu'elle ne bénéficie pas d'un droit d'accès au dossier. Les seules informations qu'elle aura sont celles liées à la communication et aux droits qui en découlent. Elle doit être informée de manière complète et compréhensible sur les raisons qui ont conduit à sa surveillance[637]. 416

D'un côté, l'information devrait être complète et permettre à la personne surveillée de connaître l'intégralité des informations recueillies, mais aussi des éléments qui ont conduit à la mise en place de la surveillance. C'est l'unique moyen pour la personne surveillée de contrôler si la décision prise était justifiée et si un recours s'impose dans le cas contraire. D'un autre côté, une difficile 417

633 ATF 1P.15/2003 du 14 février 2003, consid. 2 et RUCKSTUHL, *Technische Überwachungen*, p. 151; SCHMID, *Praxiskommentar*, p. 525.

634 Sur le contenu en fonction du destinataire : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 313-315.

635 SCHMID, *Praxiskommentar*, p. 525.

636 Cela pose d'ailleurs un bon nombre de problèmes en pratique, puisque certaines autorités policières ne joignent pas au dossier officiel tous les éléments recueillis, mais seulement ceux qu'elles jugent utiles comme preuves dans la procédure pénale.

637 ATF 8G.109/2003 du 21 octobre 2003, consid. 3.

pesée d'intérêts naît puisqu'il y a lieu de tenir compte de la protection de la sphère privée d'autres personnes concernées. Le dossier renfermera généralement des données personnelles sur des tiers. Dans ces circonstances, l'information doit permettre à la personne de comprendre les raisons qui ont conduit à la surveillance et indiquer qu'elle a le droit de consulter le dossier. Le droit de prendre connaissance des données recueillies est alors respecté, et l'atteinte à la sphère privée des tiers est réduite. Il revient au ministère public de décider quels détails doivent figurer dans la communication. Celle-ci devrait également indiquer le droit de consulter le dossier et les voies de recours[638].

5. Le destinataire

418 En matière d'observation, le CPP prévoit que la personne qui a été observée doit être informée. Pour les autres mesures, le code parle du prévenu ainsi que du tiers qui ont fait l'objet d'une surveillance.

419 Le correspondant de la personne surveillée n'a pas à être informé[639]. En plus des problèmes pratiques que cela poserait, l'information de tous les correspondants aurait très souvent des conséquences désagréables pour la personne contre laquelle est dirigée la surveillance. Cela revient en effet à informer toutes les personnes qui ont été en contact avec elle qu'une procédure pénale est en cours et que les infractions reprochées sont d'une gravité telle que des mesures techniques de surveillance se justifiaient[640]. Le droit de chacun d'être informé d'une atteinte à sa sphère privée s'oppose ici à la protection de la sphère privée de la personne principalement visée par la surveillance[641]. Une priorité absolue ne devrait pas être accordée définitivement à l'un ou à l'autre, mais il convient bien plus de procéder à une pesée d'intérêts et de tenir compte de l'intensité de la surveillance.

---

[638] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 315-316.

[639] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 317; HAUSER / SCHWERI / HARTMANN, *Schweizerisches Strafprozessrecht*, p. 361. En faveur d'une information large, y compris du détenteur du raccordement téléphonique surveillé, même s'il ne l'a pas utilisé personnellement : SCHMID, *Die nachträgliche Mitteilung (1)*, pp. 40-41.

[640] Dans le même sens : SCHWOB, *Die nachträgliche Mitteilung (2)*, p. 167.

[641] Un parallèle peut être fait avec l'application du principe de transparence à l'activité de l'administration et la protection de la sphère privée de l'administré lorsque la première a traité des données personnelles du second. Voir à ce sujet : FLÜCKIGER, *Le conflit entre le principe de transparence et la protection de la sphère privée.*

Dans les cas d'un correspondant très régulier, la situation devrait selon toute vraisemblance être étudiée de la même manière que celle d'un tiers utilisant régulièrement l'objet de la surveillance. La fréquence d'utilisation peut constituer une augmentation sensible de l'atteinte et justifie, au regard du principe de la proportionnalité, une décision différente de celle prise concernant un simple correspondant occasionnel. Le correspondant régulier devrait aussi recevoir une communication et avoir la possibilité de déposer un recours. 420

6. L'exception

Le ministère public peut renoncer à la communication ou la différer si les informations recueillies ne sont pas utilisées à des fins probatoires et si cela est indispensable pour protéger des intérêts publics ou privés prépondérants. L'accord du tribunal des mesures de contrainte est exigé, sauf en matière d'observation où le ministère public peut décider seul[642]. Le CPP ne précise pas de quelle manière le ministère public doit procéder pour obtenir l'accord du tribunal des mesures de contrainte. En cas de refus de ce dernier, le ministère public n'a pas de possibilité de recourir (art. 393 al. 1 lit. c CPP). Il n'existe aucune autorité chargée de surveiller si l'information a lieu ou si une exception à la communication est obtenue. 421

Pour le Conseil fédéral, le CPP correspond à la réglementation en vigueur sous l'empire de la LSCPT[643]. A y regarder de plus près, la LSCPT prévoyait trois exceptions : la protection d'intérêts publics prépondérants, un risque sérieux de mise en danger de tiers ou l'impossibilité d'atteindre la personne concernée[644]. Même si ce cas de figure n'a pas été repris dans le CPP, nous pouvons néanmoins admettre que l'on puisse renoncer à informer la personne qui ne peut raisonnablement pas être atteinte. La question demeure ouverte de savoir si le ministère public peut y renoncer de lui-même ou si, par analogie avec les dispositions appliquées avant le CPP, il doit avoir l'accord du tribunal des mesures de contrainte. 422

[642] Art. 279 et 283 CPP.

[643] *Message du CF relatif à l'unification de la procédure pénale*, p. 1233.

[644] Pour des exemples d'intérêts prépondérants (avant l'introduction de la LSCPT, mais applicables *mutatis mutandis*) : SCHMID, *Die nachträgliche Mitteilung (1)*, pp 42-43.

423 Le CPP regroupe les intérêts privés et publics prépondérants et rappelle que les informations recueillies ne doivent pas être utilisées à des fins probatoires si la communication est différée ou que le ministère public y renonce. Cette condition ne sera pas une nouveauté lors de l'entrée en vigueur du CPP, même si elle ne figurait pas expressément dans la LSCPT. Elle découle du droit d'être entendu et du droit du prévenu à avoir un accès complet à son dossier[645]. Il s'agit d'une interdiction absolue.

424 Le ministère public ne doit en revanche pas pouvoir simplement renoncer à utiliser les informations obtenues comme preuves dans la procédure seulement pour éviter d'informer la personne surveillée[646]. L'information doit également avoir lieu si les informations recueillies ne servent pas de preuve ou si la surveillance n'a donné aucun résultat. Admettre le contraire permettrait aux autorités de poursuite d'opérer des surveillances à l'insu de la personne surveillée, d'utiliser les informations recueillies pour obtenir d'autres preuves voire des aveux et finalement de supprimer toutes traces de la surveillance initiale.

425 Il se justifie de différer l'information lorsqu'une autre procédure pénale est en cours et que son aboutissement serait compromis, qu'il s'agisse de coauteurs ou d'une autre procédure dirigée contre la même personne, ou que la surveillance n'a pas donné de résultats et qu'elle a été abandonnée, mais que de forts soupçons subsistent et qu'une nouvelle surveillance sera mise en place prochainement[647]. Le fait de différer ou renoncer à l'information ne doit pas servir à empêcher le recours de la personne surveillée[648].

426 Si le ministère public doit recueillir l'accord du tribunal des mesures de contrainte pour différer ou renoncer à une communication, il peut en revanche décider librement du cercle des personnes qui recevront la communication. Mis à part dans le cas de la personne principalement visée par la surveillance, soit généralement le prévenu, le ministère public pourrait considérer que la

[645] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p.317.

[646] Déjà dans le même sens : SCHWOB, *Die nachträgliche Mitteilung (2)*, p. 167.

[647] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 320-321.

[648] Un tel recours devrait être considéré comme recevable. Voir à ce sujet le chapitre G. Le contrôle *a posteriori*, p. 189 ci-dessous et en particulier la note de bas de page n° 660.

communication n'est pas nécessaire. Il se dispenserait ainsi de l'accord du tribunal des mesures de contrainte et personne ne pourrait s'y opposer. Il manque donc une autorité de contrôle. L'autorité de recours pourrait par exemple se voir notifier systématiquement une copie de l'autorisation de surveillance et des communications. Elle pourrait vérifier à réception d'une communication qu'il n'y avait personne d'autre à informer. Périodiquement, elle pourrait s'inquiéter du sort réservé aux dossiers pour lesquels elle n'a pas reçu de communication et en vérifier le bien-fondé. Ce contrôle devrait être effectivement mené, car il ne sert à rien d'instaurer une instance supplémentaire dont l'activité resterait théorique.

G. Le contrôle *a posteriori*

1. Au niveau cantonal

a) Les mesures concernées

Au sens de l'art. 393 CPP, la voie du recours est ouverte de manière générale contre les décisions et les actes de procédure de la police et du ministère public[649]. Il s'agit notamment des ordonnances prescrivant des mesures de contrainte. Les décisions du tribunal des mesures de contrainte sont en principe définitives[650]. Un recours peut seulement être déposé contre les décisions du tribunal des mesures de contrainte si le code le prévoit expressément. C'est le cas après la communication de la surveillance en matière de surveillance de la correspondance[651], de surveillance des relations bancaires[652], d'utilisation d'autres dispositifs techniques de surveillance[653] et d'observation[654]. Il ne s'agit 427

[649] PIETH, *Schweizerisches Strafprozessrecht*, pp 229-231. Sur les voies de recours avant l'entrée en vigueur du CPP, voir par exemple : STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 184-190.

[650] *Message du CF relatif à l'unification de la procédure pénale*, p. 1296.

[651] Art. 279 al. 3 CPP.

[652] Le droit de recours est expressément prévu à l'art. 285 al. 4 CPP, bien que le message du Conseil fédéral ne le mentionne pas : *Message du CF relatif à l'unification de la procédure pénale*, p.1296.

[653] Art. 279 al. 3 CPP, par renvoi de l'art. 281 al. 4 CPP.

pas à proprement parler d'un recours contre une décision du tribunal des mesures de contrainte, mais plutôt d'un recours suite à la communication et dont le but est de contrôler *a posteriori* l'ensemble de la surveillance.

428 Le Tribunal fédéral a confirmé, sous l'angle de la LSCPT, qu'un recours contre une décision autorisant la surveillance déposé avant la communication de celle-ci était irrecevable parce que le délai de recours n'avait pas encore commencé à courir[655]. Le tribunal voulait vraisemblablement éviter de devoir se prononcer sur une surveillance en cours[656]. Le Tribunal fédéral a rappelé que la décision autorisant (ou refusant) la surveillance est par nature une décision non susceptible de recours[657]. Il considère qu'en cas de refus de l'autorisation, il n'y a aucun intérêt à communiquer la décision à d'autres personnes que l'autorité qui a ordonné la surveillance. Si la surveillance est autorisée, le caractère secret de la surveillance empêche de communiquer la décision aux personnes surveillées. Le Tribunal fédéral relève que le contrôle juridique de la surveillance au début de la procédure est par nature limité et que le juge compétent pour donner son approbation examine seul, pour garantir la confidentialité de la mesure, tous les intérêts en jeu à ce stade-là. Il lui appartient de prendre également en compte les intérêts des personnes visées, qu'il représente en quelque sorte puisqu'elles ne peuvent pas participer à la procédure[658]. Cette jurisprudence distingue ainsi le contrôle limité *a priori* du contrôle plus complet *a posteriori*. Le Tribunal fédéral ne s'est pas penché sur le cas où la personne surveillée aurait des soupçons voire aurait connaissance de

[654] Art. 283 CPP. La possibilité de déposer un recours n'est pas mentionner dans le texte de la loi, mais la communication perd tout son sens si la mesure n'est pas contestable devant une autorité judiciaire.

[655] ATF 1P.15/2003 du 14 février 2003, et HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 323 et 328. Si cette solution évite à l'autorité de recours de se prononcer lorsqu'une surveillance est en cours et d'indiquer au prévenu s'il fait ou non l'objet d'une surveillance, elle est problématique car elle l'empêche de faire valoir ses droits avant la fin de la surveillance, et de l'atteinte qu'il estime injustifiée.

[656] Dans le même sens, le CPP ne prévoit pas un recours contre la décision ordonnant ou autorisant la surveillance en tant que telle, mais la possibilité d'interjeter un recours après avoir reçu la communication (art. 279 al. 3 CPP). D'une certaine manière, le recours est dirigé contre l'utilisation possible des résultats de la surveillance litigieuse, plutôt que contre l'autorisation de la surveillance elle-même. La surveillance en tant que telle constitue pourtant déjà une atteinte.

[657] ATF 133 IV 182, 183-187, Ministère public de la Confédération, du 15 mars 2007.

[658] ATF 133 IV 182, 185, Ministère public de la Confédération, du 15 mars 2007.

la surveillance indépendamment de la procédure d'autorisation. Un recours constitutionnel subsidiaire devant le Tribunal fédéral ne serait pas plus recevable qu'un recours en matière pénale[659].

La position du Tribunal fédéral ne peut pas être suivie, puisqu'il existe des cas où il peut être renoncé à une communication. La personne surveillée, si elle a connaissance d'une mesure de surveillance, doit pouvoir immédiatement en faire contrôler le bien-fondé. On ne peut pas exiger d'elle qu'elle attende de recevoir une communication, alors qu'elle ne sait pas quand celle-ci interviendra et même si elle interviendra. Ce sera tout de même un contrôle *a posteriori*, même si il est légèrement anticipé. Le Conseil fédéral semble partager cet avis, même si ce dernier ne ressort pas du CPP[660]. De la même manière, le recours ne devrait pas seulement être ouvert à la personne contre qui la surveillance était dirigée comme le prévoit l'art. 279 al. 3 CPP, mais à toute personne surveillée, même accessoirement[661]. 429

De manière générale, tout acte de procédure peut faire l'objet d'un recours, y compris toute abstention ou toute omission[662]. Une décision écrite n'est pas nécessaire et le fait qu'une autorisation ultérieure du tribunal des mesures de contrainte puisse devoir être accordée ne semble pas s'opposer à un recours. Il est envisageable, du moins théoriquement, de recourir contre un acte d'exécution de la surveillance. Ce recours sera probablement rejeté au fond, pour autant encore qu'il soit jugé recevable, puisque son objet sera limité à vérifier que la police a agi conformément à la requête du ministère public ou 430

[659] L'irrecevabilité est premièrement liée, selon le Tribunal fédéral, au fait que le délai n'a pas commencé à courir. Le recours constitutionnel subsidiaire n'est en outre pas ouvert lorsque les conditions de recevabilité des recours ordinaires ne sont pas remplies s'agissant du type de décision : DONZALLAZ, *Commentaire LTF*, p. 1635.

[660] Alors que le projet de CPP était en discussion devant les Chambres, le Conseil fédéral a relevé dans le message concernant l'ajout de moyens spéciaux de recherche d'informations dans la LMSI que si la personne surveillée n'est pas informée « que des informations la concernant ont été récoltées grâce à de tels moyens, celle-ci ne pourra en général pas l'attaquer, à moins qu'elle n'en ait eu connaissance par une autre voie (…) comme lors de procédures pénales ». Cela signifie que le Conseil fédéral admet qu'un recours puisse être déposé même en l'absence de communication : *Message du CF relatif à la LMSI II*, p. 4838.

[661] Dans le même sens, retenant que toute personne qui a utilisé un raccordement surveillé est légitimée à recourir : BIEDERMANN, *BÜPF*, p. 102. Pour un avis contraire : HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 323.

[662] *Message du CF relatif à l'unification de la procédure pénale*, p. 1296.

l'autorisation du tribunal des mesures de contrainte. Cette requête ou cette autorisation ne pouvant précisément pas être attaquée selon la jurisprudence du Tribunal fédéral, elle ne sera pas contestable par le biais d'un acte d'exécution. Une requête pourrait en revanche être déposée devant la Cour européenne des droits de l'homme en invoquant le droit à un recours effectif garanti par l'art. 13 CEDH.

431 Dans une affaire liée à la saisie de matériel de propagande, le Tribunal fédéral avait admis la recevabilité d'un recours bien que le texte clair de la Loi d'organisation judiciaire[663] (OJ) alors en vigueur l'excluait expressément. Le Tribunal avait retenu qu'en vertu de l'art. 6 CEDH le recourant devait pouvoir porter le litige devant une autorité judiciaire indépendante et que le droit international primait sur le droit national contraire[664]. En suivant ce raisonnement, et pour autant que l'on admette l'exigence d'un contrôle judiciaire indépendant *a priori* également lorsque le contrôle *a posteriori* est judiciaire et indépendant, le Tribunal fédéral devrait entrer en tout temps en matière sur un recours déposé contre une mesure de surveillance en cours[665].

432 Le prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure au sens de l'art. 256 CPP semble échapper à tout contrôle par le biais du recours cantonal. Cette mesure est en effet ordonnée par le tribunal des mesures de contrainte et le code ne mentionne pas que la voie du recours est ouverte. Il faudrait alors saisir directement le Tribunal fédéral. Ce cas de figure est surprenant car la compétence du tribunal des mesures de contrainte est justifiée par le fait que l'atteinte est plus importante puisque les personnes dont l'ADN est prélevé ne sont pas formellement soupçonnées[666]. Si la décision ordonnant le prélèvement d'ADN ne peut pas être attaquée, l'acte de la police y procédant pourrait éventuellement l'être. Il risque toutefois d'être couvert par la décision du tribunal des mesures de contrainte. L'exigence du double degré de juridiction rappelé à l'art. 80 al. 2 LTF n'étant pas respectée, la loi a été modifiée avant

[663] OJ, RO 1948 473.

[664] ATF 125 II 417, 420 et 426, A., du 26 juillet 1999.

[665] Dans cette hypothèse, le Tribunal fédéral n'écarterait pas un texte de droit interne car contraire au droit supérieur, mais sa propre jurisprudence.

[666] *Message du CF relatif à l'unification de la procédure pénale*, p. 1224.

même l'entrée en vigueur du CPP pour exclure les décisions du tribunal des mesures de contrainte de l'exigence du double degré de juridiction[667].

Cette situation n'est pas satisfaisante, et vraisemblablement pas conforme à l'idée initiale du législateur[668]. En matière de surveillance, il a voulu ouvrir largement le contrôle des mesures de contrainte, puisque tous les actes de la police et du ministère public sont sujets à recours. Il faut dès lors admettre l'existence d'une lacune. Cela est confirmé également par le fait que dans d'autres domaines, le code prévoit expressément que le tribunal des mesures de contrainte statue définitivement, excluant ainsi un recours[669]. Cette lacune doit être comblée en admettant, par analogie avec les autres mesures de surveillance ordonnées par le tribunal des mesures de contrainte et malgré le texte clair de la loi, qu'un recours cantonal peut être déposé également en matière de prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure. La décision ordonnant de se soumettre au prélèvement est assimilée à la communication. La modification de l'art. 80 al. 2 LTF ne s'y oppose pas et c'est le seul moyen d'exercer un contrôle judiciaire. SCHMID considère, en s'appuyant sur des procès-verbaux de commissions, qu'un recours contre la décision générale autorisant le prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure n'est pas recevable, mais qu'un recours est en revanche recevable contre l'ordre ordonnant à un individu précis de s'y soumettre[670]. 433

[667] La Loi sur l'organisation des autorités pénales (LOAP) adoptée le 19 mars 2010 a modifié les art. 80 al 2 LTF et 222 CPP : FF 2010 1881 et 1883. Voir aussi le *Message du CF relatif à la LOAP*, p. 7426. Sur l'exigence du double degré de juridiction : AUER, *Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht*, pp 126-128; KUHN / PERRIER, *Quelques points problématiques du CPP*; SCHMID, *Die Strafrechtsbeschwerde*, pp 166-171.

[668] *Message du CF relatif à la LOAP*, p. 7426.

[669] C'est le cas en matière de garantie de l'anonymat (art. 150 al. 2 CPP) et d'hospitalisation à des fins d'expertise (art. 186 al. 2 CPP, qui précise également que le tribunal statue en procédure écrite).

[670] SCHMID, *Praxiskommentar*, pp 472-473.

b) Le recours cantonal

434 Le recours cantonal est un moyen de droit complet et l'autorité de recours statue avec un plein pouvoir d'examen en fait et en droit (art. 393 al. 2 CPP)[671]. C'est au droit cantonal qu'il revient de désigner l'autorité de recours[672]. Un membre du tribunal des mesures de contrainte ne peut pas siéger également au sein de l'autorité de recours lorsque celle-ci est appelée à statuer sur des recours contre des décisions dudit tribunal. Le CPP ne le précise pas parce que cela va de soi[673]. S'il est évident qu'une même personne ne peut pas statuer à deux titres dans la même cause, la question de savoir si une personne peut statuer dans une cause en tant que membre du tribunal des mesures de contrainte, et dans une autre cause en tant que membre de l'autorité de recours est moins évidente. Une telle situation ne semble en tout cas pas exclue et risque de se produire dans de petits cantons, bien qu'elle ne soit pas idéale. Celui qui siège dans l'autorité de recours sera moins enclin à sanctionner ses pairs s'ils ont admis trop largement des mesures de surveillance. Il aura tendance à suivre plus ou moins aveuglément la décision précédente, sans effectuer un contrôle approfondi[674].

435 Le recours doit être formé par le dépôt d'un mémoire écrit dans un délai de dix jours[675]. Le délai court dès la notification de la communication ou dès la connaissance de l'acte de procédure qui n'est pas notifié par écrit (art. 384 CPP). Le Tribunal fédéral a jugé qu'un recours déposé avant qu'une communication ne soit notifiée n'était pas recevable[676]. Le ministère public n'a pas la possibilité de recourir contre une décision du tribunal des mesures de contrainte qui refuse

[671] *Message du CF relatif à l'unification de la procédure pénale*, p. 1296; JOSITSCH, *Grundriss des schweizerischen Strafprozessrechts*, pp 203-206; KUHN, *La procédure pénale suisse selon le futur CPP unifié*, pp 161-162; PIETH, *Schweizerisches Strafprozessrecht*, pp 229-231; SCHMID, *Praxiskommentar*, pp 755-764.

[672] *Message du CF relatif à l'unification de la procédure pénale*, p. 1116.

[673] *Message du CF relatif à l'unification de la procédure pénale*, p. 1114.

[674] Sur le problème posé par l'absence de spécialisation des juges statuant sur des mesures de contrainte : CORNU, *L'enquête selon le CPP*, pp 75-76.

[675] La LSCPT prévoyait un délai de recours de trente jours (art. 10 al. 5).

[676] ATF 1P.15/2003 du 14 février 2003, et HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 323 et 328.

ou restreint la surveillance ordonnée ou demandée, même s'il est destinataire de la décision[677]. Il peut en revanche toujours déposer une nouvelle demande.

Le recours n'a pas d'effet suspensif (art. 387 CPP). Il ne permet donc pas d'éviter qu'une mesure de surveillance soit exécutée. Tout au plus permet-il d'en contrôler le bien-fondé après coup et d'en annuler les effets. Même lorsque la mesure n'est pas secrète, dans le cas d'un acte de procédure de la police par exemple, il n'est dans les faits pas possible de déposer un mémoire de recours écrit et motivé et encore moins d'obtenir immédiatement une décision de l'autorité de recours, avant même que la police ne procède à l'acte contesté. C'est donc bien un moyen de contrôle *a posteriori*. 436

Lors du contrôle *a posteriori*, il est parfois difficile de savoir quels éléments découlent de la mesure de surveillance et quels éléments auraient été également découverts en l'absence de toute surveillance, ainsi que ceux qui étaient connus avant la décision et ceux qui ne l'ont été qu'après. L'autorité de recours ne devrait ainsi statuer que sur la base du dossier tel qu'il était au moment où la surveillance a été autorisée, et non en prenant connaissance des résultats[678]. 437

Les frais de recours sont mis à la charge de la partie qui succombe[679]. En matière de surveillance, il est probable que la pratique en vigueur avant l'introduction du CPP soit maintenue, à savoir que l'autorité de recours renonce à mettre des frais à la charge de la personne surveillée qui succombe notamment lorsque le recours a été provoqué par l'attitude du ministère public[680]. 438

[677] ATF 133 IV 182, Ministère public de la Confédération, du 15 mars 2007.
[678] RUCKSTUHL, *Technische Überwachungen*, p. 151.
[679] Art. 426 al. 5 et 428 CPP.
[680] ATF 8G.109/2003 du 21 octobre 2003, consid. 4.

2. Devant le Tribunal fédéral

a) Le recours en matière pénale

439 Le recours en matière pénale au Tribunal fédéral est ouvert contre les décisions prises par les autorités cantonales de dernière instance et par le Tribunal pénal fédéral (art. 78ss LTF)[681]. C'est une voie de recours extraordinaire de nature cassatoire et réformatoire. En ce qui concerne les mesures de surveillance, il est recevable contre les décisions rendues par l'autorité de recours cantonale (statuant sur un recours déposé contre une décision de la police, du ministère public ou du tribunal des mesures de contrainte, ou sur un recours formé à la suite de la communication de la surveillance) et contre les décisions du tribunal des mesures de contrainte lorsqu'il statue en matière de prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure[682]. Ces décisions doivent remplir les exigences de motivation de l'art. 112 LTF. Le recours n'a en général pas d'effet suspensif, mais le président du tribunal peut l'accorder d'office ou sur requête (art. 103 LTF)[683].

440 Le recours en matière pénale est une voie de recours incomplète. En général, il peut être formé pour violation du droit fédéral et du droit international, ainsi que pour constatation manifestement inexacte des faits[684]. Etant donné que les décisions rendues au sujet de mesures de contrainte sont des décisions portant sur des mesures provisionnelles, seule peut être invoquée la violation des droits constitutionnels[685]. Par violation des droits constitutionnels, il faut évidemment comprendre le les droits constitutionnels écrits et non écrits, et les normes de

[681] Sur le recours en matière pénale en général : DONZALLAZ, *Commentaire LTF*, pp 936-1013; JOSITSCH, *Grundriss des schweizerischen Strafprozessrechts*, pp 219-231; PIETH, *Schweizerisches Strafprozessrecht*, pp 237-242; PIQUEREZ, *Traité*, pp 873-878 et 880-893; SEILER / WERDT / GÜNGERICH, *BGG*, pp 280-293; THOMMEN, *Art. 78-81 BGG*, pp 662-697.

[682] A moins que l'on admette, par analogie avec les autres mesures de surveillance, qu'un recours cantonal soit ouvert comme proposé à la p. 193 ci-dessus.

[683] A la notion de juge instructeur de l'art. 103 al. 3 LTF correspond celle de la direction de la procédure de l'autorité de recours de l'art. 61 CPP.

[684] DONZALLAZ, *Commentaire LTF*, pp 1274-1323 et 1334-1452; THOMMEN, *Art. 95-98 BGG*, pp 927-945 et 949-960; SEILER / WERDT / GÜNGERICH, *BGG*, pp 397-407 et 412-418.

[685] Art 93 al 1er et 98 LTF, DONZALLAZ, *Commentaire LTF*, pp 1250-1251 et 1462-1464; JEANNERET, *Le recours en matière pénale*, pp 8 et 16; SCHMID, *Die Strafrechtsbeschwerde*, p. 194.

droit international directement applicables[686]. Le délai de recours est de trente jours à compter de l'expédition complète de la décision attaquée (art. 100 LTF)[687].

b) Le recours constitutionnel subsidiaire

Le recours constitutionnel subsidiaire est ouvert contre les décisions rendues par les autorités judiciaires cantonales de dernière instance ne pouvant faire l'objet d'un recours en matière civile, d'un recours en matière pénale ou d'un recours en matière de droit public (art. 113 LTF)[688]. Seule la violation des droits constitutionnels peut être invoquée, soit les droits constitutionnels écrits et non écrits, et les normes de droit international directement applicables[689]. Le délai de recours est également de trente jours à compter de l'expédition complète de la décision attaquée (art. 100 LTF)[690]. 441

En matière de surveillance, le recours constitutionnel subsidiaire ne semble pas avoir d'application pratique. 442

3. Devant la Cour européenne des droits de l'Homme

La saisine de la Cour européenne des droits de l'Homme exige un épuisement des voies de recours internes. Elle n'entre en ligne de compte qu'à la suite d'une décision du Tribunal fédéral, ou d'une décision qui ne peut plus faire l'objet 443

[686] *Message du CF concernant la révision totale de l'organisation judiciaire*, pp 4134-4135; DONZALLAZ, *Commentaire LTF*, p. 1467; JEANNERET, *Le recours en matière pénale*, p. 15; SCHMID, *Die Strafrechtsbeschwerde*, p. 194. Les droits constitutionnels doivent être compris comme tous les droits garantis par la Constitution dont les particuliers peuvent invoquer la violation devant le Tribunal fédéral. Cette notion est plus large que celle de droits fondamentaux puisque des griefs comme la séparation des pouvoirs, la légalité ou la force dérogatoire du droit fédéral sont admis : Aubert / Mahon, *Petit commentaire*, p. 62; Auer / Malinverni / Hottelier, *Droit constitutionnel suisse I*, pp 694-697.

[687] Contrairement au recours cantonal où le délai est de dix jours.

[688] Sur le recours constitutionnel subsidiaire en général : BIAGGINI, *Art. 113-119 BGG*, 1111-1166; DONZALLAZ, *Commentaire LTF*, pp 1627-1655; SEILER / WERDT / GÜNGERICH, *BGG*, pp 483-502.

[689] DONZALLAZ, *Commentaire LTF*, pp 1643-1646; EHRENZELLER, *Die subsidiäre Verfassungsbeschwerde*, p. 106. *Message du CF concernant la révision totale de l'organisation judiciaire*, pp 4134-4135; Donzallaz, *Commentaire LTF*, p. 1467; Jeanneret, *Le recours en matière pénale*, p. 15; Schmid, *Die Strafrechtsbeschwerde*, p. 194. Voir également la note de bas de page 686 ci-dessus.

[690] Contrairement au recours cantonal où le délai est de dix jours.

d'un recours interne (cantonal ou fédéral). La procédure devant la Cour européenne des droits de l'Homme est gratuite et le requérant ne peut pas être condamné au paiement de dépens. Il s'agit d'une nouvelle procédure, dirigée contre l'Etat partie à la CEDH. Elle ne bénéficie pas de l'effet suspensif et ne peut conduire qu'à un jugement de condamnation dudit Etat. La décision contestée ne peut pas être modifiée par la Cour, qui peut seulement constater une violation de la CEDH et accorder une «satisfaction équitable», soit une indemnité financière, et le remboursement des frais engagés[691]. L'art. 122 LTF permet la révision d'un arrêt du Tribunal fédéral si la Cour européenne des droits de l'homme a constaté une violation et que la révision est nécessaire pour remédier aux effets de la violation. La révision n'a pas lieu d'office, mais seulement sur requête[692].

444 Le délai pour saisir la Cour européenne des droits de l'Homme est de six mois à compter de la notification de la décision contestée (art. 35 CEDH). La requête peut être rédigée dans n'importe quelle langue officielle d'un Etat contractant, même si la procédure devant la Cour se poursuit ensuite en français ou en anglais[693]. Elle doit être transmise par courrier postal[694]. Le requérant peut invoquer la violation des droits reconnus par la CEDH ou l'un des protocoles additionnels, mais il doit avoir déjà soulevé ces moyens devant la dernière instance nationale[695].

445 Si l'on part du principe que le contrôle *a priori* et le contrôle *a posteriori* doivent bénéficier d'une voie de recours judiciaire indépendante, le dépôt d'une requête devant la Cour européenne des droits de l'Homme semble donc envisageable non seulement en suite d'une décision du Tribunal fédéral, mais

691 Sur la procédure en général et les conséquences d'un arrêt de la Cour : VILLIGER, *Das Urteil des EGMR*.

692 ATF 5F_6/2008 du 18 juillet 2008, consid. 2 et DONZALLAZ, *Commentaire LTF*, pp 1683-1687.

693 Un formulaire *ad hoc* de requête est disponible sur le site internet de la Cour : http://www.echr.coe.int/ECHR/homepage_fr.

694 Une transmission par fax suffit à respecter le délai. La requête doit néanmoins être déposée ensuite par courrier.

695 Pour la Suisse, il s'agit du Protocole no 6 du 28 avril 1983 concernant l'abolition de la peine de mort (RS 0.101.06), du Protocole no 7 du 22 novembre 1984 (RS 0.101.07) et du Protocole no 13 du 3 mai 2002 relatif à l'abolition de la peine de mort en toutes circonstances (RS 0.101.093).

également lorsque le tribunal des mesures de contrainte autorise une surveillance de la correspondance, une surveillance des relations bancaires, l'utilisation d'autres dispositifs techniques de surveillance, ou encore lorsqu'il ordonne un prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure, étant donné que ces décisions sont définitives[696]. Sinon, et c'est le plus probable, la Cour européenne ne sera saisie qu'à la suite de décisions du Tribunal fédéral et en matière de prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure[697]. A notre sens, et par analogie avec les autres mesures de surveillance, un recours cantonal (contrôle *a posteriori*) devrait être recevable en matière de prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure même si le CPP ne le prévoit pas[698].

H. Le sort des données recueillies

1. Les données protégées par le secret professionnel

Les mesures techniques de surveillance doivent respecter le secret professionnel[699]. Celui-ci doit être entendu ici au sens large, puisqu'il s'agit du secret applicable à l'ensemble des personnes appartenant à l'une des catégories professionnelles énumérées aux art. 170 à 173 CPP[700]. 446

[696] Voir à ce sujet le chapitre 4. Le contrôle de la surveillance par une autorité judiciaire, p. 119 ci-dessus.

[697] Malgré le texte de la loi qui exclut un recours, le Tribunal fédéral pourrait s'estimer compétent pour entrer en matière afin d'éviter une violation de la CEDH (et une condamnation par la CourEDH) : ATF 125 II 417, 425- 426, A., du 26 juillet 1999.

[698] La décision ordonnant de se soumettre au prélèvement est alors assimilée à la communication. Voir à ce sujet le chapitre 1. Le contrôle *a posteriori*, p. 229 ci-dessous.

[699] Sur la notion de secret : JENDLY, *La coexistence des secrets*, pp 14-40 et les nombreuses références bibliographiques. Sur les raisons de protéger le secret : GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 135-150; HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 196-198.

[700] Il s'agit notamment des fonctionnaires, des membres des autorités, des ecclésiastiques, des avocats, des défenseurs en justice, des notaires, des médecins, des dentistes, des pharmaciens, des sages-femmes, des journalistes professionnels, des conseillers conjugaux, des médiateurs familiaux, des collaborateurs des centres de consultation en matière de grossesse et d'aide aux victimes d'infractions.

447 Trois cas de figure peuvent se présenter : premièrement la surveillance est dirigée contre le prévenu qui est détenteur du secret professionnel, deuxièmement la surveillance est dirigée contre le prévenu dépositaire du secret et le détenteur du secret professionnel apparaît comme un tiers, et troisièmement le dépositaire et le détenteur du secret apparaissent dans une surveillance dirigée contre un prévenu qui n'est aucun des deux[701].

448 Le secret professionnel a pour but de protéger le dépositaire, mais ne doit pas servir à cacher la personne soumise au secret professionnel contre qui la surveillance est dirigée. Ainsi, dans le premier cas, seuls les intérêts des dépositaires doivent être pris en compte et justifient que des éléments soient écartés du dossier. Dans les deux autres cas, le secret est absolu puisque la surveillance n'est pas dirigée contre le détenteur du secret. Il protège complètement les dépositaires, qu'ils soient visés par la surveillance ou qu'ils y apparaissent comme des tiers[702].

449 Dans le premier cas, l'art. 271 CPP prévoit que le tri des informations protégées par le secret professionnel et qui n'ont de lien ni avec l'objet de l'enquête ni avec le motif pour lequel la personne concernée est soumise à la surveillance doit être opéré sous la surveillance d'un tribunal[703]. Le message du Conseil fédéral précise que l'autorité, qui doit être judiciaire, n'est pas tenue de procéder au tri elle-même, mais qu'elle peut se contenter de diriger l'opération. Cette tâche peut être confiée au tribunal des mesures de contrainte[704]. Celui-ci ne pourrait alors plus statuer dans la cause, qu'il s'agisse de l'autorisation d'une autre mesure de surveillance, de détention provisoire, ou d'une autre de ses compétences. L'autorité judiciaire devrait néanmoins contrôler les informations qui seront remises au ministère public, même si elle ne procède pas au tri elle-

[701] Sur les conditions auxquelles un détenteur de secret peut être surveillé : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 195-206; OBERHOLZER, *Grundzüge des Strafprozessrechts*, p. 252; PIQUEREZ, *Traité*, pp 593-596 et 621; RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, pp 449-451; STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 137-139.

[702] L'exemple classique du dépositaire objet de la surveillance est le prévenu qui s'entretient avec son avocat. Les informations recueillies ne doivent jamais être utilisées.

[703] HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 213-217.

[704] *Message du CF relatif à l'unification de la procédure pénale*, pp 1231-1232.

même[705]. La formulation de l'art. 271 al. 1 CPP pourrait être modifiée par l'avant-projet de révision de la LSCPT qui préciserait que non seulement un tri doit être opéré, mais également que l'accès direct par les autorités de poursuite pénale aux informations recueillies dans le cadre de la surveillance est empêché[706]. Il s'agirait d'une simple clarification.

Les informations écartées doivent être soustraites non seulement à la curiosité du ministère public, mais aussi à celle des policiers chargés de l'investigation. Une fois le tri effectué, les informations écartées en raison du secret professionnel ne doivent pas être conservées dans un dossier séparé. Elles doivent être entièrement détruites, c'est-à-dire que ne peuvent être conservés ni les supports de données, ni les transcriptions[707]. Le branchement direct n'est possible dans ce cas qu'à des conditions très strictes, puisque l'autorité policière prend connaissance des informations avant même qu'un tri ne puisse avoir lieu[708]. Avant l'introduction du CPP, il n'était pas autorisé pour les personnes soumises au secret professionnel[709]. La formulation de l'art. 271 al. 2 CPP pourrait également être modifiée par l'avant-projet de révision de la LSCPT. La notion de branchement direct utilisée jusqu'alors pour parler de surveillance en temps réel disparaîtrait et l'accès direct aux informations recueillies en temps réel serait en principe empêché pour qu'un tri puisse avoir lieu[710]. Lorsqu'un branchement direct est techniquement nécessaire, un tri ne peut pas être opéré avant mais des mesures supplémentaires doivent être prises. 450

[705] STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 162. Pour des exemples d'informations qui doivent être écartées en raison du secret professionnel : STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 165-166.

[706] *Rapport du CF relatif à l'AP LSCPT*, pp 44-45.

[707] STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, p. 163.

[708] Art. 271 al. 2 CPP. Le branchement direct est entendu ici dans le sens de surveillance en temps réel, contrairement à la notion de branchement direct lorsque la surveillance par le CSI-DFJP n'est techniquement pas possible et que les résultats sont transmis directement à l'autorité policière qui est responsable de leur enregistrement. Pour un exemple : *Rapport du CF relatif à l'AP LSCPT*, pp 25-26. Sur le branchement direct en général : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 176-184. Le problème de l'accès à des données protégées existe évidemment tout autant en cas de branchement direct au sens propre.

[709] Art. 3 al. 4 aLSCPT et HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 183-184.

[710] .*Rapport du CF relatif à l'AP LSCPT*, pp 44-45.

451 En pratique, il est souvent difficile de savoir si une conversation est couverte ou non par le secret professionnel sans l'écouter, notamment en l'absence d'informations relatives à l'identité des interlocuteurs des personnes surveillées. La violation du secret professionnel semble inévitable, même si ces informations sont ensuite inexploitables[711]. Une mesure de tri supplémentaire devrait être instaurée.

452 Dans les deux autres cas, soit lorsque la surveillance n'est pas dirigée contre le prévenu dépositaire du secret, l'art. 271 al. 3 CPP prévoit que les informations couvertes par le secret ne peuvent pas être exploitées. Elles doivent être retirées du dossier de la procédure pénale et immédiatement détruites[712]. Si le principe est clair, la mise en pratique est bien plus compliquée[713]. Lorsque la procédure est dirigée contre une personne soumise au secret professionnel, il est évident avant même le début de la surveillance que des informations protégées seront surveillées et qu'il faudra par conséquent soumettre au tri par l'autorité judiciaire l'ensemble des données recueillies[714]. En revanche lorsqu'il n'y a, *a priori*, pas de raison de se douter que de telles informations seront recueillies, les données sont transmises directement aux personnes chargées de l'instruction. Ces données seront écartées et ne pourront pas servir de preuves, mais elles auront néanmoins été portées à la connaissance des policiers et parfois du ministère public.

453 Bien qu'idéal, le tri systématique des données recueillies par une autorité judiciaire indépendante n'est que difficilement réalisable en pratique[715]. Un tel tri doit alors être opéré dès qu'il existe un soupçon raisonnable que des informations protégées par le secret tomberont sous le champ de la surveillance. Dans les autres cas, elles devront être immédiatement écartées et ceux qui pourraient en avoir eu connaissance devront en faire abstraction. Les informations écartées ne pourront pas servir de preuves. Il est en revanche

711 AELLEN / HAINARD, *Secret professionnel et surveillance des télécommunications*.

712 HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 269.

713 STRÄULI, *La surveillance de la correspondance par poste et télécommunication*, pp 160-161.

714 Encore faut-il que l'objet de la surveillance soit identifié comme étant au bénéfice du secret. Sur cette question : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 201-204.

715 Sur les différentes possibilités : GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 157-160.

difficile de contrôler que ces informations n'aideront pas pour autant la police dans sa recherche d'autres preuves. On est ici réduit à faire confiance à l'autorité dans son respect de la loi.

Dans un arrêt non publié concernant le tri d'une douzaine de cartons de documents saisis dans le cadre d'une enquête fiscale contre deux avocats, le Tribunal fédéral a souligné que lorsque la distinction ne peut pas être faite clairement entre des documents protégés par le secret professionnel et ceux qui ne le sont pas, l'intérêt public à poursuivre les infractions graves qui sont soupçonnées prévaut sur la protection du secret professionnel[716]. Cette entorse au secret professionnel ne doit pas permettre d'utiliser les informations couvertes par le secret professionnel à l'encontre des dépositaires du secret. 454

2. Les données inutiles

Les données obtenues par une mesure de surveillance sont généralement très nombreuses. Une grande quantité n'est cependant d'aucune utilité, parce qu'elle n'a aucun lien avec l'enquête en cours par exemple[717]. Comme dans le cas d'une perquisition, un tri doit être effectué[718]. Il convient de séparer les éléments utiles à la procédure des éléments inutiles, après avoir cas échéant écarté ceux qui sont inutilisables en raison de la protection du secret professionnel. C'est d'ailleurs souvent au cours de la procédure, et non pas déjà lors de la surveillance, que la distinction entre les documents utiles et inutiles peut être effectuée[719]. 455

Le CPP prévoit en outre que les documents et enregistrements collectés lors d'une surveillance dûment autorisée qui ne sont pas nécessaires à la procédure doivent être conservés séparément (art. 276 al. 1). Si cette règle est expressément prévue en matière de surveillance de la correspondance et des autres dispositifs techniques de surveillance, nous l'appliquerons par analogie 456

[716] ATF 1B_288/2007 du 30 septembre 2008, consid. 3.6.

[717] GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, p. 202.

[718] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 75.

[719] GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 130-131; HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 264; RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*, p. 457.

pour toutes les mesures de surveillance, comme en ce qui concerne le tri des informations soumises au secret professionnel.

457 Le CPP ne précise toutefois pas qui est responsable d'opérer ce tri et sur quelle base, pas plus qu'il ne prévoit une possibilité de faire contrôler ce tri, une possibilité de demander que des documents soient ajoutés ou écartés, ni une voie de recours. Lorsqu'il s'agit de protéger un secret professionnel, il est évident que les personnes chargées de l'investigation ne peuvent opérer le tri entre ce qui peut être porté à leur connaissance et ce qui doit rester secret. Lorsqu'il s'agit en revanche simplement de séparer ce qui est utile à la procédure de ce qui ne l'est pas, il n'y a aucun problème à ce que la police ou le ministère public effectue le tri, puisqu'il n'y a pas d'empêchement à ce que ces autorités aient connaissance de toutes les informations. Afin de préserver les droits de la défense, ne devront toutefois être écartées que les pièces qui sont totalement inutiles à la procédure. Le fait qu'il s'agisse de conversations tenues entre le prévenu visé par la surveillance ou des tiers uniquement ne joue en revanche aucun rôle[720].

458 Les informations écartées seront conservées dans un dossier séparé, parfois appelé dossier fantôme. Les documents et enregistrements collectés lors d'une surveillance qui ne sont pas nécessaires à la procédure doivent être détruits immédiatement après la clôture de la procédure (art. 276 al. 1 CPP)[721]. Une destruction au fur à mesure de leur récolte n'est pas envisageable, car des éléments qui apparaissent initialement comme inutiles pourraient ultérieurement s'avérer importants[722]. De même des informations considérées comme inutiles par les enquêteurs peuvent avoir leur importance pour le prévenu et son défenseur.

459 Le législateur a choisi de faire prévaloir la protection des tiers sur les droits du prévenu à un accès intégral au dossier : le droit de consulter le dossier ne concerne pas le dossier fantôme[723]. Le fait de conserver ces informations séparément permet d'éviter que toute personne qui a le droit de consulter le

[720] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 267.

[721] Sur la notion de clôture de la procédure : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 266-267.

[722] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 264.

[723] HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 265.

dossier n'ait accès à des données personnelles de tiers résultant de la surveillance et dont la connaissance n'est pas utile à la procédure[724]. Le droit de consulter le dossier n'est pas absolu, mais les autorités pénales ne peuvent fonder leurs décisions sur des pièces auxquelles une partie n'a pas eu accès que si celle-ci a été informée de leur contenu essentiel (art. 108 al. 4 CPP)[725]. Ce cas de figure devrait rester exceptionnel. Les cas où des pièces inutiles et inutilisées sont confinées dans un dossier fantôme auquel le prévenu n'a pas accès peut en revanche être admis. Si une partie souhaite que certains éléments soient ajoutés au dossier de la cause, et qu'elle suppose qu'ils figurent dans le dossier fantôme, elle doit pouvoir le demander comme elle solliciterait n'importe quelle autre preuve[726].

3. Les autres données

Les données obtenues sont rarement utilisées telles quelles, mais le plus souvent retranscrites, résumées, traduites ou encore analysées. Afin de pouvoir s'assurer que ces opérations ne contiennent pas d'erreurs, il est essentiel de conserver les données originales et les informations liées aux transformations (nom du traducteur, méthode de décodage, etc.) jusqu'à la clôture définitive de la procédure[727]. Le CPP ne contient pourtant pas de dispositions à ce sujet[728]. Les données recueillies devraient aussi mentionner les informations liées à leur

460

[724] ATF 125 I 96, 101-102, A.G., B.G., C.G. et D.G, du 28 janvier 1999.

[725] Sur les restrictions à la consultation du dossier : VERNIORY, *L'accès au dossier*, pp 136-142; VERNIORY, *Les droits de la défense*, pp 393-400.

[726] M. Calmanovici s'est plaint devant la Cour européenne des droits de l'Homme du fait qu'il n'avait pas la possibilité de consulter la partie des enregistrements jugés non pertinents par le tribunal. La Cour n'a malheureusement pas jugé nécessaire d'examiner ce grief. Elle a retenu l'absence de plusieurs autres garanties minimales nécessaires pour éviter les abus des autorités et a conclu que les dispositions nationales présentaient des insuffisances incompatibles avec le degré minimal de protection voulu par la prééminence du droit dans une société démocratique : arrêt CALMANOVICI c. Roumanie, no 42250/02, §§ 114 et 125, du 1er juillet 2008.

[727] Sur ces différentes données et leurs supports : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 257-260.

[728] OBERHOLZER, *Die Regeln bei polizeilich erhobenen Daten sind unklar*, pp 25-26.

véracité et leur authenticité[729]. Ces informations ne sont que très rarement fournies, ce qui est inquiétant et empêche tout contrôle.

461 A l'inverse, il est important que des données inutiles ne soient pas conservées indéfiniment. A fin de cause, les données devraient être détruites. Il arrive pourtant régulièrement que le tribunal oublie de se prononcer sur ces questions, comme c'est parfois aussi le cas pour le sort de certains séquestres. Une liste des supports de données pourrait par exemple figurer dans le dossier officiel. Ainsi lors du jugement, le tribunal saurait exactement ce dont il doit ordonner la destruction. A titre de garantie subsidiaire, une disposition légale indiquant que la police doit détruire les données d'une surveillance dans les trente jours suivant l'entrée en force du jugement final pourrait être ajouté dans le CPP. Les lois cantonales et fédérale en matière de protection des données seraient applicables pour le surplus.

462 L'avant-projet de révision de la LSCPT mention qu'un nouveau système informatique de traitement des données recueillies lors de la surveillance de la correspondance par télécommunication exploité par le CSI-DFJP sera mis en fonction complète à l'entrée en vigueur de la nouvelle LSCPT[730]. Les données ne seraient plus envoyées par poste sous forme de DVD comme actuellement, mais seraient consultables directement par un droit d'accès informatique à distance[731]. On peut craindre que cette manière de faire empêche l'accès du prévenu ou de son défenseur à l'intégralité des données récoltées[732]. Elles seraient conservées jusqu'à l'échéance du délai de prescription de l'action pénale, puis supprimées. L'autorité en charge du dossier aurait la possibilité de demander le transfert des données avant leur effacement pour respecter les obligations liées à la conservation des dossiers ou l'intérêt de la procédure[733].

[729] Chacun ne peut en principe que garantir l'authenticité des données qu'il maîtrise. Si un opérateur téléphonique peut ainsi assurer que le numéro surveillé en Suisse est bien le bon, il lui est souvent impossible d'en faire de même pour le numéro du correspondant étranger.

[730] « Interception System Schweiz »(ISS).

[731] Art 9 AP LSCPT et *Rapport du CF relatif à l'AP LSCPT*, pp 8-9 et 19.

[732] Voir à ce sujet le chapitre 6. La conservation des enregistrements intacts jusqu'à la fin du procès pénal, p. 120 ci-dessus.

[733] Art 11 AP LSCPT et *Rapport du CF relatif à l'AP LSCPT*, pp 21-22.

I. Les découvertes fortuites

Bien que les mesures d'enquêtes soient ordonnées sur la base de soupçons se rapportant à une infraction concrète, il arrive que les résultats obtenus mettent en lumière une autre infraction qui peut avoir été commise par le prévenu ou par un tiers. On appelle ainsi découvertes fortuites les éléments concernant une infraction découverte lors d'une enquête portant sur une autre infraction[734]. Les lois cantonales de procédure ne régissaient que très rarement cette question. S'il ne permet pas la recherche indéterminée de preuves[735], l'art. 243 CPP autorise pourtant largement l'utilisation des découvertes fortuites[736]. Le secret professionnel ou d'autres garanties légales doivent néanmoins être respectés également si les informations sont découvertes fortuitement[737]. 463

La situation est un peu différente en matière de surveillance technique, puisqu'elle est en principe soumise à autorisation contrairement aux autres actes d'enquête. On trouve des dispositions spéciales, singulièrement pour la surveillance de la correspondance par poste et télécommunication, ainsi que pour l'utilisation d'autres dispositifs de surveillance à l'art. 278 CPP[738]. Aucune règle ne figure en revanche dans le CPP pour ce qui est de l'observation et de la surveillance des relations bancaires. Il s'agit d'une lacune et les dispositions régissant les découvertes fortuites en matière de surveillance de la 464

[734] GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 202-206; OBERHOLZER, *Grundzüge des Strafprozessrechts*, pp 560-561; SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*, p. 285.

[735] Aussi appelée « fishing expedition », soit des actes d'enquêtes motivés par aucun soupçon, mais dont le but est précisément de fournir des indices propres à fonder un soupçon.

[736] *Message du CF relatif à l'unification de la procédure pénale*, p. 1219; PIQUEREZ, *Traité*, pp 582-583.

[737] BÉNÉDICT, *Le sort des preuves illégales*, pp 193-194; PIQUEREZ, *Traité*, pp 582-583; SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*, pp 301-302.

[738] Sur la situation avant l'entrée en vigueur du CPP et notamment sous l'empire de l'art. 9 LSCPT : FICKERT, *Die Behandlung von Zufallserkenntnissen*; GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*, pp 202-220; HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 275-305; HÜPPI, *Zufallsfunde aus genehmigten Telephonüberwachungen*; JEAN-RICHARD-DIT-BRESSEL, *Ist ein Millionendiebstahl ein Bagatelldelikt*; NATTERER, *Die Verwertbarkeit von Zufallsfunden*; RUCKSTUHL, *Technische Überwachungen*, pp 154-158; SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*.

correspondance doivent s'appliquer par analogie[739]. Une fois encore, nous regrettons que le CPP ne règle pas toutes les mesures de surveillance de manière commune.

465 En matière de profils d'ADN, la question des découvertes fortuites ne se pose pas puisque la LADN permet de comparer le profil d'une personne avec la base de données, sans qu'il existe le soupçon de la commission d'une autre infraction que celle pour laquelle elle est poursuivie, ou encore de comparer le profil de traces avec celui des personnes enregistrées, sans qu'il existe pour autant un soupçon précis contre l'une d'entre elles[740]. Le résultat ne devrait en revanche pas porter atteinte à une personne qui n'est pas enregistrée ou ne remplit pas les conditions d'enregistrement. Nous pensons ici à la possibilité de déduire qu'il s'agit d'un parent du profil enregistré lorsque les traces comparées concordent presque sans être totalement identiques[741]. La base de données devrait être conçue de sorte que le résultat obtenu lors d'une comparaison soit identique ou non. Rien ne justifie qu'une personne soit plus exposée à une poursuite pénale parce que l'un ou l'autre de ses proches parents est un criminel enregistré[742]. L'art. 2 al. 2 LADN interdit de chercher à déterminer l'état de santé ou d'autres caractéristiques propres à la personne en cause lors de l'analyse de l'ADN, à l'exception de son sexe. La recherche de proches paraît donc exclue[743]. Une utilisation de la base de données des profils d'ADN au-delà de ce que la loi prévoit est également interdite (art. 1 et 2 LADN).

466 Le principe de base est que les découvertes fortuites faites lors d'une surveillance ne doivent pas permettre d'éluder les dispositions régissant les mesures de surveillance. Ce n'est pas parce qu'une personne est prévenue en raison d'un acte justifiant une surveillance, que cette surveillance peut être

[739] SCHMID, *Praxiskommentar*, p. 536. Pour un avis plus nuancé en matière d'observation, une distinction étant faite entre la simple observation (die polizeiliche Beobachtung) et l'observation soumise à autorisation (die Observation) : RHYNER / STÜSSI, *Kommentar zu Art. 282-283 StPO*, pp 481-482. A notre avis, cette dernière interprétation permet d'utiliser trop largement des informations pour lesquelles une autorisation n'aurait pas été accordée.

[740] Art. 11 LADN et pour un avis critique: RUCKSTUHL, *Technische Überwachungen*, p. 155.

[741] TARONI / CASTELLA / RIBAUX, *et al.*, *Partial DNA profiles and familial searching*, p. 10.

[742] TARONI / CASTELLA / RIBAUX, *et al.*, *Partial DNA profiles and familial searching*, pp 16-17.

[743] La question d'une action en constat ou désaveu de paternité au sens du Code civil étant bien entendue réservée.

utilisée pour prouver d'autres actes pour lesquels une surveillance n'est pas autorisée, ou pour viser une tierce personne contre qui la surveillance n'est pas autorisée. De la même manière ce n'est pas parce qu'une personne a un proche parent enregistré dans la base de profils d'ADN qu'elle doit être désavantagée par rapport à celle n'ayant aucun parent enregistré. L'utilisation extensive d'une surveillance pour aller à la pêche aux indices est prohibée.

467 L'art. 278 CPP vise à l'al. 1er le cas d'autres infractions que celles justifiant la surveillance mais commises par la personne surveillée[744], alors que l'al. 2 concerne les infractions commises par une autre personne[745]. Dans les deux cas, les informations recueillies ne peuvent être utilisées que si les conditions avaient été remplies pour ordonner la surveillance. Dans ce cas, le ministère public doit ordonner la surveillance et demander l'autorisation nécessaire au tribunal des mesures de contrainte. Si les conditions ne sont pas remplies, si le ministère public n'ordonne pas la surveillance ou encore si le tribunal des mesures de contrainte ne l'autorise pas, les documents et les enregistrements concernant ces découvertes fortuites ne peuvent pas être utilisés. Ils doivent être conservés séparément et détruits immédiatement après la clôture de la procédure, y compris les éléments recueillis grâce à ces découvertes fortuites[746]. Il s'agit d'un cas de preuves inexploitables au sens de l'art. 141 al. 2 CPP[747].

468 L'art. 278 CPP est plus strict que ne l'était l'ancien art. 9 LSCPT, puisque ce dernier permettait de retenir les informations concernant des actes qui ne justifiaient pas une mesure de surveillance, mais commis en plus d'actes justifiant la mesure[748]. La personne soupçonnée d'avoir commis en plus une infraction pour laquelle une mesure de surveillance pouvait être ordonnée était désavantagée par rapport à la personne qui n'était soupçonnée que d'un acte qui ne pouvait pas être surveillé[749]. L'utilisation de la surveillance pour l'infraction

[744] Pour des exemples: HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 279-281.

[745] Pour des exemples: HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 288-291.

[746] SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*, pp 309-314.

[747] ATF 133 IV 329, 331, X du 9 octobre 2007, consid 4.4. Voir à ce sujet le chapitre b). Les preuves inexploitables p. 212 ci-dessous. Les preuves ne sont pas détruites immédiatement comme le prévoit l'art. 277 CP mais seulement à la clôture de la procédure car des preuves pourraient contenir simultanément des éléments exploitables et d'autres inexploitables.

[748] WOLTER, *Kommentar zu Art. 269-281 StPO*, p. 267.

[749] *Message du CF relatif à l'unification de la procédure pénale*, p. 1233.

qui ne permettait normalement pas la surveillance n'était pas sans limite. Contrairement à ce que laissait penser le texte de la loi, une condamnation pour la seconde infraction n'était admise que si une condamnation était également prononcée pour la première[750].

469 Cette interdiction stricte d'utiliser les résultats d'une surveillance qui n'aurait pas pu être ordonnée seule est entièrement justifiée[751]. On peut être à première vue surpris que des informations prouvant matériellement la commission d'une infraction ne soient pas formellement utilisables, mais cela assure le respect de la loi de la même manière vis-à-vis de tous, y compris vis-à-vis de celui qui est soupçonné d'avoir commis une autre infraction. Rien ne justifie de sanctionner une infraction mineure dont la commission n'a été connue de l'autorité que parce qu'il existe le soupçon d'une infraction plus grave. La sanction de l'infraction pour laquelle la surveillance est ordonnée ne doit pas être complétée par la sanction supplémentaire d'une infraction qui n'aurait pas pu être découverte normalement.

470 En matière de recherche de personnes, le CPP prévoit que toutes les informations recueillies lors d'une surveillance peuvent être utilisées pour rechercher une personne signalée (art. 278 al. 5)[752]. Dans le cadre des recherches au sens de l'art. 210 CPP, les moyens à disposition des autorités de poursuite ne sont pas mentionnés[753]. L'art. 278 al. 5 pourrait laisser penser qu'une mesure de surveillance peut être mise en place sans autorisation si elle a pour but de retrouver une personne[754]. L'al. 5 constitue certes une exception, mais le fait qu'il figure dans une disposition consacrée aux découvertes fortuites limite sa portée. Y voir une possibilité de mettre en place une surveillance différente sans autorisation est dangereux et ne se justifie pas. Les raisons qui ont poussé le législateur à soumettre ces mesures à autorisation dans le cadre de

[750] HANSJAKOB, *Das neue BVE*, p. 291; SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*, pp 281-283.

[751] Pour un avis contraire, plutôt favorable à la vérité matérielle : JEAN-RICHARD-DIT-BRESSEL, *Ist ein Millionendiebstahl ein Bagatelldelikt*, pp 69-70.

[752] Pour un avis critique : HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 303-305; SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*, pp 302-305.

[753] *Message du CF relatif à l'unification de la procédure pénale*, p. 1203.

[754] Dans ce sens : SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*, p. 306.

la recherche de preuves sont aussi valables lors de la recherche de personnes[755]. Une mesure de surveillance téléphonique visant uniquement à localiser une personne recherchée serait illégale si elle a été mise en place sans autorisation et les éventuels résultats obtenus sont absolument inexploitables. Il est alors surprenant que les informations découvertes fortuitement lors d'une surveillance menée à l'encontre d'une autre personne et pour des autres faits soient exploitables.

J. Les preuves illégales

1. En général

a) Les preuves exploitables

471 Le Code de procédure pénale a repris la jurisprudence du Tribunal fédéral et distingue différents cas d'illégalité et y attribue des conséquences différentes[756]. Une preuve illégale n'est pas automatiquement nulle et inutilisable. Ainsi, la simple violation de prescriptions d'ordre dans l'administration des preuves n'empêche pas leur utilisation (art. 140 al. 3 CPP). De telles preuves illégales sont donc exploitables de la même manière que des preuves recueillies légalement[757].

[755] La protection de la sphère privée et le caractère secret des mesures de surveillance notamment.

[756] KAUFMANN, *Beweisführung und Beweiswürdigung*, pp 240-241; OTTINGER, *L'exploitation des moyens de preuve obtenus illégalement*. Cette jurisprudence est contestée par une partie de la doctrine. Pour un état des avis voir l'ATF 131 I 272, 280, X., du 3 mai 2005, et RUCKSTUHL, *Rechtswidrige Beweise erlaubt*, p. 17 et les références citées; VEST / HÖHENER, *Beweisverwertungsverbote*, pp 102-106. Pour un résumé de la jurisprudence récente : VEST / HÖHENER, *Beweisverwertungsverbote*, pp 95-98. Sur la notion de l'illégalité de la preuve : BÉNÉDICT, *Le sort des preuves illégales*, pp 20-22; FORNITO, *Beweisverbote im schweizerischen Strafprozess*, pp 3-7. Plus généralement sur la notion de preuve en droit civil, pénal et administratif, ainsi que sur la question de l'appréciation des preuves : KAUFMANN, *Beweisführung und Beweiswürdigung*.

[757] C'est une nouveauté introduite par le CPP. La jurisprudence antérieure imposait de recourir à une pesée des intérêts également lorsque la violation ne concernait qu'une prescription d'ordre : OTTINGER, *L'exploitation des moyens de preuve obtenus illégalement*, ch. 42.

b) Les preuves inexploitables

472 L'art. 141 al. 1 CPP consacre une interdiction absolue d'exploiter deux catégories de preuves, à savoir celles obtenues par des méthodes interdites et celles que le CPP mentionne comme inexploitables. Parmi les méthodes interdites, on trouve les moyens de contrainte, le recours à la force, les menaces, les promesses, la tromperie et les moyens susceptibles de restreindre les facultés intellectuelles ou le libre arbitre (art. 140 CPP)[758]. Certains auteurs estiment néanmoins que le droit de l'inculpé de prouver son innocence ne doit connaître aucune restriction de principe et que les preuves à décharge devraient toujours être admises[759]. L'interdiction doit pourtant être absolue pour les méthodes prohibées, comme le prévoit expressément le CPP, et cela que la preuve soit recueillie par l'autorité ou par un privé, et même si le prévenu y consent. Permettre au prévenu d'accepter ces méthodes reviendrait à exercer sur lui une contrainte indirecte, puisqu'un refus de sa part serait interprété comme un élément suspect[760]. Ces méthodes portent en outre atteinte au noyau dur de plusieurs droits fondamentaux, parmi lesquels la garantie du respect de la dignité humaine. La Cour européenne des droits de l'Homme considère également que des éléments matériels à charge rassemblés au moyen d'actes de violence, du moins si ces actes peuvent être qualifiés de torture, ne doivent jamais, quelle qu'en soit la valeur probante, être invoqués pour prouver la culpabilité de la personne qui en a été victime[761].

[758] Sur la situation en droit français et américain : VUCHER-BONDET, *La recevabilité d'un témoignage sous hypnose*. Sur l'inadmissibilité d'une preuve obtenue par la torture en droit comparé : Arrêt GÄFGEN c. Allemagne [GC], no. 22978/05, §§ 69-74, du 1er juin 2010.

[759] BÉNÉDICT, *Le sort des preuves illégales*, pp 237-238; HAUSER / SCHWERI / HARTMANN, *Schweizerisches Strafprozessrecht*, p. 285; PIQUEREZ, *Traité*, pp 461-462.

[760] Art. 140 al. 2 CPP, *Message du CF relatif à l'unification de la procédure pénale*, p. 1162; KAUFMANN, *Beweisführung und Beweiswürdigung*, pp 140-141; PIQUEREZ, *La preuve pénale*, p. 19.

[761] Arrêt GÄFGEN c. Allemagne [GC], no. 22978/05, §§ 167-168, du 1er juin 2010. La Grande Chambre a néanmoins considéré dans cette affaire que si les preuves recueillies en suite de torture (violation de l'art. 3 CEDH) n'étaient pas exploitables, la procédure dans son ensemble n'était pas contraire à l'art. 6 CEDH, la condamnation reposant sur des aveux et des preuves matérielles recueillies dans un second temps de manière légale (Arrêt GÄFGEN c. Allemagne [GC], no. 22978/05, §§ 169-188, du 1er juin 2010). Pour un avis contraire, voir l'Opinion partiellement dissidente commune aux juges ROZAKIS, TULKENS, JEBENS, ZIEMELE, BIANKU et POWER.

La seconde catégorie de preuves inexploitables contient celles que le CPP cite comme telles. Il s'agit des preuves qui auraient été administrées en violation du droit de participer à l'administration des preuves et qui ne sont pas exploitables à la charge de la partie qui n'était pas présente (art. 147 CPP), des déclarations faites sous couvert d'anonymat si le tribunal des mesures de contrainte a refusé son approbation (art. 150 CPP), des premières auditions effectuées sans avoir informé le prévenu de ses droits (art. 158 CPP)[762], de l'audition d'un témoin qui n'a pas été informé de son droit de refuser de témoigner et qui fait valoir ultérieurement ce droit (art. 177 CPP), des informations couvertes par le secret professionnel lorsqu'une personne autre que le détenteur du secret est surveillée (art. 271 CPP), des informations recueillies lors d'une surveillance non autorisée de la correspondance ou lors de l'utilisation de dispositifs techniques de surveillance (art. 277 CPP)[763], des découvertes fortuites pour lesquelles une autorisation ne peut pas être obtenue ultérieurement (art. 278 CPP), et des informations recueillies lors d'une investigation secrète non autorisée (art. 289 CPP). 473

Dans ces cas, nous pourrions éventuellement admettre les preuves à décharge lorsque la règle violée a pour but de protéger le prévenu[764]. Il faut en revanche faire preuve de plus de réserve lorsque les intérêts de tiers sont en jeu, par exemple des informations couvertes par le secret professionnel. Au surplus, la qualité et la fiabilité de la preuve obtenue illégalement peuvent être plus faibles[765]. 474

[762] Avant l'entrée en vigueur du CPP, le TF considérait qu'il s'agissait d'une violation d'un droit formel et que les déclarations faites par un prisonnier auquel ses droits n'avaient pas été rappelés n'étaient pas exploitables, avant d'ajouter que la pesée d'intérêts prévue en matière de preuves illégales s'appliquait également ici : ATF 130 I 126, 132, X., du 18 mai 2004. Cette pesée d'intérêts n'est plus admissible aujourd'hui.

[763] Que l'autorisation ait été refusée ou qu'elle n'ait pas été demandée. Voir le chapitre 2 En matière de surveillance.

[764] Cela pose toutefois des problèmes pratiques car le CPP prévoit la destruction immédiate des preuves illégales et le prévenu n'y a pas accès. Une telle preuve pourrait être admise par exemple lorsque le prévenu en avait déjà connaissance d'une autre manière mais n'avait pas les moyens de la produire.

[765] Sur le risque d'altération de la preuve et de déclarations fausses : RUCKSTUHL, *Rechtswidrige Beweise erlaubt*, p. 20.

c) Les preuves relativement inexploitables

475 Entre la violation de simples prescriptions de forme et les méthodes interdites, on trouve les preuves qui ont été administrées d'une manière illicite ou en violation de règles de validité par les autorités pénales. Elles ne sont en principe pas exploitables (art. 141 al. 2 CPP). Cette interdiction est relative, car l'exploitation de ces preuves est autorisée si elle est indispensable pour élucider des infractions graves, que les preuves soient à charge ou à décharge[766]. Le Tribunal fédéral estime que l'utilisation d'une preuve obtenue illégalement est inadmissible s'il était impossible de se la procurer par un moyen conforme au droit[767]. Si la preuve pouvait être recueillie de manière conforme au droit, il faut alors procéder à une pesée des intérêts en présence, soit d'une part l'intérêt de l'Etat à ce que le soupçon concret soit confirmé ou infirmé, et d'autre part l'intérêt légitime de la personne concernée à la sauvegarde de ses droits personnels[768]. Autrement dit, plus les faits reprochés sont graves, plus l'intérêt de l'Etat à la découverte de la vérité prend le pas sur l'intérêt privé du prévenu à ce que la preuve illégale ne soit pas utilisée[769]. En pratique, la pesée des intérêts a presque toujours lieu en faveur de la poursuite pénale et au détriment du prévenu[770]. Quant à la Cour européenne des droits de l'Homme, elle se contente de contrôler si le procès est équitable dans son ensemble et que la condamnation ne repose pas exclusivement sur une preuve illégale[771], et si l'illégalité a pu être contestée devant une autorité nationale[772]. Lorsque la décision sur la recevabilité d'une preuve est prise par le juge du fond, il sera influencé par cette preuve, qu'il l'accepte ou qu'il l'écarte, et les droits de la défense seront irrémédiablement entravés[773].

[766] *Message du CF relatif à l'unification de la procédure pénale*, p. 1163.
[767] ATF 96 I 437, 441, VON DÄNIKEN, du 4 novembre 1970.
[768] ATF 109 Ia 244, 246, X. (SCHENK), du 7 septembre 1983.
[769] ATF 131 I 272, 279, X., du 3 mai 2005.
[770] VETTERLI, *Bemerkungen zur BGE 1P.51/2007*, p. 85.
[771] SCHENK c. Suisse, arrêt du 12 juillet 1988, série A, n° 140.
[772] Arrêt BYKOV c. Russie, no. 4378/02, § 95, du 10 mars 2009.
[773] GAUTHIER, *Enregistrement clandestin*, p. 340.

476 Dans un arrêt du 16 juin 2008, le Tribunal fédéral a toutefois considéré que les informations recueillies par un agent infiltré en violation des prescriptions de la Loi fédérale sur l'investigation secrète (LFIS), singulièrement le défaut d'autorisation judiciaire, ne pouvaient être utilisées ni dans cette enquête ni dans d'autres. Il a retenu que la perquisition ordonnée sur la base de ces informations était illégale et que les éléments obtenus lors de la perquisition n'étaient pas utilisables non plus. Dans cette affaire le Tribunal fédéral a refusé d'exploiter les preuves illégales, y compris celles obtenues ensuite à l'aide des premières. Il n'a pas procédé à une pesée des intérêts, même si les faits reprochés étaient graves (tentative d'actes d'ordre sexuel avec un enfant et pornographie enfantine)[774]. Le Tribunal fédéral a confirmé ultérieurement qu'il ne procédait pas à une pesée d'intérêts car l'art. 18 al. 5 LFIS prévoyait que les éléments recueillis en l'absence d'autorisation n'étaient pas exploitables[775]. En matière de surveillance téléphonique, le Tribunal fédéral a déjà eu l'occasion de rappeler que la pesée d'intérêts ne s'applique pas lorsque la loi prévoit explicitement que la preuve irrégulière n'est pas exploitable, y compris pour les preuves subséquentes lorsque la preuve originaire en est une condition *sine qua non* d'obtention ou pour reprendre une autre formulation lorsque les preuves subséquentes sont indissociables de la preuve originaire[776].

477 La lettre de l'art. 141 CPP ne mentionne pas le fait que la preuve aurait pu être obtenue de manière légale, mais se limite à mentionner qu'elle est admissible si son exploitation est indispensable pour élucider des infractions graves. Il conviendra de voir comment la jurisprudence applique cette disposition, mais il n'est pas impossible que les tribunaux se contentent désormais d'accepter d'autant plus aisément les preuves illégales que l'infraction est grave, sans vérifier si la preuve pouvait être recueillie légalement.

478 Cette admissibilité des preuves illégales est inquiétante, car elle peut représenter une tentation pour l'autorité policière de procéder illégalement et obtenir ainsi les preuves nécessaires, qui seront ensuite admises malgré leur illégalité

[774] ATF 134 IV 287-288, Oberstaatsanwaltschaft des Kantons Zürich, du 16 juin 2008.
[775] ATF 6B_211/2009 du 22 juin 2006, consid. 1.4.
[776] ATF 133 IV 329, 331-332, X., du 9 octobre 2007 et 6B_211/2009 du 22 juin 2006, consid. 1.4.2.1.

formelle, alors que si elle procédait selon le CPP, elle ne pourrait les obtenir[777]. Le risque que le policier agissant de la sorte soit sanctionné à titre personnel est relativement faible. Si la surveillance n'aboutit pas, son auteur ne s'en vantera pas et l'autorité judiciaire n'en aura pas connaissance. Si elle débouche en revanche sur des résultats positifs, il y a fort à penser que l'on renoncera à sanctionner celui qui apporte la preuve de la commission d'un crime, d'autant plus si une autorité judiciaire autorise *a posteriori* l'utilisation des preuves récoltées. Le Tribunal fédéral écarte un tel risque d'un revers de main en rappelant que les preuves ne seraient pas admises en cas de violation systématique des prescriptions légales ou d'une atteinte grave[778]. Pour mémoire, les preuves expressément déclarées inexploitables par le CPP ne sont pas concernées par cette question.

d) Le sort de la preuve inexploitable

479 Si un moyen de preuve n'est pas exploitable, toutes les pièces qui s'y réfèrent sont retirées du dossier pénal et conservées à part jusqu'à la clôture définitive de la procédure, puis détruites. Les autres preuves obtenues grâce à la preuve déclarée inexploitable sont également inexploitables si la première preuve était la condition *sine qua non* pour les obtenir[779].

2. En matière de surveillance

480 L'art. 277 CPP prévoit que les résultats d'une surveillance non autorisée ne peuvent pas être exploités, et ce de manière absolue[780]. C'est le cas si l'autorisation n'a pas été accordée, si elle n'a pas été demandée, ou encore si elle n'a pas été prolongée[781]. Cela concerne uniquement la surveillance de la

[777] Elle est également critiquable car la garantie de procès équitable n'est pas sujette à une pesée d'intérêts, les droits de la défense sont absolus, et finalement toute personne est présumée innocente tant que sa culpabilité n'a pas été démontrée de façon légale : HOTTELIER, *Les droits de l'homme et la procédure pénale en Suisse*, pp 499-501.

[778] ATF 1P.51/2007 du 24 septembre 2007, consid. 3.5.6.

[779] Art. 141 CPP, *Message du CF relatif à l'unification de la procédure pénale*, pp 1163-1164. Sur la situation sous l'ancien droit : BÉNÉDICT, *Le sort des preuves illégales*, pp 239-250; SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*, pp 305-314.

[780] Sur la question des écoutes téléphoniques illégales en droit espagnol et français, avec des références à la jurisprudence de la CourEDH : SIMON, *Les preuves illicites*.

[781] ATF 131 I 272, 281, X., du 3 mai 2005, HANSJAKOB, *BÜPF und VÜPF Kommentar*, pp 250-253.

correspondance par poste et télécommunication, l'obtention de données relatives au trafic, à la facturation et à l'identification des usagers, ainsi que l'utilisation d'autres dispositifs techniques de surveillance[782]. Les résultats d'une surveillance non autorisée n'étant pas exploitables, ils ne pourront pas être pris en compte par l'autorité. Il ne sera pas nécessaire de répondre à la question de savoir si l'autorisation nécessaire aurait pu ou non être accordée[783].

Les informations obtenues dans le cadre d'une observation ou d'une surveillance des relations bancaires ne font pas partie des preuves citées comme inexploitables. On est donc face à un cas de preuves relativement inexploitables : elles peuvent être utilisées si elles sont indispensables pour élucider des infractions graves. 481

Le CPP prévoit que les documents et enregistrements collectés lors d'une surveillance non autorisée doivent être immédiatement détruits. Cette obligation l'emporte sur la communication de la surveillance et le droit de consulter le dossier qui en découle[784]. Si l'inexploitabilité immédiate et rétroactive de ces éléments est compréhensible, leur destruction ne devrait pas intervenir trop rapidement au risque de priver la personne visée par la surveillance de moyens de preuves importants pour réclamer une indemnisation au sens des art. 431ss CPP[785]. La destruction des documents ne doit pas non plus dispenser le ministère public d'informer la personne qui a été visée par la surveillance. Même si elle ne pourra pas consulter le résultat de la surveillance, elle a le droit de savoir qu'une surveillance a été opérée, dans quel but et sur la base (ou l'absence) de quelles décisions. 482

[782] Art. 281 al. 4 CPP.

[783] ATF 133 IV 329, X., du 9 octobre 2007, consid 4.4. Pour une critique de cet arrêt : HANSJAKOB, *Bemerkungen zur BGE 133 IV 329*, pp 214-215. Dans le même sens et pour une critique de la possibilité, avant l'entrée en vigueur du CPP, d'exploiter les résultats de certaines mesures de surveillance malgré l'absence d'autorisation : VETTERLI, *Bemerkungen zur BGE 1P.51/2007*, pp 84-86.

[784] Art 277 CPP. Voir aussi : BACHER, *Art. 277 CPP*, n 4 ad art. 277; HANSJAKOB, *BÜPF und VÜPF Kommentar*, p. 251.

[785] De manière plus judicieuse, l'art. 278 al. 4 CPP prévoit dans le cas de découvertes fortuites inexploitables que les documents et enregistrements doivent être conservés séparément et détruits immédiatement après la clôture de la procédure.

483 Ainsi, les éléments récoltés devraient être mis sous scellés et conservés séparément et la personne qui a fait l'objet d'une surveillance illicite devrait être informée. Ce n'est qu'une fois que la question de l'indemnisation sera définitivement réglée que les pièces mises sous scellés devraient pouvoir être détruites.

K. L'indemnisation en cas de surveillance illégale

484 L'art. 431 CPP prévoit que le prévenu qui a fait l'objet de mesures de contrainte de manière illicite a droit à une juste indemnité et à la réparation du tort moral[786]. Cette disposition est surtout prévue pour les cas de détention provisoire et de détention pour des motifs de sûreté, mais elle s'applique également aux autres mesures de contrainte comme les mesures de surveillance[787]. Cette indemnisation concerne le prévenu, soit toute personne qui, à la suite d'une dénonciation, d'une plainte ou d'un acte de procédure accompli par une autorité pénale, est soupçonnée, prévenue ou accusée d'une infraction (art. 111 CPP). Le fait que le prévenu soit finalement condamné ne s'oppose pas à l'octroi de l'indemnité[788].

485 Une disposition similaire est prévue pour les tiers à l'art. 434 CPP qui donne droit à la réparation du dommage et du tort moral causé par le fait d'actes de procédure ou du fait de l'aide apportée aux autorités pénales[789]. Cette disposition a pour but de permettre aux personnes qui subissent des mesures de contrainte telles que des perquisitions ou des écoutes téléphoniques d'obtenir une indemnisation sans avoir à chercher une base légale en dehors du droit procédural[790]. Seul le dommage direct est indemnisé[791]. Ces prétentions à

[786] GOLDSCHMID / MAURER / SOLLBERGER, *Kommentierte Textausgabe zur StPO*, pp 431-432; PIETH, *Schweizerisches Strafprozessrecht*, pp 221-222; SCHMID, *Handbuch*, pp 837-839; SCHMID, *Praxiskommentar*, pp 837-839.

[787] SCHMID, *Praxiskommentar*, p. 837.

[788] PIETH, *Schweizerisches Strafprozessrecht*, p. 222; SCHMID, *Handbuch*, p. 837. Pour l'indemnité en cas de détention, l'excès de la durée de détention se calcule toutefois en fonction de la durée de la peine ou de la sanction privative de liberté prononcée (et d'une éventuelle imputation du solde sur les sanctions prononcées à raison d'autres infractions).

[789] GOLDSCHMID / MAURER / SOLLBERGER, *Kommentierte Textausgabe zur StPO*, pp 434-435; PIETH, *Schweizerisches Strafprozessrecht*, p. 222; SCHMID, *Handbuch*, pp 841-842; SCHMID, *Praxiskommentar*, pp 843-845.

[790] *Message du CF relatif à l'unification de la procédure pénale*, p. 1315.

charge de l'Etat sont réglées dans le cadre de la décision finale, voire directement par le ministère public au stade de la procédure préliminaire[792].

Une mesure de contrainte n'est pas illicite du fait qu'elle ne permet pas la condamnation du prévenu. Elle est illicite lorsque les règles l'autorisant n'ont pas été respectées, qu'il s'agisse de conditions de fond ou de règles de formes. C'est par exemple le cas pour des écoutes téléphoniques opérées sans autorisation, pour poursuivre une infraction ne figurant pas dans le catalogue ou encore dont la durée dépasse celle de l'autorisation. Il est néanmoins à craindre, vu les dispositions régissant les preuves illégales, que la violation de simples prescriptions d'ordre en matière d'observation ou de surveillance des relations bancaires ne soit pas considérée comme suffisante pour ouvrir la voie à une indemnisation. 486

L'indemnisation et la réparation du tort moral sont fournies par l'Etat selon la libre appréciation de l'autorité compétente[793]. A cela s'ajoute la responsabilité causale prévue par l'art. 429 CPP en cas d'acquittement total ou partiel, ou encore en cas de classement : le prévenu a droit à une indemnité couvrant ses frais de défense, le dommage économique subi par sa participation obligatoire à la procédure et, dans les cas d'atteinte particulièrement grave à sa personnalité, la réparation du tort moral subi. 487

La Cour européenne des droits de l'Homme, lorsqu'elle constate une violation, peut accorder une satisfaction équitable servant à réparer le dommage subi, y compris le tort moral. Elle estime parfois que la reconnaissance des droits du requérant est suffisante et qu'une indemnité ne se justifie pas. De manière plus générale, la condamnation d'un pays conduit en principe celui-ci à modifier sa législation interne pour la mettre en conformité avec les exigences de la CEDH[794]. 488

[791] SCHMID, *Handbuch*, p. 841.

[792] Le ministère public est compétent lorsque le cas est clair (art. 434 al. 2 CPP).

[793] *Message du CF relatif à l'unification de la procédure pénale*, p. 1314.

[794] Pour des exemples en matière d'écoutes téléphoniques et de surveillance de la correspondance : RUEDIN, *Exécution des arrêts de la Cour européenne des droits de l'homme*, pp 294-295 et 306-307.

III. Synthèse et critique de la surveillance selon le CPP

A. En général

489 La réglementation consacrée aux mesures de surveillance dans le Code de procédure pénale est globalement conforme aux exigences du droit supérieur. Le CPP est une base légale claire et accessible, rendant prévisibles les cas et les conditions d'utilisation, et prévoyant des autorités de recours.

490 La surveillance doit être proportionnée et des mesures moins invasives, lorsqu'elles sont possibles, doivent lui être préférées. Elle est prioritairement dirigée contre le prévenu et elle n'a lieu que lorsque des soupçons suffisants laissent présumer qu'une infraction a été commise. La surveillance préventive ou générale est ainsi exclue.

B. Les mesures de surveillance

1. Les mesures actuelles et futures

491 Sous le chapitre « mesures de surveillance secrètes », le Code de procédure pénale prévoit la surveillance de la correspondance par poste et télécommunication ainsi que la récolte de données relatives au trafic, à la facturation et à l'identification des usagers, la surveillance des relations bancaires, l'observation et les autres dispositifs techniques de surveillance. D'autres dispositions du CPP permettent la recherche de personnes, ainsi que la récolte et l'analyse d'ADN ou d'autres données biométriques.

492 Le législateur n'a pas vraiment prévu de place pour l'évolution future de la technique et a oublié certaines mesures de surveillance. Il y a certes la disposition sur les autres dispositifs de surveillance prévus par l'art. 280 CPP, soit 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. Cet article vise surtout

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.

493 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 autres que celles citées avant[795]. 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[796]. 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.

2. Les mesures oubliées

494 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. Parmi ces oublis malheureux[797], il y a tout d'abord la surveillance des relations bancaires en temps réel. Les art. 284ss CPP ne précisent pas ce que le législateur entend par surveillance des relations bancaires. L'examen des travaux préparatoires laisse penser qu'il a complètement perdu de vue que l'intérêt dans la surveillance des relations bancaires était la surveillance en temps réel, vu que les autres informations et documents peuvent être réclamés par une simple injonction de dépôt ou une mesure de séquestre. Il serait également illogique d'imposer l'autorisation du

[795] *Message du CF relatif à l'unification de la procédure pénale*, p. 1234.

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

[797] Le fait que l'autorité policière ne sache pas si une mesure de surveillance pourrait être admise ou comment obtenir l'autorisation la poussera à l'utiliser sans qu'elle ne figure dans le dossier à titre de preuve : BOSONNET, *In der Dunkelkammer geheimer Polizeimethoden*, p. 14.

tribunal des mesures de contrainte pour obtenir des extraits de comptes bancaires alors que le ministère public reste compétent pour les perquisitions et les séquestres.

495 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 eût été préférable de régler à l'avance et de manière générale ces questions, comme en matière de surveillance de la correspondance. En l'espèce, un établissement bancaire pourrait se voir obligé de répondre dans des formes différentes selon que la demande émane d'un canton ou d'un autre. Les conséquences de l'impossibilité pour une banque de fournir certaines informations ne sont pas non plus résolues. Des compétences pourraient être accordées dans ce sens au Service de surveillance de la correspondance et des télécommunications (Service SCPT)[798]. Ce Service, ou le Département fédéral de justice et police, pourrait alors adopter des normes techniques auxquelles les banques devraient se conformer. Ainsi une véritable surveillance en temps réel serait mise en place au lieu de demandes de documents continuelles dont les résultats dépendront tout autant de l'établissement bancaire sollicité que du tribunal requérant.

496 L'installation d'un « cheval de Troie » ou « Government-Software » n'a pas été prévue par le CPP. Selon l'utilisation qui en est faite, il peut servir à surveiller la correspondance électronique, mais également l'activité d'un ordinateur sans qu'il y ait de communications. Le « cheval de Troie » doit être permis en application de l'art. 280 CPP tant qu'une disposition spécifique n'est pas introduite dans le CPP. Il n'a pas exactement pour but d'enregistrer des conversations non publiques ou des actions se déroulant dans des lieux qui ne sont pas publics ou librement accessibles, mais il entre dans le champ plus large de la récolte d'informations qui ne sont pas librement accessibles, ce que permet

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

l'interprétation de l'art. 280 CPP[799]. Pour les mêmes raisons, les appareils servant à intercepter des champs électromagnétiques doivent être considérés comme des autres dispositifs de surveillance[800].

497 L'avant-projet de révision de la LSCPT prévoit d'introduire un nouvel art. 270bis CPP qui autoriserait l'installation d'un « cheval de Troie » et le décryptage de données. Cette mesure est conçue comme une mesure de surveillance de la correspondance subsidiaire aux autres mesures de surveillance de la correspondance par télécommunication, bien qu'elle permette finalement d'accéder à l'ensemble des données présentes sur le système informatique, y compris celles qui ne font pas partie de la correspondance. Il eût probablement été plus judicieux d'ajouter une lit. d à l'article 280 et d'en faire une autre mesure technique de surveillance, au lieu de l'insérer parmi la surveillance de la correspondance avec des conditions un peu différentes[801].

498 L'IMSI-Catcher doit, quant à lui, 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 recours de l'opérateur ou du Service SCPT n'est pas nécessaire. Ce sera aussi le cas si l'IMSI-Catcher est utilisé pour localiser un téléphone, contrairement à la détection de puces RFID qui appartient à la catégorie des 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[802].

499 Finalement la récolte d'échantillons d'écriture et de voix en l'absence d'accord de la personne concernée n'est pas prévue, alors que la récolte d'ADN et son analyse sont admis. Une fois encore le législateur n'a pas voulu exclure ce moyen, mais a plutôt oublié que ces méthodes existaient et pouvaient être

[799] Même s'il se rapproche par son objet le plus souvent de la surveillance de la correspondance, son objet peut être plus large et en l'état, seul l'art. 280 CPP peut servir de base légale.

[800] SCHMID, *Handbuch*, p. 529.

[801] *Rapport du CF relatif à l'AP LSCPT*, pp 41-43.

[802] Voir pour l'IMSI-Catcher le chapitre 3. Les écoutes téléphoniques, p. 38 ci-dessus et pour les puces RFID le chapitre 9. Les puces RFID, p. 62 ci-dessus.

utilisées dans un but de surveillance. Il faut ici aussi retenir que l'on à faire à un cas d'utilisation d'autres dispositifs de surveillance. Ces dispositions devraient de toute façon êtres appliquées lorsque le dispositif mis en place est un micro, une surveillance vidéo ou un dispositif de type « cheval de Troie ».

C. La procédure d'autorisation

1. Les différentes procédures de mise sous surveillance

500 Les mesures de surveillance ne sont pas toutes ordonnées selon la même procédure. La procédure que prévoyait la LSCPT (dans sa teneur avant l'entrée en vigueur du CPP) est la procédure que l'on pourrait qualifier de normale : 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 et l'utilisation d'autres dispositifs de surveillance.

501 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. La police peut ordonner une observation ne dépassant pas un mois, l'émission d'un avis de recherche en cas d'urgence, le prélèvement non invasif d'ADN sur des traces ou sur une personne et l'analyse de l'ADN sur la base de traces récoltées (mais non pas sur la base du prélèvement effectué sur une personne). Le ministère public dispose des compétences accordées à la police, mais peut en plus autoriser la poursuite d'une observation au-delà d'un mois, ordonner la recherche d'une personne ou lancer un avis de recherche, astreindre une personne à fournir un échantillon d'écriture ou de voix, ordonner la saisie de données signalétiques en cas de refus de la personne concernée, ordonner un prélèvement invasif d'échantillon d'ADN et l'analyse de l'échantillon d'ADN prélevé sur une personne.

2. Le cas particulier des mesures ordonnées par le tribunal des mesures de contrainte

Le législateur a prévu une procédure particulière pour le prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure et la surveillance des relations bancaires. Cette répartition différente des compétences est inutile et ne fait que compliquer la situation. Si elle est défendable pour le prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure, la surveillance des relations bancaires doit en revanche obéir aux mêmes règles que la surveillance de la correspondance[803]. Une modification légale est donc nécessaire et il serait judicieux d'en profiter pour régler l'exécution de la surveillance, plus particulièrement les tâches des établissements bancaires et d'un service de surveillance géré par la Confédération (ces tâches pourraient être confiées au Service SCPT rattaché administrativement au Centre de services informatiques du Département fédéral de justice et police CSI-DFJP). Ce service pourrait aussi rédiger des directives techniques précisant les obligations des banques, la manière dont les données doivent être transmises, les délais accordés à l'établissement bancaire et les mesures à prendre pour assumer les cas urgents, etc[804]. 502

Si le prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure n'a généralement pas de caractère urgent et qu'il porte une atteinte particulière aux personnes concernées, la procédure prévue pour la surveillance de la correspondance eût été suffisante. En retirant cette compétence au procureur pour la confier à un tribunal, le législateur a peut-être cru qu'il soumettrait cette mesure à un meilleur contrôle, mais il a perdu de vue que si l'autorité qui ordonnait la mesure était désormais une autorité judiciaire indépendante, il 503

[803] L'avant-projet de Code de procédure pénale donnait la compétence au ministère public d'ordonner seul une surveillance des relations bancaires d'une durée d'un mois (art. 318ss AP-CPP). Sans explication, le projet a changé.

[804] L'avant-projet de révision de la LSCPT ne prévoit plus de compétences du service SCPT en matière de surveillance de la correspondance par poste. Il étend en revanche les compétences en matière de surveillance de la correspondance dans le domaine par télécommunication, notamment en cas de difficultés techniques (art. 16 AP LSCPT). Le service exercera également le rôle d'autorité de surveillance (art. 33 AP LSCT) : *Rapport du CF relatif à l'AP LSCPT*, pp 39-40.

excluait ainsi le contrôle automatique qu'assurait le tribunal des mesures de contrainte, empêchant tout recours au niveau cantonal.

504 Pour ce qui est de la surveillance des relations bancaires, le texte légal varie malheureusement selon la langue consultée. Si l'on s'appuie sur le message du Conseil fédéral, on devrait retenir que le ministère public ne fait que proposer une mesure qui entrera en vigueur avec la décision du tribunal des mesures de contrainte, ce dernier devant encore définir les modalités de la surveillance. Aucun délai ne lui est fixé pour se prononcer. Cette procédure est applicable si elle ne concerne que la production de documents bancaires existants ou futurs et non une véritable surveillance en temps réel. Le CPP aurait pu se contenter de la possibilité existant pour le ministère public de prononcer une injonction de dépôt ou une mesure de séquestre. La surveillance des relations bancaires en temps réel pourrait alors être assimilée à l'utilisation d'un dispositif technique de surveillance et soumise à la procédure normale d'autorisation. La surveillance en temps réel implique la mise en place par l'institut bancaire de moyens informatiques assurant une surveillance systématique[805].

505 La surveillance des relations bancaires au sens des art. 284ss CPP doit aussi être considérée comme étant une surveillance en temps réel. C'est en effet la seule possibilité de donner une raison d'être à ces règles spéciales par rapport aux autres possibilités d'obtenir des documents relevant de la compétence du ministère public. Du point de vue de la systématique ensuite, la surveillance des relations bancaires figure dans le titre consacré aux mesures de surveillance secrètes. Ces mesures ont toutes lieu, au moins en partie, en temps réel[806]. Ainsi nous retiendrons que le ministère public ordonne la surveillance et que le tribunal des mesures de contrainte l'autorise, comme en matière de surveillance de la correspondance et de l'utilisation des autres dispositifs de surveillance. C'est donc évidemment au ministère public qu'il reviendra de donner des directives à la banque, directives que le tribunal pourra ensuite librement

[805] SCHMID, *Praxiskommentar*, p. 539. Il ne faut pourtant pas y voir un autre dispositif technique de surveillance, puisque les logiciels utilisés par les opérateurs téléphoniques lors de l'exécution de la surveillance de la correspondance ne le sont pas non plus. On se rend néanmoins compte du problème si la surveillance bancaire est doublée de l'utilisation d'un autre dispositif puisqu'il faudrait suivre deux procédures d'autorisation différentes.

[806] La surveillance de la correspondance prévoit une surveillance rétroactive, mais elle est traitée séparément.

compléter ou modifier. Les normes prévues pour la surveillance de la correspondance concernant les délais, le sort réservé aux découvertes fortuites et la communication sont également applicables par analogie.

D. L'information

1. La communication

Le CPP appelle communication (art. 279 CPP) l'information transmise à la fin d'une surveillance secrète. La simple mention du résultat d'une mesure de surveillance dans un dossier ou au cours d'un interrogatoire ne remplace pas la communication, qui est d'ailleurs la seule information officielle qui est faite de l'existence d'une mesure de surveillance. Le ministère public est responsable de cette information, même si la surveillance nécessitait l'approbation du tribunal des mesures de contrainte. Elle doit avoir lieu dès que possible mais dans tous les cas avant la clôture de l'instruction pour permettre à la personne de faire valoir correctement ses droits[807]. 506

La communication a la particularité d'ouvrir la voie à un recours contre la surveillance (contrôle *a posteriori*) et de marquer le point de départ du délai de recours. Ce n'est, selon le Tribunal fédéral, qu'à partir de là qu'une éventuelle contestation de la surveillance est recevable[808]. En plus de la mention de cette voie de recours, la communication doit préciser le type et la durée de la surveillance, sa raison, pourquoi et par qui elle a été ordonnée/autorisée, ainsi que la possibilité de consulter le dossier. 507

Le ministère public, avec l'accord du tribunal des mesures de contrainte, peut différer la communication, voire renoncer à communiquer l'existence d'une surveillance si des intérêts publics ou privés l'exigent. Dans ce cas, l'exploitation des résultats de la surveillance à titre de preuve est interdite. A mesure que la personne surveillée n'a pas connaissance de la surveillance et 508

[807] Même si le CPP mentionne qu'elle peut avoir lieu lors de la clôture de la procédure préliminaire. La communication simultanément à la clôture n'empêche pas le recours contre la surveillance, mais elle rend plus compliquée l'administration de moyens de preuves que la connaissance de la surveillance peut suggérer aux parties.

[808] Sur la nécessité d'admettre un recours déjà avant la communication, voir le chapitre 2. Les voies de droit manquantes, p. 230 ci-dessous.

qu'elle ne peut donc ni la contester ni démontrer que certaines informations peuvent être erronées, les résultats de la surveillance ne devraient pas être exploitables qu'il s'agisse ou non de preuves.

509 Vu l'importante atteinte à la sphère privée causée par les mesures de surveillance et le fait que la personne surveillée n'en a pas connaissance, il devrait y avoir un contrôle de l'information des personnes surveillées. Une autorité judiciaire indépendante devrait être informée des autorisations de surveillance, des communications et des renonciations à une communication. Elle pourrait se prononcer sur le bien-fondé de ces décisions, ainsi que sur le cercle des personnes à informer.

2. Les personnes concernées

510 La personne qui a été l'objet principal de la surveillance pénale doit évidemment être informée. La question est plus délicate de savoir jusqu'où s'étend cette obligation spontanée d'informer. D'un côté, il est tentant d'exiger que toute personne qui a été visée, de près ou de loin, soit informée qu'elle a été surveillée, des raisons pour lesquelles elle l'a été et de ce qui a été retenu. En plus des difficultés pratiques, une information très large représente le risque de permettre à un grand nombre de personnes de savoir qu'un de leurs contacts a été l'objet d'une surveillance et dans quel cadre. Le droit d'être informé des tiers pour pouvoir faire contrôler l'atteinte portée à leur sphère privée s'oppose ici au droit à la protection de la sphère privée de la personne surveillée qui ne souhaite souvent pas que tous ses correspondants sachent qu'il a été l'objet d'une surveillance et la raison qui y a conduit.

511 Il convient de procéder à une pesée d'intérêts et de distinguer trois groupes de personnes. Ce sont premièrement celles qui n'ont été visées qu'occasionnellement par la mesure de surveillance, par exemple parce qu'elles ont eu un contact avec la personne surveillée sans lien avec la raison de la surveillance, et au sujet desquelles aucun résultat de surveillance ne sera exploité. Si les personnes appartenant à ce premier groupe n'ont pas besoin d'être informées, le droit de recourir contre une mesure de surveillance et de consulter les résultats de la surveillance les concernant doivent leur être reconnus. Ces personnes devraient également être informées si elles venaient à

s'en inquiéter auprès de l'autorité ayant ordonné, autorisé ou exécuté la surveillance.

Deuxièmement, il y a les personnes qui ne sont pas directement visées par la surveillance mais qui ont été régulièrement surveillées. Il s'agit par exemple du conjoint ou du colocataire de la personne surveillée avec qui il partage un raccordement téléphonique fixe. Le risque d'informer une personne qui n'aurait pas été au courant est ici mis en balance avec l'intensité de la surveillance qui justifie une information. De plus la proximité entre ces personnes, parfois simplement de fait, commande également que l'information puisse être transmise plus facilement. 512

On trouve finalement les personnes qui n'étaient pas visées par la surveillance et qui n'ont pas été surveillées très régulièrement, mais pour lesquelles le résultat de la surveillance a été exploité. Le résultat de la surveillance n'est évidemment pas utilisé à leur encontre[809], mais il sera conservé et exploité dans une procédure judiciaire. Ces personnes ont donc le droit de connaître comment elles ont été mêlées à un délit pénal. Il est également important qu'elles sachent que des données les concernant sont enregistrées et utilisées, ce qui justifie également qu'elles soient informées. 513

E. Les voies de recours

1. Le contrôle *a posteriori*

Le CPP ne prévoit pas de voie de recours contre les décisions du tribunal des mesures de contrainte autorisant une surveillance, mais une procédure particulière de contrôle *a posteriori* : le recours contre la surveillance. Ce recours cantonal est formellement dirigé contre la communication, alors que matériellement il permet de faire contrôler, en fait et en droit, toute la procédure de surveillance et surtout d'éliminer les résultats obtenus si la procédure n'a pas été respectée. 514

[809] Sinon une autorisation serait nécessaire au sens de l'art. 278 al. 2 CPP et la personne recevrait une information personnelle.

515 Un recours en matière pénale peut ensuite être déposé devant le Tribunal fédéral contre la décision rendue en dernière instance cantonale, ainsi que contre la décision du tribunal des mesures de contrainte autorisant le prélèvement d'échantillons d'ADN lors d'enquêtes de grande envergure. Les décisions du tribunal des mesures de contrainte ne sont sujettes à recours que si la loi le prévoit (ce qui n'est pas le cas en l'espèce) et le CPP ne prévoit pas de communication pour cette mesure. L'absence de recours cantonal étant contraire à l'esprit du CPP et le texte de la loi n'excluant pas un recours comme le font d'autres dispositions, il est admissible de considérer qu'il s'agit d'une lacune et retenir, par analogie avec les autres mesures de surveillance, qu'un recours cantonal est recevable. La décision ordonnant de se soumettre au prélèvement est assimilée à la communication.

2. Les voies de droit manquantes

516 Le CPP ne permet actuellement pas de recourir contre une surveillance s'il n'y a pas eu de communication, que le tribunal des mesures de contrainte ait donné son accord pour y renoncer, que la communication soit différée, ou que le ministère public ait considéré que la communication à la personne souhaitant finalement recourir n'était pas nécessaire. Apparemment, seul un recours au Tribunal fédéral invoquant le droit à un recours effectif garanti par la Convention européenne des droits de l'homme serait envisageable, et cela malgré le texte clair de la loi qui l'exclut[810]. Le recours à la suite de la communication d'une observation, bien qu'évident, n'est pas mentionné dans la loi[811].

517 Il est nécessaire de permettre un recours plus large contre la surveillance. Le plus simple est d'admettre la recevabilité du recours également lorsqu'aucune communication n'a (encore) eu lieu. Un recours pourrait alors être déposé en tout temps. Une modification législative n'est pas obligatoire, puisque c'est une jurisprudence du Tribunal fédéral qui exclut pour l'instant la recevabilité d'un tel recours. Une précision dans la loi que le recours est également ouvert en l'absence de communication permettrait de clarifier la situation et serait

[810] Art. 6 et 13 CEDH. Le Tribunal fédéral pourrait s'estimer compétent pour entrer en matière afin d'éviter une violation de la CEDH (et une condamnation par la CourEDH) : ATF 125 II 417, 425- 426, A., du 26 juillet 1999.

[811] Art. 283 CPP.

l'occasion de préciser le sort à réserver à celui-ci si une surveillance est en cours. Le contrôle *a posteriori* n'a pas pour but de permettre de savoir si une surveillance a actuellement lieu. Pour cette raison la loi devrait prévoir la possibilité de différer la réponse au plus tard jusqu'à la clôture de l'instruction, par analogie avec le droit d'accès prévu par l'art. 9 LPD.

F. Les résultats de la surveillance

1. Les données à conserver et à détruire

La mise en place d'une mesure de surveillance conduit la plupart du temps à l'obtention d'un très grand nombre de données, plus ou moins utiles et plus ou moins utilisables. Dans tous les cas l'intégralité de ces données doit être conservée jusqu'à fin de cause sous leur forme originale, et cas échéant également sous leur forme transformée (traitement, traduction, modifications, etc.). C'est l'unique moyen de pouvoir contrôler l'authenticité des informations utilisées en cas de contestation. Un accès libre et complet doit être assuré au prévenu ou à son défenseur.[812] 518

Il n'est en revanche pas nécessaire que toutes ces informations figurent à titre de preuves dans le dossier principal de la cause. Une annexe au dossier contenant tous les résultats considérés par les enquêteurs comme inutiles est parfaitement admissible, si les parties y ont également accès et qu'elles peuvent demander à la direction de la procédure d'en utiliser certaines à titre de preuves. 519

La conservation de ces données une fois la procédure terminée est de nature à causer un dommage important, le plus souvent sans aucune justification. Le CPP aurait dû prévoir la destruction de tous les résultats de la surveillance, y compris les copies encore en mains des services de police, dès que la cause n'est plus susceptible de recours. En l'absence de dispositions *ad hoc*, il revient à l'autorité de jugement d'ordonner la destruction de ces pièces comme elle le fait avec les séquestres. Une modification du CPP introduisant une destruction automatique 520

[812] L'avant-projet de révision de la LSCPT prévoit que les données ne seraient plus transmises sous forme de DVD comme actuellement, mais qu'un droit d'accès informatique à distance serait accordé (art. 9 et 11 AP LSCPT). A moins que la défense dispose du même droit d'accès que la police et les instances judiciaires (ce qui ne semble pas être prévu), cette méthode n'est pas acceptable vu que l'accès intégral ne sera plus garanti.

pallierait les oublis et permettrait à la personne concernée d'obtenir la destruction après la clôture de la cause, sans devoir entamer une nouvelle procédure dans laquelle elle devrait démontrer que la conservation de ces données lui cause un dommage important. Un délai de dix jours à compter du jugement définitif paraît adéquat si l'on précise que les données peuvent être conservées plus longtemps si le dépôt d'une requête devant la Cour européenne des droits de l'Homme est envisagé.

2. Les données illégales et les données protégées

521 Les preuves qui sont recueillies par des moyens restreignant les facultés intellectuelles ou le libre arbitre, ou encore obtenues par des menaces, des promesses, ou le recours à la force sont interdites et inexploitables. Le CPP considère également comme inexploitables les preuves issues d'une mesure de surveillance de la correspondance non autorisée. Les preuves inexploitables sont totalement inutilisables, autant comme preuve dans la procédure que comme simple information que la police utiliserait pour son enquête. Il en est de même des éléments obtenus grâce aux preuves illégales.

522 Ces données doivent être immédiatement écartées du dossier. Elles doivent être détruites, mais il faut s'assurer auparavant que la personne surveillée ait bien été informée et qu'elle puisse faire valoir ses droits à une indemnisation. Dans cette optique, il devrait être admis de conserver ces informations sous scellés, un magistrat indépendant de la cause pouvant alors les consulter pour prendre les mesures nécessaires concernant la communication et l'indemnisation. Une fois ces questions résolues, elles doivent être définitivement détruites.

523 Le CPP prévoit expressément l'inexploitabilité des preuves recueillies sans autorisation en matière de surveillance de la correspondance (art. 277). Pour les autres mesures de surveillance, cette disposition doit être appliquée par analogie. Sinon on se retrouverait face à un cas de preuves relativement inexploitables, c'est-à-dire qu'elles sont admises pour élucider une infraction grave. La procédure d'autorisation et de contrôle serait vidée de sa substance pour les infractions graves, ce qui n'est pas admissible. La jurisprudence du Tribunal fédéral antérieure au CPP exigeait dans de tels cas que la preuve eût pu être recueillie légalement, ce que le CPP ne semble plus exiger.

Les mesures techniques de surveillance causent une atteinte importante aux droits de l'individu, raison pour laquelle une procédure particulière a été prévue et doit toujours être respectée. Tous les éléments obtenus au mépris de cette procédure doivent être inutilisables 524

Les informations couvertes par le secret professionnel sont également inexploitables, sauf si la surveillance est dirigée contre le détenteur du secret. Des mesures adéquates doivent néanmoins être prises pour protéger les dépositaires du secret professionnel qui ne sont pas visés par la surveillance, notamment par le tri des informations par une autorité judiciaire indépendante. Les informations écartées doivent être détruites sans délai. Un tri doit aussi être effectué, même s'il est difficile en pratique, chaque fois que des données couvertes par le secret professionnel apparaissent ou sont susceptibles d'apparaître pendant la surveillance. 525

La surveillance est autorisée pour prouver la commission de certaines infractions par la personne mentionnée dans l'autorisation de surveillance. En dérogation à ce principe, le CPP admet que soient retenues les preuves liées à la commission d'autres infractions par la personne surveillée ou d'infractions commises par une autre personne, à la condition qu'une autorisation « rétroactive » puisse être obtenue aux conditions habituelles. Sinon ces preuves sont considérées comme illégales et inexploitables. Ce n'est en effet pas parce qu'un prévenu est poursuivi pour des infractions justifiant une mesure de surveillance que l'on doit admettre également une surveillance pour les infractions pour lesquelles la loi n'en admet pas. Le CPP a prévu cette réglementation pour la surveillance de la correspondance, mais elle doit évidemment s'appliquer à toutes les mesures soumises à autorisation. 526

Quatrième partie :
la surveillance préventive (selon la LMSI)

I. Remarques préliminaires

Alors que le Code de procédure pénale (CPP) est la disposition légale de référence en matière de surveillance dans le cadre de l'instruction pénale, la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) est la principale loi régissant la surveillance préventive civile. 527

La surveillance préventive n'est pas la conséquence de la commission d'une infraction, mais elle intervient en amont pour détecter et éviter la réalisation d'un danger pour la sécurité. C'est une activité typique de renseignement. 528

Nous nous attacherons donc à présenter les différents cas de surveillance préventive prévus par la LMSI. Comme pour la procédure pénale, la procédure, les conditions et le contrôle seront abordés. Vu les procédures de contrôle limitées, un accent particulier sera mis sur les droits d'accès. Le projet de modification de la LMSI visant à étendre les pouvoirs d'investigation sera également abordé. 529

II. Exposé de la procédure prévue par la LMSI

A. Les mesures de surveillance

1. En général

530 La Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) donne à la Confédération la compétence de prendre des mesures préventives pour détecter précocement certains dangers et les combattre[813]. Il s'agissait initialement des dangers liés au terrorisme, au service de renseignement prohibé et à l'extrémisme violent[814]. La violence lors de manifestations sportives a été ajoutée lors de l'Euro 2008 (art. 2 al. 1 LMSI)[815]. Ces mesures de surveillance ne concernent pas des infractions déjà commises, mais elles ont pour but d'éviter la commission future d'infractions[816].

531 Les mesures techniques de surveillance entrent dans le cadre des mesures préventives, particulièrement le traitement des informations relatives à la sûreté intérieure et extérieure, les contrôles de sécurité relatifs à des personnes et les mesures de protection (art. 2 al. 4 lit. b à d LMSI). Le législateur a cependant expressément interdit au Service d'analyse et de prévention (SAP) d'avoir recours à des mesures de contrainte et d'observer des faits dans des locaux privés, tel que cela est autorisé dans le cadre de procédures pénales[817].

[813] Sur la sécurité intérieure en Suisse en général : MÜLLER, *Innere Sicherheit Schweiz*, pp 393-496.

[814] Le service de renseignements prohibé correspond aux infractions suivantes : service de renseignements politiques (art. 272 CP), service de renseignements économiques (art. 273 CP), service de renseignements militaires (art. 274 CP) et espionnage militaire au préjudice d'un Etat étranger (art. 301 CP) : *Message du CF concernant la LMSI*, p. 1169.

[815] BICHOVSKY, *Prévention de la violence commise par les spectateurs*, pp 208-211 et 264-265.

[816] Le renseignement en général doit aussi permettre l'ouverture d'enquêtes pénales portant sur des infractions déjà commises, mais il ne doit pas servir à obtenir ce que la procédure pénale ne permet pas.

[817] *Message du CF relatif à la LMSI II*, p. 4784.

Parallèlement, l'art. 99 de la Loi du 3 février 1995 sur l'armée et l'administration militaire (LAAM) vise la recherche d'informations sur l'étranger qui sont importantes pour l'armée. Cette disposition est notamment complétée par l'Ordonnance du 4 décembre 2009 concernant le Service de renseignement de l'armée[818] et l'Ordonnance du 15 octobre 2003 sur la guerre électronique[819]. Si l'OSRA est limitée au renseignement militaire, l'art. 99 LAAM et l'OGE concernent également l'exploration radio civile, raison de leur mention ici[820]. 532

L'appartenance ou le soutien à une organisation criminelle et le financement du terrorisme constituent des infractions pénales en tant que telles (art. 260ter et 260^{quinquies} CP), de sorte que les mesures de surveillance prévues par le CPP peuvent être ordonnées dans le cadre d'une instruction pénale. Le recours à des mesures de surveillance plus limitées au sens de la LMSI n'est donc pas nécessaire. 533

2. La recherche d'informations

a) Les moyens utilisés

Les moyens utilisables pour la recherche d'informations sont énumérés à l'art. 14 al. 2 LMSI, complété par les art. 16ss de l'Ordonnance sur le Service de renseignement de la Confédération (OSRC)[821]. En plus de l'exploitation des sources accessibles au public et de la consultation de documents officiels, le Service d'analyse et de prévention (SAP) reçoit directement des informations 534

[818] OSRA, RS 510.291. Jusqu'à fin 2009, c'était l'Ordonnance du 26 septembre 2003 sur l'organisation des services de renseignements au sein du Département fédéral de la défense de la protection de la population et des sports (Orens).

[819] OGE, RS 510.292.

[820] Depuis le 1er janvier 2010, l'art. 18 OSRC sert de base légale pour l'exploration radio. Précédemment, c'était l'art. 9a OMSI qui servait de base légale pour l'exploration radio. Le Conseil fédéral avait admis que cette base légale devait figurer dans une loi formelle comme la LMSI : *Message du CF relatif à la LMSI II*, pp 4822-4824; FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 37-38. Nous regrettons que, malgré l'adoption de la loi sur le renseignement civil, l'exploration radio continue à reposer sur une simple ordonnance.

[821] RS 120.52.

des autorités cantonales et fédérales (art. 4 OSRC)[822]. Il peut demander des renseignements, le relevé des déplacements et des contacts de personnes, la surveillance de lieux publics et librement accessibles, y compris au moyen d'enregistrements d'images et de sons, ainsi que l'interpellation de personnes et des recherches sur leur lieu de séjour en vue d'établir leur identité. Le Service d'analyse et de prévention ne mène pas d'observations vidéo permanentes de certains lieux, mais il se limite à l'enregistrement de certains événements lorsqu'il effectue des observations. Il recourt en revanche aux enregistrements vidéo que les organes de sécurité et de police ont réalisés sur le fondement de leurs propres bases légales[823].

535 L'analyse des rayonnements électromagnétiques émanant d'installations techniques ou de systèmes de télécommunication, aussi connue sous le nom d'exploration radio, n'est autorisée que pour les systèmes de télécommunications et installations techniques situés à l'étranger. Elle est réglée par l'art. 18 OSRC et l'Ordonnance sur la guerre électronique[824]. L'exploration radio peut être réalisée à la demande du Service de renseignement stratégique, du Service d'analyse et de prévention ou du Service de renseignement militaire.

536 L'art. 18 al. 2 OSRC permet une forme d'exploration radio particulière en Suisse : les rayonnements électromagnétiques qui ne sont pas soumis au secret des télécommunications. Cette disposition vise notamment les rayonnements émis en ondes courtes et ne disposant pas de moyens les protégeant d'une réception par des tiers[825]. Le recours à des mesures de contrainte prévues par la procédure pénale et l'observation de faits dans des locaux privés ne sont pas autorisés au stade préventif. Ces mesures ne peuvent être prises qu'après

[822] Des enregistrements d'images et de sons effectués par les organes cantonaux de police et de sûreté peuvent aussi être remis au SAP.

[823] Art. 17 OSRC (précédemment art. 9 OMSI), DFJP, *Rapport sur la vidéosurveillance*, p. 20.

[824] Ordonnance du 15 octobre 2003 sur la guerre électronique (OGE, RS 510.292).

[825] L'art. 9a al. 2 OMSI a été remplacé par l'art 18 al. 2 LMSI le 1er janvier 2010. *Message du CF relatif à la LMSI II*, p. 4822; FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, p. 37.

l'ouverture d'une procédure formelle d'enquête de police judiciaire ou d'une instruction préparatoire (art. 14 al. 3 LMSI)[826].

537 L'Etat ne bénéficie actuellement pas du droit de procéder à une surveillance préventive de manière beaucoup plus étendue qu'une personne privée[827]. Il bénéficie en revanche de compétences nettement plus larges en matière de traitement des informations dont il dispose. Les organes de sûreté peuvent établir et traiter des profils de personnalité des personnes soupçonnées d'avoir un comportement représentant une menace pour la sûreté de la Suisse. Ils peuvent également traiter d'autres données sensibles s'il ressort d'informations existantes que ces données ont un lien avec la préparation ou l'exécution d'activités terroristes, d'espionnage ou d'extrémisme violent, ou ont un lien avec le crime organisé (art. 21 OSRC).

b) Les opérations préventives et les programmes de recherche préventifs

538 Les opérations préventives, les programmes de recherche préventifs et les procédures d'examen sont des formes particulières de la recherche d'informations. Les opérations préventives sont des actions concentrées pour traiter des cas dont l'importance, l'étendue, les moyens requis ou le maintien du secret dépassent le cadre normal d'une investigation de service de renseignement. Les programmes de recherche préventifs sont des opérations de police de longue haleine servant à détecter des faits intéressants la sécurité dans un domaine délimité. Ils sont organisés en collaboration avec les autorités cantonales de poursuite pénale. Le Service d'analyse et de prévention décide de la mise en œuvre des opérations et programmes de recherche préventifs. Il fixe par écrit le but, la durée et les moyens à engager, ainsi que la périodicité et la forme des comptes rendus. Il évalue par écrit au moins une fois par année dans quelle mesure la poursuite des opérations et programmes de recherche préventifs s'impose (art. 24 OSRC).

[826] Art. 14 LMSI et 8ss LMSI, *Rapport du CF à la suite des attentats terroristes du 11 septembre 2001*, p. 1713; FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 7 et 18.
[827] MÉTILLE, *L'utilisation privée de moyens techniques de surveillance*.

c) La procédure d'examen

539 La procédure d'examen sert à recueillir et à exploiter toutes les informations concernant des Suisses, des personnes domiciliées en Suisse ou des organisations et des groupements actifs en Suisse déployant de manière systématique des activités compromettant la sûreté de la Suisse. Une telle procédure peut être ouverte s'il y a présomption, sur la base d'indices concrets, que des activités relevant des domaines énumérés à l'art. 25 OSRC sont déployées[828]. La procédure d'examen doit être revue au moins une fois par semestre pour savoir si les conditions de sa poursuite sont encore réunies.

d) La liste d'observation

540 Le DDPS dresse également une liste d'observation qui est confidentielle[829]. Elle mentionne les faits qui doivent être communiqués au Service d'analyse et de prévention mais qui ne peuvent pas être publiés en raison de l'obligation de maintenir le secret, ainsi que des organisations et groupements dont l'activité ou les membres sont concrètement soupçonnés de menacer la sûreté intérieure ou extérieure et au sujet desquels il y a lieu de communiquer toutes les informations possibles. Le Service d'analyse et de prévention traite toutes les informations que l'on peut obtenir sur ces organisations et groupements, ainsi que sur leurs protagonistes[830]. Cette liste fait l'objet d'une appréciation générale tous les quatre ans. Elle est soumise une fois par an à l'approbation du Conseil fédéral, puis à la Délégation des commissions de gestion pour qu'elle en prenne connaissance, mais le DDPS peut en tout temps inscrire provisoirement des organisations et groupements sur cette liste. L'observation est levée et l'inscription sur la liste effacée lorsque les indices sont infirmés par de nouvelles données et qu'il n'y a pas de nouveaux éléments à charge, lorsque les activités ont cessé ou ne représentent plus un risque, ou encore lorsqu'aucune information nouvelle dénotant une mise en danger de la sûreté de la Suisse n'est

[828] Activités terroristes, service de renseignements prohibé, extrémisme violent, commerce illicite de substances radioactives, transfert illégal de technologies, activités menaçant la sûreté intérieure ou extérieure de la Suisse, actes de violence lors de manifestations sportives.

[829] Contrairement à l'Union européenne par exemple, dont la liste est publique : *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 66.

[830] Y compris les informations sur les engagements politiques qui seraient sinon protégées par les limites de l'art. 3 LMSI : *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 65.

apparue au cours des quatre dernières années[831]. La liste d'observation est le principal moyen à la disposition du Conseil fédéral pour influer sur l'activité de la protection de l'Etat[832].

3. Le contrôle de sécurité

Le contrôle de sécurité est réglé par les art. 19ss LMSI et l'Ordonnance du 19 décembre 2001 sur les contrôles de sécurité relatifs aux personnes[833]. Il concerne les personnes liées à l'Etat par un rapport spécial et qui ont connaissance dans leurs activités d'informations en lien avec la sécurité de l'Etat[834]. En 2008, 34 000 contrôles ont été effectués et le Service d'analyse et de prévention a procédé à un examen approfondi dans 35 % des cas[835]. Le contrôle doit servir à déterminer si l'engagement de la personne fait courir un risque pour la sécurité. 541

4. La protection des personnes et des bâtiments

La protection des personnes et des bâtiments est réglée par les art. 22ss LMSI et l'Ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale[836]. 542

L'art. 15 OSF permet au Service fédéral de sécurité d'utiliser des appareils de prise de vues et d'enregistrement afin de déceler les dangers qui menacent des personnes et leurs biens, des bâtiments de la Confédération, ainsi que des représentations étrangères et des organisations internationales si celles-ci consentent à l'enregistrement de ces données, mais uniquement dans les lieux publics et accessibles à tous. Si une surveillance est nécessaire pour la protection des bâtiments de la Confédération et de ses occupants, elle est permise à la demande de la personne exerçant le droit de police dans ce bâtiment au sens de l'art. 23 al. 2 LMSI. Les images contenant des données concernant des personnes ne peuvent pas être conservées plus de deux semaines. Elles ne 543

831 Art. 11al. 2 LMSI et 27 OSRC.
832 *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, pp 65-67.
833 OCSP, RS 120.4.
834 Voir à ce sujet les annexes à l'OCSP.
835 FEDPOL, *Rapport 2008*, p. 26.
836 OSF, RS 120.72.

peuvent être mises à disposition des autorités pénales, civiles ou administratives qu'en vertu d'une décision judiciaire.

5. Les mesures contre la violence lors de manifestations sportives

544 Les mesures contre la violence lors de manifestations sportives sont réglées par les art. 24a ss LMSI, les art. 4ss de l'Ordonnance sur les mesures de police administrative et les systèmes d'information de l'Office fédéral de la police[837], ainsi que le Concordat instituant des mesures contre la violence lors de manifestations sportives (CMVMS)[838]. Ces mesures sont composées de la récolte d'informations relatives aux actes de violence commis lors de manifestations sportives, des interdictions de périmètre ou de se rendre dans un pays donné, et de l'obligation de se présenter à la police. Les mesures de surveillance ne sont concernées que par la première de ces mesures, raison pour laquelle les mesures contre la violence lors de manifestations sportives ne seront pas traitées de manière approfondie[839].

545 Les données relatives aux personnes qui ont été l'objet d'une des mesures précitées ou qui ont été soumises à des interdictions de stades et qui ont commis des actes de violence lors de manifestations sportives sont enregistrées dans le système d'informations HOOGAN[840]. Après trois ans d'utilisation, soit à fin 2009, 797 personnes étaient enregistrées dans le système d'information HOOGAN. Il contenait 259 interdictions de stade et 269 interdictions de

[837] Sur ce sujet en lien avec la LMSI et de manière plus large : BICHOVSKY, *Prévention de la violence commise par les spectateurs.*

[838] Disponible à l'adresse : http://www.lexfind.ch/dta/30211/3. Ce concordat a été adopté par la Conférence des chefs des départements de justice et police le 15 novembre 2007 et est entré en vigueur le 1er janvier 2010. Il remplace les dispositions concernant l'interdiction de périmètre, la garde à vue et l'obligation de se présenter à la police, qui figuraient de janvier 2007 à décembre 2009 aux art. 24b, 24d et 24e LMSI et pour lesquelles la Confédération n'était pas compétente.

[839] Sur les différentes mesures prévues : VON DÄNIKEN, *Sicherheit bei Sportveranstaltungen*. Sur l'interdiction de périmètre en particulier : SOÒS / VÖGELI, *Top oder Flop?*, pp 157-161.

[840] Système électronique d'information relatif aux personnes qui ont commis des actes de violence lors de manifestations sportives, art. 8ss de l'Ordonnance sur les mesures de police administrative et les systèmes d'information de l'Office fédéral de la police (RS 120.52).

périmètre[841]. Moyennant l'approbation de l'autorité qui a fourni les données, elles peuvent être transmises aux responsables de sécurité de manifestations sportives. Ces données peuvent être traitées dans des systèmes électroniques de reconnaissance des personnes. Elles doivent en revanche n'être utilisées que pour lutter contre la violence lors de la manifestation sportive désignée. Les données doivent être détruites immédiatement après la manifestation sportive et l'autorité qui a fourni les données doit être informée dans les vingt-quatre heures.

6. L'exploration radio et le renseignement militaire

Le service de renseignement militaire a pour tâche de rechercher et d'évaluer des informations sur l'étranger importantes pour l'armée. Il peut communiquer aux autorités de poursuite pénale de la Confédération les informations qu'il a obtenues sur des personnes en Suisse et qui peuvent être importantes pour la poursuite pénale (art. 99 LAAM). L'exploration radio est réglée par l'Ordonnance sur la guerre électronique[842]. En matière civile, elle est basée sur l'art. 18 OSRC[843]. 546

Sous le nom de guerre électronique, on englobe l'exploration radio permanente menée par les services du DDPS et la guerre électronique de l'armée. La recherche d'informations par l'exploration radio est autorisée par le Service de renseignement stratégique, le Service d'analyse et de prévention ou le Service de renseignement militaire[844]. Elle doit permettre d'obtenir des informations pertinentes pour la politique de sécurité. 547

[841] FEDPOL, *Rapport 2009*, pp 55-56. A fin 2008, on comptait 506 personnes enregistrées dans le système d'information HOOGAN, 185 interdictions de stade et 164 interdictions de périmètre : FEDPOL, *Rapport 2008*, p. 25.

[842] Ordonnance sur la guerre électronique du 15 octobre 2003 (OGE, RS 510.292).

[843] Cette disposition, qui a remplacé l'art. 9a OMSI le 1er janvier 2010, devrait figurer dans une base légale formelle : *Message du CF relatif à la LMSI II*, pp 4822-4824; FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 37-38.

[844] Il n'y a actuellement pas de base légale suffisante pour permettre l'exploration radio pour les mandats du SAP : *Rapport de la DélCdG du 9 novembre 2007 sur le projet Onyx*, p. 2306.

B. La procédure de mise sous surveillance

1. L'absence de procédure d'autorisation

548 Au niveau fédéral, la LMSI ne prévoit pas une procédure générale d'autorisation des mesures de surveillance techniques. Le législateur a considéré que les mesures de surveillance utilisées préventivement ne constituaient pas, au contraire de celles appliquées dans le cadre d'une instruction pénale, une atteinte suffisante à la sphère privée pour justifier une procédure codifiée. Cela conduirait d'ailleurs à imposer aux organes étatiques une procédure d'autorisation pour des mesures qu'un privé peut mettre en place sans la moindre autorisation[845].

549 Les mesures de surveillance ne nécessitent alors aucune autorisation ou approbation particulière pour être mises en place légalement, une autorisation de principe étant accordée par la loi. Ce sont des moyens à disposition des autorités compétentes, dont l'usage peut éventuellement être réglé de manière interne par des directives[846]. Il en va différemment du contrôle de sécurité pour lequel une procédure précise est prévue en raison des atteintes importantes qu'il peut avoir dans la sphère privée de l'individu contrôlé[847].

550 L'utilisation qui est faite des données recueillies est encadrée par les art. 15ss LMSI ainsi que l'Ordonnance du 4 décembre 2009 sur les systèmes d'information du Service de renseignement de la Confédération[848]. L'exactitude des données doit être vérifiée et leur accès limité. Elles sont conservées dans un système séparé des autres informations de la police ou de l'administration. Un contrôle interne de la protection des données est mis en place et doit garantir la qualité et la pertinence des données. Les exigences de contrôle périodique et les durées de conservation des données sont également réglées dans l'Ordonnance (art. 32 et 33).

---

[845] MÉTILLE, *L'utilisation privée de moyens techniques de surveillance*.

[846] Si de telles directives existent, elles ne sont ni librement accessibles, ni soumises à un contrôle administratif ou judiciaire.

[847] Et dans une moindre mesure de l'exploration radio au vu de l'existence de l'ACI et de la procédure qui en découle.

[848] OSI-SRC, RS 121.2

2. Le contrôle de sécurité

La procédure de contrôle est ouverte par l'autorité de nomination pour les employés de l'administration, par la hiérarchie pour les militaires, et par l'autorité qui donne le mandat pour les tiers participant à des projets classifiés. La personne contrôlée est informée de la procédure et doit donner son accord à l'aide d'un formulaire préétabli. Ce formulaire mentionne que la personne concernée autorise expressément le service spécialisé à recueillir les données nécessaires et à utiliser pour le contrôle de sécurité les renseignements figurant dans le formulaire[849]. Dans le cas de l'audition de tiers, la personne concernée doit donner son accord pour chacune des personnes à auditionner. L'autorisation de recueillir des données est valable six mois et peut être révoquée par écrit à tout moment. La personne concernée peut évidemment renouveler son accord si la recherche des données n'est pas terminée dans les six mois. Une fois l'accord recueilli, l'autorité requérante mandate le service spécialisé pour l'exécution du contrôle (art. 13ss OCSP). 551

Si le service spécialisé envisage de prendre une décision négative ou assortie de réserves, il donne le droit à la personne concernée de se prononcer par écrit sur le résultat du contrôle. Elle peut en outre prendre connaissance des pièces du dossier en tout temps, sauf si un intérêt privé ou public prépondérant ne l'exige[850]. La décision relative au risque ne peut toutefois se baser que sur des données qui ont été portées à la connaissance de la personne concernée. Elle peut également demander la rectification des données erronées ou obsolètes, la suppression immédiate des données qui ne correspondent pas au but de l'opération ou dont le traitement est illicite, voire apposer une remarque de contestation. 552

[849] Soit à partir des registres des organes de sûreté et de poursuite pénale de la Confédération et des cantons et du casier judiciaire, à partir des registres des offices cantonaux des poursuites et des faillites et des contrôles de l'habitant, par des enquêtes sur les personnes soumises au contrôle effectuées par les polices cantonales compétentes sur mandat du service spécialisé, en demandant des renseignements relatifs à des procédures pénales en cours aux organes de poursuite pénale compétents et bien sûr par le biais de l'audition de la personne concernée (art. 20 al. 2 lit. a à d et f LMSI).

[850] Au sens de l'art. 9 LPD notamment.

553 La décision du service spécialisé est communiquée à la personne concernée ainsi qu'à l'autorité requérante et aux éventuels tiers autorisés à recourir. L'autorité requérante n'est pas liée par la décision du service spécialisé. Elle rend sa propre décision qu'elle communique à la personne concernée et au service spécialisé, si la décision qu'elle a rendue diffère de celle du service spécialisé. L'autorité requérante peut, après avoir obtenu l'accord écrit de la personne concernée, prendre connaissance des pièces du contrôle et avoir un entretien avec cette personne afin de clarifier les questions en suspens. Le service spécialisé peut aussi y être associé (art. 20ss OCSP).

554 Les pièces du contrôle de sécurité ne peuvent pas être utilisées à d'autres fins que celles pour lesquelles elles avaient été créées. Sur message écrit de l'autorité requérante, le service spécialisé propose aux Archives fédérales les pièces relatives au contrôle de personnes dont la candidature n'a pas été retenue. Le service spécialisé détruit les données enregistrées sur support électronique. Si la personne a été retenue, le service spécialisé conserve les pièces de la procédure de contrôle aussi longtemps qu'elle occupe la fonction considérée ou collabore à l'exécution du mandat, mais au maximum durant dix ans. Le service spécialisé propose ensuite les documents aux Archives fédérales et le service spécialisé détruit les données enregistrées sur support électronique (art. 24ss OSCP). Un retard important a été pris et les collaborateurs du Service analyse et prévention pourraient encore avoir accès à des données effacées[851].

3. L'exploration radio

555 Le service qui a donné le mandat de procéder à une exploration radio est tenu de s'assurer de la légalité et de la proportionnalité de cette surveillance (art. 14 OGE). En matière civile, il s'agit du Service d'analyse et de prévention. L'autorité de contrôle indépendante (ACI)[852] contrôle tous les mandats, les nouveaux objets d'exploration radio ajoutés à un mandat existant, ainsi que les résultats de l'exploration radio, leur transmission et leur traitement. Elle peut demander au département du mandant de suspendre des mandats d'exploration radio qui ne satisfont pas aux principes de la légalité et de la proportionnalité, ainsi qu'émettre des recommandations concernant le traitement ou l'effacement

[851] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 33.
[852] Voir également le chapitre b) L'autorité de contrôle indépendante à la p. 254 ci-dessous.

des résultats obtenus. Le chef du DDPS est informé des propositions et des décisions de suspension.

C. Les conditions auxquelles une surveillance peut être ordonnée

1. La recherche d'informations (14 LMSI)

Si les mesures de surveillance mises en place dans le cadre de la LMSI, et singulièrement la recherche d'informations, ne sont pas soumises à une procédure d'autorisation judiciaire à l'instar de la procédure prévue par la procédure pénale, cela ne permet pas pour autant la récolte de n'importe quelles données et leur utilisation sans limites. 556

Les informations recherchées doivent d'abord être nécessaires à prévenir et lutter contre les dangers liés au terrorisme, au service de renseignement prohibé, à l'extrémisme violent et à la violence lors de manifestations sportives[853]. La surveillance doit ensuite, comme dans le cadre d'une instruction pénale, reposer sur des soupçons[854]. 557

Lorsque la surveillance porte sur des informations relatives à l'engagement politique ou à l'exercice des droits découlant de la liberté d'opinion, d'association et de réunion, un soupçon qualifié est exigé. La loi parle d'une présomption sérieuse permettant de soupçonner une organisation ou des personnes qui en font partie de se servir de l'exercice des droits politiques ou des droits fondamentaux pour dissimuler la préparation ou l'exécution d'actes relevant du terrorisme, du service de renseignement ou de l'extrémisme violent (art. 3 al. 1 LMSI). Des informations liées à l'engagement politique ou à l'exercice des droits découlant de la liberté d'opinion, d'association et de réunion est admissible si la personne concernée figure sur la liste d'observation (art. 11 LMSI). L'inscription sur la liste d'observation n'est possible que si l'organisation est concrètement soupçonnée de représenter un danger pour la 558

[853] Art. 2 et 14 LMSI.

[854] FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, p. 6.

sécurité intérieure ou extérieure du pays[855]. Lorsque de telles informations sont recueillies et que les soupçons relatifs à un comportement punissable ne sont pas corroborés par les activités observées, elles ne peuvent pas être enregistrées avec référence nominale. Les prises de vues et les enregistrements sonores doivent alors être détruits dans un délai de trente jours (art. 3 al. 1 LMSI).

2. Le contrôle de sécurité

559 Le contrôle de sécurité concerne une catégorie limitée de personnes liées à l'Etat par un rapport spécial. Elles ont librement choisi d'entrer dans ce rapport spécial. Ces personnes sont en outre informées de la procédure et doivent donner leur accord préalablement. Une ingérence plus grande est admissible dans ce cas, car il est différent d'une surveillance opérée à l'insu de la personne et en l'absence de tout consentement.

560 Le contrôle de sécurité est possible aux conditions de l'art. 19 LMSI, soit lorsque la personne concernée peut exercer une influence sur la politique de sécurité, lorsqu'elle a accès à des secrets relevant de la sûreté intérieure ou extérieure ou à des informations militaires classifiées ou lorsqu'elle a régulièrement accès à des données personnelles sensibles, dont la révélation pourrait porter gravement atteinte aux droits individuels des personnes concernées. En pratique, il s'agit de toutes les fonctions figurant dans les annexes 1 et 2 de l'OCSP.

561 Le contrôle de sécurité consiste essentiellement dans la consultation de bases de données des organes de sûreté et de poursuite pénale, et plus particulièrement le casier judiciaire informatisé (VOSTRA), le système de recherches informatisées de police (RIPOL), le système de traitement des données relatives à la protection de l'Etat (ISIS), le système informatisé IPAS[856], les registres cantonaux des poursuites et des faillites, les registres des contrôles de l'habitant. Une enquête sur la personne soumise au contrôle peut être confiée aux polices cantonales, qui collectent aussi des informations pertinentes sur le mode de vie, notamment sur l'entourage proche, la situation financière, les relations avec l'étranger et les

[855] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p.51.

[856] Voir l'Ordonnance du 15 octobre 2008 sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (Ordonnance IPAS, RS 361.2)

activités qui pourraient représenter un risque pour la sécurité intérieure et extérieure de la Suisse[857]. L'audition de la personne concernée, ainsi que de tiers, est également prévue.

3. L'exploration radio

En matière civile, l'exploration radio doit avoir été commandée par le Service d'analyse et de prévention et servir exclusivement à obtenir des informations pertinentes pour la politique de sécurité (art. 2 OGE). L'exploration ne peut porter, selon l'art. 5 OGE, que sur des objets d'exploration radio à l'étranger. Si des informations relatives à des personnes sises en Suisse sont acquises de manière non intentionnelle par le biais de communications avec ces personnes, elles sont effacées. Des produits dérivés peuvent néanmoins être transmis. Ces personnes sont, dans la mesure du possible, rendues anonymes. Les dispositions concernant la recherche d'informations s'appliquent pour le surplus. 562

D. Le contrôle

1. L'absence de contrôle *a priori*

La LMSI ne prévoit pas de contrôle *a priori* puisqu'il n'y a pas de procédure d'autorisation. En ce qui concerne le contrôle de sécurité, la personne concernée doit donner son accord préalablement. Il ne s'agit pas d'une procédure de contrôle indépendante. 563

Le droit d'accès indirect prévu par l'art. 18 LMSI est un contrôle administratif particulier et indépendant. Même s'il peut avoir lieu en tout temps, il doit être considéré comme un contrôle *a posteriori*, puisqu'il ne porte que sur le résultat des mesures de surveillance et pas sur des mesures futures. Il est exercé en première instance par le Préposé fédéral à la protection des données et à la transparence (PFPDT)[858] et en seconde instance par le Président de la Cour I du Tribunal administratif fédéral (TAF). Il s'agit dans ce deuxième cas d'une 564

[857] FEDPOL, *Rapport 2008*, p. 27.

[858] Avec l'entrée en vigueur le 1er juillet 2006 de la Loi sur le principe de la transparence dans l'administration le Préposé fédéral à la protection des données (PFPD) est devenu le Préposé fédéral à la protection des données et à la transparence (PFPDT).

autorité judiciaire. Cela reste pourtant un contrôle indirect. Si le contrôle est effectué à la suite d'une requête individuelle, le requérant n'a pas pour autant connaissance du résultat et encore moins la possibilité de participer à la procédure. Ces deux autorités ne bénéficient en outre pas des connaissances et des moyens suffisants pour contrôler complètement l'exactitude des données, en particulier la fiabilité des informations, ainsi que la nécessité et la proportionnalité de leur récolte dans un cas d'espèce.

2. Le contrôle judiciaire

565 En matière de contrôle de sécurité, le Tribunal administratif fédéral est l'autorité de recours contre la décision rendue par le service spécialisé conformément à l'art. 21 OSCP[859]. L'autorité de recours contre la décision rendue par l'autorité requérante n'est en revanche pas unique et dépend de la procédure à laquelle est soumise cette dernière, puisqu'il peut s'agir d'une autorité administrative ou militaire.

566 Pour le reste, aucun contrôle judiciaire n'est actuellement prévu par le droit fédéral. Les décisions concernant la sûreté intérieure ou extérieure du pays sont des actes de gouvernement contre lesquels le recours au Tribunal administratif fédéral est en principe irrecevable[860]. Il existe une exception lorsque le droit international confère le droit à ce que la cause soit jugée par un tribunal. L'emploi de moyens techniques de surveillance porte atteinte au droit au respect de la vie privée garanti par l'art. 8 CEDH, ce qui devrait ouvrir la voie à un recours judiciaire. Le législateur a toutefois considéré que les moyens limités accordés par la LMSI, contrairement à ceux prévus par le CPP, ne portaient pas une atteinte suffisante aux droits fondamentaux pour imposer une autorité judiciaire[861].

[859] Précédemment la Commission de recours DDPS conformément à l'art. 22 OSCP, par exemple Décision 470.05.03 de la Commission de recours DDPS du 28 janvier 2004, publiée in JAAC 70.27

[860] Art. 32 al. 1 lit. a LTAF, *Message du CF relatif à la LMSI II*, pp 4849-4850.

[861] Dans le cas de l'utilisation à titre préventif des moyens de surveillance actuellement utilisés dans le cadre d'une enquête pénale : FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 4833-4834.

3. Le contrôle administratif et politique

a) La Délégation des Commissions de gestion des Chambres fédérales

La Délégation des Commissions de gestion des Chambres fédérales (DélCdG) a pour mandat de contrôler en détail les activités dans les domaines de la sécurité de l'Etat et des services de renseignement (art. 53 LParl). Elle exerce la Haute surveillance parlementaire, alors que la surveillance administrative revient au Conseil fédéral[862]. L'instauration d'une délégation remonte à la commission d'enquête parlementaire mise en place à la suite de l'affaire des fiches[863]. En plus des droits d'information habituellement réservés aux commissions (art. 150 LParl), la DélCdG peut interroger directement un service ou une autorité et obtenir les documents dont elle a besoin, y compris en dehors de l'administration. Elle a également le droit de consulter les documents sur lesquels le Conseil fédéral s'est directement fondé pour prendre une décision ainsi que les documents qui doivent rester secrets pour des raisons relevant de la sécurité de l'Etat ou du renseignement (le secret de fonction ou le secret militaire ne peut pas s'y opposer). Elle peut finalement encore entendre des personnes en qualité de témoins[864]. Elle dispose du même droit à obtenir des informations qu'une commission d'enquête parlementaire (CEP)[865]. 567

Les Commissions de gestion et la Délégation des Commissions de gestion des Chambres fédérales publient chaque année un rapport dont une partie concerne l'activité des services de renseignement[866]. Lorsqu'elle est confrontée à des problèmes ou des questions de portée générale, la Délégation procède à une 568

862 Les rapports de la DélCdG sont disponibles à l'adresse : http://www.parlament.ch/f/dokumentation/berichte/berichte-delegationen/berichte-der-geschaeftspruefungsdelegation/Pages/default.aspx.

863 Intervention parlementaire 89.006 du 31 janvier 1989 « Evénements survenus au sein du DFJP. Commission d'enquête parlementaire ». Les documents de la CEP DFJP sont disponibles à l'adresse : http://www.parlament.ch/f/organe-mitglieder/kommissionen/aufsichtskommissionen/puk/puk-vorkommnisse-ejpd/Pages/default.aspx

864 Art. 169 Cst., 53, 150 et 154 LParl, ainsi que 25ss LMSI. Voir également : CONSEIL FÉDÉRAL, *Réponse du Conseil fédéral à la motion MALAMA*; KELLER, *Die politische Polizei*, pp 473-474.

865 *Rapport annuel 2009 des CdG et de la DélCdG*, pp 2498-2499.

866 Ces rapports sont publiés dans la Feuille fédérale, mais également disponible à l'adresse : http://www.parlament.ch/f/dokumentation/berichte/berichte-aufsichtskommissionen/geschaeftspruefungskommission-gpk/Pages/default.aspx.

enquête formelle et consigne ses conclusions dans un rapport public, comme elle l'a fait concernant le système d'exploration radio « onyx »[867] ou plus récemment s'agissant du Traitement des données dans le système d'informations relatif à la protection de l'Etat (ISIS)[868].

b) L'autorité de contrôle indépendante

569 L'autorité de contrôle indépendante (ACI) est une instance de contrôle interdépartementale interne à l'administration[869]. Composée de trois membres, elle est compétente en matière d'exploration radio. Elle veille au respect de la légalité et de la proportionnalité des mandats d'exploration radio et du traitement des résultats. L'ACI peut faire des recommandations écrites et demander au département de suspendre un mandat d'exploration. Elle adresse également un rapport annuel aux chefs du DDPS et du DFJP. Dans l'exercice de son mandat, l'ACI a accès aux installations et aux locaux affectés à l'exploration radio permanente et elle peut obtenir sur place toutes les informations et tous les renseignements nécessaires.

c) La surveillance SR

570 La surveillance administrative appartient au Conseil fédéral (art. 26 al. 1 LMSI). Actuellement, elle est exercée par le Département fédéral de la défense, de la protection de la population et des sports (DDPS), plus précisément par la Surveillance SR, un organe composé de trois personnes et rattaché à l'Etat-major du chef du Département[870]. La Surveillance SR peut collaborer avec la DélCdG pour mener par exemple une inspection sur un domaine particulier.

571 Contrairement aux rapports de la Délégation des Commissions de gestion des Chambres fédérales, les rapports de la Surveillance SR ne sont pas publiés.

[867] *Rapport de la DélCdG du 9 novembre 2007 sur le projet Onyx*; *Rapport de la DélCdG du 10 novembre 2003 sur le projet Onyx*.

[868] *Rapport annuel 2007 des CdG et de la DélCdG*; *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 4666.

[869] Art. 15ss OGE. *Rapport de la DélCdG du 9 novembre 2007 sur le projet Onyx*, pp 2308-2309.

[870] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, pp 19 et 31; SRC, *Rapport annuel 2009*, p. 97.

d) Le Préposé fédéral à la protection des données et à la transparence

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) est nommé par le Conseil fédéral. Bien qu'indépendant, il est rattaché administrativement à la Chancellerie fédérale. Il surveille l'application par les organes fédéraux de la LPD et des autres dispositions fédérales relatives à la protection des données. Aux fins d'établir les faits, il peut exiger la production de pièces, demander des renseignements et se faire présenter des traitements. En cas de violation des prescriptions sur la protection des données, le Préposé recommande à l'organe fédéral responsable de modifier ou de cesser le traitement et en informe le département compétent ou la Chancellerie fédérale. Si sa recommandation est rejetée ou n'est pas suivie, il peut porter l'affaire pour décision auprès du département ou de la Chancellerie fédérale. Cette décision sera communiquée aux personnes concernées et le Préposé a qualité pour recourir contre cette décision ainsi que contre celle que pourra rendre l'autorité de recours. Le Préposé fait en outre rapport régulièrement au Conseil fédéral et prend part aux procédures législatives. En pratique, le Préposé ne procède que très rarement à de tels contrôles[871]. Son activité s'exerce bien plus par le droit d'accès indirect, éventuellement par un contrôle plus étendu à la suite d'un droit d'accès indirect. 572

4. Le rapport de la délégation relatif à ISIS

De graves lacunes avaient été relevées à la fin des années nonante par la Commission d'enquête parlementaire alors constituée pour investiguer au sujet des événements survenus au Département fédéral de justice et police (DFJP), autrement dit lors de l'affaire des fiches[872]. On pouvait s'attendre à ce que la collecte d'informations erronées ou inutiles ne soit plus pratiquée aujourd'hui. Le dernier rapport de la Délégation des commissions de gestion des Chambres fédérales montre malheureusement que ce n'est pas encore le cas[873]. 573

[871] Ces contrôles sont souvent consécutifs à la demande d'un individu (par l'exercice du droit d'accès indirect de l'art. 18 LMSI) ou à des informations parues dans la presse et mentionnant des violations de la LPD, voire en collaboration avec la DélCdG.

[872] *Rapport complémentaire de la CEP DFJP*; *Rapport de la CEP DFJP*.

[873] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*.

574 Lors de ses contrôles, la Délégation a découvert que les enregistrements dans ISIS ne correspondaient pas forcément aux exigences légales. Ainsi, des personnes présentées comme inoffensives ou plus du tout actives étaient enregistrées, alors que d'autres l'étaient uniquement parce qu'elles avaient fait l'objet d'un contrôle des photos d'identité à la frontière ou en raison d'une demande d'informations émanant de l'étranger[874]. Des informations liées à l'engagement politique ou à l'exercice des droits découlant de la liberté d'opinion, d'association et de réunion étaient également enregistrées alors qu'elles n'auraient pas dû l'être[875]. Le Service d'analyse et de prévention (SAP) considérait en outre qu'il pouvait enregistrer des informations à décharge des personnes concernées, ce qui ne correspond pourtant pas à un danger pour l'Etat.

575 En plus d'enregistrer des données que la loi ne permettait pas, le SAP ne procédait pas aux contrôles requis. Le contrôle initial consécutif à la saisie des données n'avait lieu que par sondage et les contrôles périodiques qui devaient avoir lieu après cinq ans puis trois ans, et lors de nouvelles inscriptions, n'ont pas été réalisés. Pire encore, de fausses dates de contrôle ont été indiquées. Quelques 16 000 contrôles initiaux et 40 000 contrôles périodiques n'ont pas été effectués ces cinq dernières années, en violation des prescriptions légales[876]. L'effacement de données obsolètes qui aurait dû avoir lieu lors des contrôles périodiques n'a évidemment pas eu lieu et des enregistrements ont été conservés bien au-delà de la durée maximale de conservation[877].

576 Globalement, on constate d'abord que les services de renseignement reçoivent un grand nombre de données qu'ils ne maîtrisent pas. Au lieu de vérifier l'authenticité des données et de n'enregistrer que les données pertinentes, les services de renseignement ont préféré enregistrer toutes les données et renoncer aux contrôles prévus. Ils disposent ainsi d'un grand nombre d'informations peu utiles. D'autre part, on constate à la lecture du rapport de la Délégation que les

[874] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, pp 16-18, 25, 45-46 et 56-57.
[875] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, pp 51-52 et 55.
[876] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, pp 31-32, 34, et 53-54.
[877] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, pp 20-24.

agents ne sont pas sensibles à la question de la protection des données et des droits des citoyens qui en découlent.

Le Conseil fédéral considérait pourtant déjà en 1994 que l'évaluation de l'exactitude et de l'importance des informations était un préalable indispensable au traitement des données. Celles-ci ne devaient pas faire l'objet d'un examen unique au moment de leur entrée, mais d'un examen périodique, ce qui est le seul moyen d'éviter le stockage et le traitement d'informations erronées, superflues ou inutiles[878]. 577

E. Le droit d'accès indirect

La LMSI ne prévoit pas d'information de la personne surveillée, mais celle-ci jouit d'un droit de contrôle. Toute personne peut saisir le Préposé fédéral à la protection des données et à la transparence (PFPDT) pour qu'il vérifie si des données la concernant sont traitées conformément au droit dans le système d'information du Service d'analyse et de prévention (ISIS)[879]. Bien que l'on parle parfois d'un droit d'accès indirect, il ne s'agit en réalité pas d'un droit de la personne concernée d'être renseignée, mais seulement d'un contrôle administratif particulier et indépendant. Le Préposé reçoit une version papier de l'ensemble des informations liées à chaque inscription concernant la personne en question. Celle-là n'aura pas accès aux données mais le Préposé lui transmettra une réponse standard confirmant qu'aucune donnée la concernant n'a été traitée illégalement ou que, dans le cas d'une éventuelle erreur dans le traitement des données, il a adressé au Service d'analyse et de prévention la recommandation d'y remédier. Cette communication ne doit pas permettre au destinataire de déduire si des informations ont été recueillies sur son compte ou pas[880]. 578

[878] *Message du CF concernant la LMSI*, p.1180.

[879] Art. 18 al. 1 LMSI. 148 demandes ont été déposées en 2008 et 34 en 2009 : PFPDT, *17ème rapport*, p. 50. A la suite du rapport de la DélCdG et des nombreux articles de presse qui lui ont été consacré, on peut s'attendre à une forte augmentation du nombre de demande pour le second semestre 2010.

[880] PFPDT, *14ème rapport*, pp 39-41; PFPDT, *15ème rapport*, pp 44-46; SCHWEGLER, *Datenschutz im Polizeiwesen*, pp 176-181.

579 La communication du Préposé fédéral à la protection des données et à la transparence n'est pas sujette à recours, mais l'art. 18 al. 2 LMSI permet à la personne concernée de demander à une seconde instance de procéder au contrôle. Le Président de la Cour I du Tribunal administratif fédéral (TAF) peut examiner la communication ou l'exécution de la recommandation émise par le Préposé. Le Président informe ensuite la personne concernée que sa requête a été examinée. Cette réponse a lieu également au moyen d'une réponse au libellé toujours identique.

580 La saisine du Préposé a deux autres effets[881]. Elle oblige premièrement le Service d'analyse et de prévention à vérifier que les informations existantes restent nécessaires et à effacer toutes celles qui ne le sont pas, même si le délai prévu de conservation n'est pas atteint. Deuxièmement, les personnes recensées qui ont saisi le Préposé seront renseignées dès lors que les intérêts liés au maintien de la sûreté intérieure n'exigent plus le secret ou au plus tard à l'échéance de la durée de conservation maximale (art. 18 al. 5 et 6 LMSI)[882]. La durée de conservation maximale des données enregistrées dans ISIS varie entre cinq et quarante-cinq ans selon les données[883]. Elle est de quinze ans pour les données préventives. Le moment jusqu'auquel la transmission des informations peut être repoussée est parfois très long. Pour les fichiers soumis à la LSIP, les personnes au sujet desquelles aucune donnée n'a été traitée en sont informées par fedpol trois ans après réception de leur demande (art. 8 al. 7 LSIP).

581 En pratique l'information ultérieure semble ne pas avoir lieu et il est difficile de contrôler son application[884]. La personne qui a reçu une communication et qui soupçonne que des informations ont été recueillies pourrait tout au plus demander au Préposé de procéder à une nouvelle vérification après quelques années. La réponse standard qu'il recevra ne lui permettra cependant toujours

[881] L'exercice du droit d'accès a encore un effet plus large, soit celui de permettre au PFPDT (et parfois au TAF) d'exercer un contrôle concret de la légalité du traitement des données : *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 68.

[882] La loi parle de l'obligation de conserver les données, ce qui est une mauvaise traduction de l'allemand « spätestens bei Ablauf der Aufbewahrungsdauer ».

[883] Art. 33 al. 1 OSI-SRC. La durée de conservation des données va de cinq ans pour les données recueillies dans le cadre des contrôles de sécurité relatifs aux personnes à quarante-cinq ans pour les données des banques DO, NEWS, IPIS, Infopress et ISIS-Info.

[884] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 43; PFPD, *11ème rapport*, pp 32-33.

pas de savoir si des données ont été recueillies et sont, le cas échéant, considérées comme étant encore utiles (ce qui empêche une information plus complète) ou si aucune donnée n'a été recueillie.

582 L'art. 18 al. 3 LMSI permet au Préposé fédéral à la protection des données et à la transparence de fournir des renseignements aux personnes qui en font la demande, à titre exceptionnel, et pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure et qu'il n'existe pas d'autre moyen pour empêcher que ces personnes soient lésées gravement et de manière irréparable[885]. La Commission fédérale de la protection des données[886] et de la transparence a examiné cette possibilité dans une décision du 31 août 2006 et elle est arrivée à la conclusion que les art. 18 al. 1 et 2 LMSI ne répondaient pas aux exigences de la CEDH. Elle a également retenu que la règle de l'al. 3 ne permettait pas de tenir compte aussi bien de la protection des droits fondamentaux que des objectifs de l'art. 1 LMSI. Le Préposé n'a pas les connaissances nécessaires pour évaluer correctement les risques pour la sécurité intérieure et extérieure, ni le risque que la personne soit lésée gravement et de manière irréparable. La possibilité d'être renseigné est ainsi pratiquement exclue, et ce de manière contraire à la CEDH[887]. Le Préposé fédéral à la protection des données et à la transparence n'a accès qu'aux informations que lui transmet l'autorité contrôlée. Il peut parfois vérifier la plausibilité des données, mais il ne peut pas contrôler la véracité des données recueillies, puisqu'il ne peut pas s'en entretenir avec la personne surveillée. Il prendrait alors le risque que la personne concernée puisse déduire qu'elle est l'objet d'une surveillance, voire savoir quelles informations sont en possession des services

[885] Le Préposé a fait usage à quelques reprises de cette possibilité, notamment dans le cas de personnes pouvant craindre d'être fichées en raison de leurs activités politiques : PFPDT, *16ème rapport*, p. 8.

[886] La Commission fédérale de la protection des données et de la transparence (CFPDT) a été remplacée le 1er janvier 2007 par le Tribunal administratif fédéral (TAF).

[887] Décision de la Commission fédérale de la protection des données et de la transparence du 31 août 2006, publiée in JAAC 70.96, consid. 10 et PFPDT, *14ème rapport*, pp 39-41. Pour une critique de cette décision : RUDIN, *Indirekte Auskunft*. Sur les compétences respectives du PFPDT et de la CFPDT : Décision de la Commission fédérale de la protection des données et de la transparence des 22 mai 2003 et 15 mars 2004, publiée in JAAC 70.95.

de renseignement, en fonction des informations complémentaires que le préposé demanderait au requérant[888].

583 La Conseillère nationale Susanne LEUTENEGGER OBERHOLZER a déposé une motion le 17 décembre 2008 demandant à ce qu'un droit d'accès aux données conforme aux art. 8 et 9 LPD soit garanti pour tous les fichiers de la Confédération, ce qui conduirait à une modification des art. 8 et 11 al. 6 LSIP et 18 LMSI. Ce droit d'accès est connu dans tous les cantons et il est la seule possibilité de permettre une rectification des données erronées, ce que le droit d'accès indirect ne permet pas puisque le Préposé fédéral à la protection des données et à la transparence ne connaît pas la vérité des informations recueillies. L'art. 9 LPD permet de refuser ou différer la communication d'information si un intérêt public prépondérant l'exige ou si une instruction pénale risque d'être compromise[889]. Dans sa réponse du 13 mars 2009, le Conseil fédéral admet que le droit d'accès indirect est problématique et qu'il ne constitue pas un vrai droit d'accès. Il considère qu'un droit d'accès au sens de l'art. 8 LPD doit être garanti à toute personne dont les données personnelles sont collectées, y compris dans les domaines de la sécurité intérieure et de l'information policière, les exceptions devant être fixées dans le cadre de l'art. 9 LPD[890]. Malgré la proposition du Conseil fédéral d'accepter la motion, elle a malheureusement été rejetée le 3 mars 2010 par le Conseil national par 95 voix contre 64[891].

584 Depuis l'entrée en vigueur de la LSIP le 1er janvier 2009, les demandes adressées au Préposé fédéral à la protection des données et à la transparence ne concernent plus que le fichier ISIS.

---

[888] BUSCH, *Freie Bahn für den Staatsschutz*, p. 18; *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 43.

[889] Avec l'entrée en vigueur de la Loi fédérale du 19 mars 2010 portant mise en œuvre de la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (FF 2010 1933), un nouvel alinéa 3 a été inséré à l'art. 9 LPD. Il dispose que dès que le motif justifiant le refus, la restriction ou l'ajournement disparaît, l'organe fédéral est tenu de communiquer les renseignements demandés, pour autant que cela ne s'avère pas impossible ou ne nécessite pas un travail disproportionné.

[890] CONSEIL FÉDÉRAL, *Réponse du CF à la motion LEUTENEGGER OBERHOLZER*.

[891] BO 2010 N 141.

F. Le sort des données recueillies

1. En matière de renseignement

Les informations recueillies sont saisies dans un système de traitement des données relatives à la protection de l'Etat (ISIS)[892]. ISIS se compose en réalité de sept systèmes[893] et dix-huit banques de données[894]. Selon le Conseil fédéral, le système ISIS relatif à la protection de l'Etat contenait les données portant sur quelque 13 000 personnes domiciliées en Suisse à fin 2008[895]. La Délégation des Commissions de gestion, citant le rapport annuel du Service d'analyse et de prévention, mentionne pour la même période des chiffres plus élevés : 117 000 personnes revêtant une importance directe pour la protection de l'Etat sont enregistrées, de même que 60 000 tiers. 12,2 % des personnes enregistrées sont domiciliées en Suisse et 5 % sont des ressortissants suisses[896]. En juin 2010, ce sont plus de 200 000 personnes qui sont enregistrées dans le système ISIS[897]. 585

Les organes de sûreté doivent évaluer l'exactitude et l'importance des informations obtenues. Ils détruisent les informations inexactes ou inutiles et en informent le service qui les a communiquées s'il s'agit d'un autre organe de sûreté (art. 15 LMSI). Le sort réservé à des informations recueillies illégalement 586

[892] Ordonnance du 4 décembre 2009 sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC, RS 121.2).

[893] ISIS00 Général, ISIS01 Protection de l'Etat, ISIS02 Administration, ISIS03 Armes, ISIS04 Explosifs, ISIS05 News et ISIS06 Contrôles de sécurité relatifs aux personnes. Le contenu de chaque système est précisé à l'art. 4 al. 1 de l'Ordonnance ISIS.

[894] Protection de l'Etat, Police administrative, Documentation, Système numérique, Administration, Acquisition d'armes par des étrangers, Acquisition d'armes par des personnes domiciliées dans un autre Etat Schengen, Révocation d'autorisations et mise sous séquestre d'armes, Remise et retrait d'armes de l'armée, Exploitation des traces laissées par des armes à feu, BARBARA, NEWS, Portail interactif pour Open Sources (IPOS), ELIS, IPIS, Infopress, ISIS-Info et Contrôles de sécurité relatifs aux personnes (PSP). Le contenu de chaque banque de données est précisé à l'art. 4 al. 2 de l'Ordonnance ISIS.

[895] CONSEIL FÉDÉRAL, *Réponse du Conseil fédéral à l'interpellation FETZ.*

[896] Rapport annuel 2008 du SAP cité dans le *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 20.

[897] Plus de 120 000 personnes ayant une importance directe pour la sécurité et plus de 80 000 enregistrements de tiers : *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, p. 59.

n'est pas réglé par la loi et tout laisse à penser que ce point n'est pas vérifié au stade de l'utilisation des données.

587 Le Service d'analyse et de prévention et l'Office fédéral de la police (fedpol) communiquent spontanément aux autres organes de sûreté de la Confédération et des cantons tous les faits susceptibles de compromettre la sûreté intérieure (art. 10 LMSI). Inversement, le Service de renseignement stratégique, les organes de poursuite pénale et les services de police doivent communiquer spontanément au Service d'analyse et de prévention les renseignements en lien avec des menaces concrètes pour la sûreté intérieure ou extérieure[898]. Dans les faits, cette communication n'est pas automatique. Elle donne néanmoins au Service d'analyse et de prévention la possibilité d'obtenir des autorités pénales les réponses aux questions qu'il leur adresserait.

588 En plus de la transmission d'informations précitée, le Service d'analyse et de prévention produit de très nombreux documents : le rapport annuel sur la sécurité intérieure de la Suisse, des rapports d'analyse stratégique destinés au grand public ou aux autorités politiques et policières, les Situations du jour et Points de la semaine qui sont des synthèses électroniques classifiées, ainsi que d'autres documents d'information. Le Service de renseignement stratégique fournit des rapports similaires dans ses domaines de compétence[899].

2. En matière pénale

589 Lorsque les renseignements obtenus sont utiles à la poursuite pénale, le Service d'analyse et de prévention communique aux autorités pénales compétentes les données qu'il traite et qui permettent de prévenir et de poursuivre des actes punissables, y compris celles que le service de renseignement militaire lui a transmises[900]. Toutes les informations recueillies ne débouchent pas sur des actes punissables pénalement, la sécurité intérieure pouvant également être mise en danger par des actes non punissables[901].

[898] Art. 11 et 13 LMSI.
[899] WEISSEN, *Les services de renseignement suisses*, pp 29 et 39.
[900] Art. 2 al. 3 et 17 al. 1 LMSI, 13 al. 1 lit. a OISIS, 99 al. 2bis LAAM, et 5 al. 3 OGE.
[901] *Message du CF relatif à la LMSI II*, p. 4798.

Lorsque les autorités de poursuite pénale reçoivent des informations ou des preuves des services de renseignement, elles doivent vérifier si elles sont légales et exploitables dans le cadre d'une procédure pénale[902]. L'art. 277 CPP prévoit que les résultats d'une surveillance non autorisée sont absolument inexploitables. Les informations issues d'une exploration radio sont ainsi inexploitables, alors que les informations obtenues dans le cadre d'une observation peuvent être utilisées si elles sont indispensables pour élucider des infractions graves (relativement inexploitables)[903]. Une exploration radio sur territoire suisse pourrait vraisemblablement être ordonnée par le ministère public sur la base des art. 280ss CPP et dans ce cas les résultats obtenus seraient utilisables dans le cadre de l'instruction pénale. Sont finalement librement utilisables toutes les informations recueillies par les services de renseignement mais qui étaient librement accessibles. 590

G. Les modifications législatives envisagées

1. Le contexte

A la suite des événements du 11 septembre 2001, les Etats sont progressivement passés d'un modèle sécuritaire réactif à un modèle sécuritaire proactif, soit la mise en place d'outils permettant de prévenir la commission d'infractions. On passe alors de la surveillance réactive (classique) à la surveillance préventive[904]. Le contexte politique a permis la mise en place de mesures de surveillance qui étaient à peine imaginables quelques mois avant ces attentats. On trouve ainsi en Europe de nombreuses lois de procédure dérogeant au droit commun et permettant un contrôle policier de situations suspectes en l'absence d'indices montrant un commencement de préparation concrète d'actions illicites[905]. Ces 591

[902] Voir à ce sujet le chapitre J. Les preuves illégales à la p. 211 ci-dessus.

[903] Art. 179bisss CP et 277 CPP, ainsi que BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, p. 526; *Rapport du CF relatif à la lutte contre le terrorisme*, p. 5458; *Rapport de la DélCdG du 10 novembre 2003 sur le projet Onyx*, pp 1397 et 1399.

[904] BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*, pp 495-506. Sur la distinction entre renseignement de sécurité (politique) et renseignement criminel (judiciaire) : LEMAN-LANGLOIS / LEMIEUX, *Renseignement de sécurité et renseignement criminel*.

[905] CESONI, *Dérives de l'antiterrorisme*, p. 56. Pour une analyse de la situation aux Etats-Unis : BLOSS, *Escalating U.S. Police Surveillance after 9/11*.

mesures ont été mises en place tantôt de manière urgente et temporaire, tantôt de manière définitive. De tels changements n'ont pas vraiment eu lieu pour l'instant en Suisse et les causes, qu'il n'est pas nécessaire d'étudier ici, sont multiples : processus législatif, absence d'attentat terroriste sur sol helvétique, affaires des fiches[906], etc. Les mesures de surveillance préventives qui peuvent actuellement être ordonnées en Suisse sont plus limitées qu'elles ne le sont à l'étranger, notamment parce que la loi ne permet pas la surveillance de la correspondance et des télécommunications, ni les observations dans le domaine privé[907].

592 Plusieurs projets de révisions sont en cours. Un premier lot de modifications concerne l'exploration radio et est demandé par la DélCdG. Le but est de rendre cette pratique conforme à la CEDH, singulièrement en créant les bases légales nécessaires dans la LAAM et la LMSI[908]. Il s'agit uniquement de régulariser une situation existante, sans étendre la surveillance pratiquée actuellement. Les autres modifications sont connues sous le nom de LMSI II. Elles consistent essentiellement à ajouter les moyens spéciaux de recherche d'informations dans la LMSI, ce qui signifie une augmentation des moyens préventifs de recherche à disposition de l'Etat. Depuis l'introduction du CPP, l'investigation secrète peut seulement être ordonnée pour élucider une infraction déjà commise, alors que la LFIS l'autorisait à l'époque aussi de manière préventive, soit pour empêcher la commission d'un acte délictueux projeté[909].

906 *Rapport complémentaire de la CEP DFJP*; *Rapport de la CEP DFJP*; GEORG, *Staatsschutz im Laufe der Zeit*.

907 *Rapport du CF à la suite des attentats terroristes du 11 septembre 2001*, pp 1715-1716.

908 *Rapport de la DélCdG du 9 novembre 2007 sur le projet Onyx*, pp 2305-2308. Avec l'entrée en vigeur de la Loi fédérale sur le renseignement civil (LFRC) et l'abrogation de l'OMSI, le législateur aurait eu l'occasion de régler cette question. Il s'est malheureusement contenté de remplacer l'art. 9a OMSI par l'art. 18 OSRC, substituant une ordonnance à une autre.

909 Art. 286 al. 1 CPP et ATF 134 IV 266, 279-280, Oberstaatsanwaltschaft des Kantons Zürich, du 16 juin 2008. Si les actes préparatoires de l'infraction projetée constituent une infraction en tant que telle, des mesures de surveillance pourront être ordonnées en application du CPP, une infraction étant déjà commise.

2. Les moyens

Le projet LMSI II (P-LMSI II) a débuté par la publication d'un avant-projet de l'Office fédéral de la police du 31 janvier 2006[910] puis d'un projet de modification de la loi et d'un message par le Conseil fédéral le 15 juin 2007[911]. Alors que le Conseil national avait choisi de ne pas entrer en matière le 17 décembre 2008 par 92 voix contre 79[912], le Conseil des Etats a voté le 3 mars 2009 l'entrée en matière avec renvoi du projet au Conseil fédéral[913]. Il demande en particulier au Conseil fédéral de préciser bon nombre de notions et de vérifier la conformité du projet avec les garanties constitutionnelles. Le Conseil national a finalement adhéré au renvoi le 28 avril 2009[914]. Vu les nombreuses oppositions suscitées, il est probable que ce projet ne sera pas représenté devant les Chambres[915]. 593

Le projet prévoit un devoir de transmission des informations pour les autorités et les transporteurs commerciaux, la possibilité de surveiller la correspondance par poste et télécommunication, ainsi que la possibilité d'utiliser des systèmes de surveillance techniques dans des lieux non accessibles au public. Ces moyens seront soumis à un double contrôle : à la demande de l'Office fédéral de la police, le Tribunal administratif fédéral examinera si les mesures sont conformes au droit, puis le chef du DFJP et le chef du DDPS examineront ensuite la demande sous l'angle politique et décideront d'un commun accord des mesures à mettre en place[916]. L'issue de ce projet étant très incertaine, nous n'entrerons pas dans les détails si ce n'est pour relever quelques éléments importants. 594

[910] FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*.

[911] *Message du CF relatif à la LMSI II*.

[912] BO 2008 N 1885-1892.

[913] BO 2009 E 19-21.

[914] BO 2009 N 672-676.

[915] Une version très allégée pourrait être proposée en ne reprenant que les dispositions non contestées (et ne concernant pas les mesures de surveillance). Une éventuelle extension des moyens de surveillance sera plutôt discutée dans le cadre de l'élaboration de la future Loi sur le service de service de renseignement de la Confédération (Loi sur le SRC) qui devrait remplacer dans quelques années la LMSI.

[916] *Message du CF relatif à la LMSI II*, p. 4804.

595 Les nouveaux moyens prévus (art. 18*k* à 18*m* P-LMSI II) sont ceux qui sont techniquement connus de la procédure pénale, à savoir la surveillance de la correspondance par poste et télécommunication, ainsi que la surveillance de lieux qui ne sont pas librement accessibles, notamment au moyen d'appareils techniques. Le P-LMSI II ajoute la perquisition d'un système informatique, qui n'est pas expressément mentionnée dans le CPP, mais qui est incluse dans les autres dispositifs de surveillance[917]. La surveillance des relations bancaires n'est en revanche pas envisagée dans la modification de la LMSI. La nouveauté de ce projet n'est pas tant les moyens de surveillance, mais la possibilité de les utiliser avant la commission d'une infraction, voire en l'absence totale de projets de commettre une infraction. L'utilisation de ces moyens de surveillance est soumise aux conditions suivantes : existence d'un soupçon, menace pour la sûreté intérieure ou extérieure, proportionnalité et subsidiarité[918]. La menace doit être concrète et être liée au terrorisme, au service de renseignement politique ou militaire prohibé ou à la prolifération des armes de destruction massive. L'extrémisme violent, le service de renseignement économique et la violence lors de manifestations sportives ne permettent pas ce genre de surveillance. Quant à la procédure, elle prévoit un contrôle judiciaire *a priori* et un contrôle judiciaire *a posteriori*[919]. Ce qui différencie fondamentalement ces mesures de celles prévues dans le cadre d'une instruction pénale, c'est qu'elles ne visent pas la poursuite d'une infraction réalisée. Elles reposent seulement sur le soupçon d'un risque.

596 Ce soupçon de risque peut être rapproché de la crainte de la commission d'une infraction permettant d'obtenir un cautionnement préventif au sens de l'art. 66 CP. Le cautionnement préventif n'est possible que dans deux cas précis : si la personne manifeste son intention de commettre un crime ou un délit ou si, ayant déjà été condamnée, elle manifeste l'intention formelle de réitérer son acte. Dans le premier cas on admet que la menace peut résulter de n'importe quel fait concluant par lequel l'auteur menace de commettre un crime ou un délit, alors

[917] BUSCH, *Freie Bahn für den Staatsschutz*, p. 16.

[918] Art. 18b P-LMSI II, *Message du CF relatif à la LMSI II*, pp 4831-4832; FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 47-48.

[919] L'avant-projet prévoyait un contrôle *a priori* quasi judiciaire : FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 49-50.

que dans le second les actes préparatoires doivent révéler clairement l'intention de réitérer l'acte[920].

A la différence du risque visé par la LMSI, le soupçon exigé par le cautionnement préventif découle donc obligatoirement d'actes commis par la personne concernée. De plus, le cautionnement préventif ne concerne que le risque de commission d'une infraction, alors que la LMSI concerne les risques pour la sécurité, sans qu'il s'agisse nécessairement d'une infraction. 597

3. La procédure

Le contrôle *a priori* se compose d'un contrôle judiciaire appelé procédure d'approbation et d'un contrôle politique appelé procédure de décision[921]. L'Office fédéral fait une demande écrite d'utilisation de moyens spéciaux de recherche d'informations au Tribunal administratif fédéral (procédure d'approbation). Cette demande contient le but précis à atteindre, le perturbateur présumé, les moyens spéciaux qui doivent être utilisés, la durée pendant laquelle ces moyens spéciaux doivent être utilisés ou le délai dans lequel l'ordre doit être exécuté. Le Tribunal administratif fédéral statue dans un délai de septante-deux heures. L'autorisation peut être accordée pour une durée de six mois au maximum et la demande peut être renouvelée deux fois pour des durées maximales de trois mois. 598

Une fois l'autorisation du Tribunal administratif fédéral accordée, l'Office demande au chef du DFJP d'ordonner l'utilisation des moyens approuvés (procédure de décision). Le chef du DFJP consulte alors le chef du DDPS et ordonne, en cas d'accord réciproque, l'utilisation des moyens spéciaux de recherche d'informations approuvés par le Tribunal administratif fédéral. L'emploi de moyens techniques de surveillance dans le cadre de la LMSI nécessitera une autorisation juridique et une double autorisation politique. Si l'un de ces trois accords n'est pas obtenu, l'utilisation ne sera pas autorisée. En 599

[920] DUPUIS / GELLER / MONNIER, *et al.*, *Petit commentaire CP I*, pp 644-645; GRAVEN, *Le cautionnement préventif*; HURTADO POZO, *Partie générale*, pp 524-525; KILLIAS / KUHN / DONGOIS, *et al.*, *Précis de droit pénal général*, pp 273-274; KUHN, *Procédure pénale unifiée*, p. 65.

[921] Art. 18d ss P-LMSI II, *Message du CF relatif à la LMSI II*, pp 4833-4837; FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 48-54. L'avant-projet ne prévoyait pas la compétence du TAF mais celle d'un organe quasi judiciaire.

cas d'urgence, l'autorisation peut être donnée par le chef de l'Office et une demande *ad hoc* est présentée dans les vingt-quatre heures au Tribunal administratif fédéral.

600 Dans le mois qui suit la fin de la surveillance, l'Office communique à la personne surveillée les motifs, le type et la durée de la surveillance dont elle a été l'objet. Comme en matière pénale, il est possible de différer la communication ou d'y renoncer si cela est nécessaire, mais les accords du Tribunal administratif fédéral et des chefs du DFJP et du DDPS sont nécessaires[922]. La possibilité de renoncer à une communication est plus large qu'en matière de surveillance pénale[923]. Le droit d'accès indirect qui peut être exercé par le biais du Préposé fédéral à la protection des données et à la transparence doit être distingué de la communication ultérieure et ne la remplace pas.

601 Un recours peut être déposé devant le Tribunal administratif fédéral, puis le Tribunal fédéral, contre les décisions prises en application de la LMSI. Le délai de recours de trente jours court à compter de la communication de la surveillance, mais le recours peut aussi être déposé avant la communication. Le recours est un moyen de droit complet étant donné que le recourant peut faire valoir une violation du droit, un abus ou excès du pouvoir d'appréciation et une constatation inexacte ou incomplète des faits[924].

602 On pourrait penser que le recours est ouvert contre la décision du Tribunal administratif fédéral autorisant la surveillance et celle des chefs du DFJP et DDPS ordonnant la surveillance. Le recours devant le Tribunal administratif fédéral contre une décision qu'il a rendue ou contre la décision des chefs du DFJP et DDPS prise dans les limites de la décision du Tribunal administratif fédéral paraît cependant douteux. Le Tribunal fédéral a d'ailleurs fait savoir, lors de la consultation, qu'il fallait préciser que la décision du Tribunal administratif

[922] Art. 18i P-LMSI II, *Message du CF relatif à la LMSI II*, pp 4838-4840; FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 54-56.
[923] RIKLIN, *Vollzugsdefizite noch und noch*, p. 20.
[924] Art. 29a P-LMSI II, *Message du CF relatif à la LMSI II*, pp 4849-4850; FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*, pp 64-65.

fédéral autorisant la surveillance n'était pas sujette à recours. La question des voies de recours devra donc être précisée.

603 Bien qu'une procédure précise avec apparemment de nombreux contrôles soit prévue, il n'en demeure pas moins que le projet LMSI-II a pour but de réintroduire des mesures de surveillance préventive. Il s'agit de développements inquiétants qui mettent en danger plusieurs droits et libertés fondamentaux[925].

[925] CESONI, *Dérives de l'antiterrorisme*, p. 56.

III. Synthèse et critique de la surveillance selon la LMSI

A. En général

604 La surveillance préventive a pour principale caractéristique qu'elle ne s'applique pas à la poursuite d'infractions déjà commises, mais à la détection d'un danger ou d'une menace pour la sécurité. Elle inclut également la recherche d'informations politiques, économiques et militaires, soit l'activité habituelle d'un service de renseignement. La personne visée par les mesures techniques de surveillance n'est donc pas prévenue au sens de la procédure pénale. Elle n'est la plupart du temps même pas soupçonnée d'avoir commis ou de vouloir commettre une infraction au sens du droit pénal.

605 En Suisse, la surveillance préventive civile repose essentiellement sur la LMSI et consiste en la recherche d'informations. La LMSI prévoit également d'autres mesures particulières comme le contrôle de sécurité pour les personnes travaillant pour le compte de l'Etat et ayant accès à des informations sensibles, la protection des bâtiments de la Confédération et des parlementaires, magistrats et agents de la Confédération particulièrement exposés, ainsi que les mesures contre la violence lors de manifestations sportives.

606 La recherche d'information se compose essentiellement de l'exploitation de sources accessibles au public, des informations transmises par d'autres autorités et la surveillance de lieux publics et librement accessibles. Le Service d'analyse et de prévention (SAP) reste très discret sur ses activités. La récolte des données, et leur exploitation, restent peu transparentes même si le cadre légal semble plutôt respecté[926]. La LMSI mentionne différents types de surveillance comme les opérations préventives, les programmes de recherche préventifs, les programmes d'examen et la liste d'observation. Pour simplifier, on peut dire qu'il s'agit de cas différents lors desquels la surveillance est opérée et les principes-cadres concernant la manière dont elle est conduite. Les détails ne sont

[926] Voir à ce sujet la partie suivante consacrée à l'exploitation des données recueillies.

pas réglés au niveau légal et il est bien difficile de savoir dans quelle mesure le SAP procède en suivant les catégories prévues par la loi ou différemment.

B. Une surveillance limitée

607 La loi ne permet actuellement pas de procéder à une surveillance aussi intrusive à titre préventif que dans le cadre d'une enquête pénale. La surveillance de la correspondance par poste et télécommunication, la surveillance des relations bancaires, la surveillance de lieux qui ne sont pas librement accessibles, notamment au moyen d'appareils techniques et la perquisition d'un système informatique, ne sont ainsi pas permises par la LMSI. Si les mesures portant le plus atteinte à la sphère privée ne sont pas autorisées, c'est simplement et logiquement parce qu'à ce stade, aucune infraction ou acte préparatoire à la commission d'une infraction au sens pénal n'a été commis.

608 D'aucuns souhaitent une extension de ces moyens et que toutes les mesures autorisées dans le cadre de l'instruction pénale soient également admises pour la surveillance préventive. Les mesures seraient alors soumises à une autorisation politique et judiciaire *a priori*, et un contrôle judiciaire *a posteriori* serait encore possible sous la forme d'un recours contre la communication de la surveillance. Ce projet, connu sous le nom de LMSI II, a suscité de très vives oppositions et son aboutissement est remis en question.

609 Si les moyens de surveillance sont limités, la quantité de données enregistrées dans ISIS est importante. La qualité des informations est pourtant sujette à caution puisque les contrôles requis n'ont la plupart du temps pas eu lieu. La conservation d'une part importante des enregistrements a lieu de manière contraire à la loi. Ces faits sont inquiétants car les informations utiles qui devraient figurer dans ISIS pour la protection de l'Etat ne peuvent pas remplir leur rôle correctement, mais encore plus parce que les droits des citoyens sont régulièrement violés. Le fait que ces derniers n'en ont pas connaissance les empêche de s'y opposer et de faire valoir leurs droits. On devrait pourtant pouvoir compter dans ces domaines sur un très strict respect de la loi par l'autorité.

610 Les moyens de surveillance à disposition des agents de renseignement et de la police ne sont pas à remettre en cause. Le respect de la loi doit par contre être assuré, en prenant les mesures de contrôle nécessaires. Un changement de la manière de considérer les droits du citoyen et la protection des données en particulier est nécessaire au sein des services de renseignement.

C. Un contrôle judiciaire limité

611 Les mesures techniques de surveillance étant limitées à celles qui portent le moins atteinte à la sphère privée, leur contrôle au cas par cas est également restreint. Mis à part le contrôle de sécurité (qui demande la collaboration et l'autorisation de la personne concernée), les mesures de surveillance basées sur la LMSI ne sont pas soumises à une procédure d'autorisation.

612 Il n'y a donc pas de contrôle judiciaire, ni *a priori*, ni *a posteriori*. La loi prévoit les cas dans lesquels une surveillance peut être mise en place et l'autorité doit agir dans ce cadre-là. Une surveillance plus globale est exercée par la Délégation des Commissions de gestion des Chambres fédérales (DélCdG) et le Préposé fédéral à la protection des données et à la transparence (PFPDT)[927]. Le législateur considère qu'une voie de recours judiciaire n'est pas nécessaire car les mesures de surveillance actuellement utilisées ne portent pas une atteinte suffisante à la vie privée. La Cour européenne des droits de l'homme a déduit de l'art. 8 CEDH que le bien-fondé de la surveillance doit pouvoir être contrôlé *a priori* ou *a posteriori* par une autorité judiciaire indépendante et impartiale[928]. L'art. 8 CEDH protège contre toute atteinte à la sphère privée, même les atteintes limitées. Que l'atteinte soit limitée donc proportionnée au but et qu'elle repose sur une base légale signifie qu'elle est admissible, mais pas qu'il n'y a pas d'atteinte et qu'un contrôle judiciaire ne serait pas nécessaire. C'est d'ailleurs ce contrôle judiciaire qui doit décider si l'atteinte est admissible ou non.

613 Le recours au Tribunal administratif fédéral doit ainsi être considéré comme recevable au sens de l'art. 32 al. 1 lit. a *in fine* LTAF. Pour éviter toute ambiguïté, une voie de recours *ad hoc* pourrait être inscrite dans la LMSI.

[927] En matière d'exploration radio : l'autorité de contrôle indépendante.
[928] Arrêt KRUSLIN c. France, du 24 avril 1990, série A n° 176-A, § 34.

D. Un droit d'accès limité

La LMSI ne prévoit pas non plus une information automatique de la personne surveillée et un droit d'accès en application de la Loi sur la protection des données n'existe pas. Il est néanmoins possible de demander au Préposé à la protection des données de procéder à un contrôle des données contenues dans le système ISIS utilisé par le Service d'analyse et de prévention. C'est le droit d'accès indirect prévu par l'art. 18 LMSI. La personne qui exerce ce droit ne recevra qu'une communication du PFPDT indiquant en substance que si des données sont traitées elles le sont de manière conforme au droit. Une seconde vérification peut être demandée au Président de la Cour I du Tribunal administratif fédéral. Si le PFPDT peut contrôler la légalité de la récolte des informations enregistrées, il n'en connaît pas la véracité, que seule la personne concernée peut vérifier. 614

Ces possibilités de vérifications par des organes tiers ne constituent pas un véritable droit d'accès alors que l'application des art. 8 et 9 LPD pourrait rendre le système conforme aux exigences de la CEDH, sans pour autant mettre en péril l'activité policière et judiciaire. Le PFPDT peut néanmoins transmettre des informations de manière exceptionnelle lorsqu'il n'existe pas d'autre moyen d'éviter un dommage grave et irréparable, et pour autant que la sécurité intérieure ou extérieure ne soit pas menacée. L'usage du droit d'accès indirect a deux autres effets sur le Service d'analyse et de prévention : il vérifie que les données sont encore pertinentes en les transmettant au PFPDT et il est tenu d'informer les personnes concernées au plus tard au moment où les données ne sont plus conservées, soit parfois plusieurs années voire dizaines d'années après. 615

E. La collaboration avec les autorités pénales

Les informations recueillies dans le cadre de la surveillance préventive sont principalement conservées dans le système de traitement des données relatives à la protection de l'Etat (ISIS). Lorsqu'elles sont utiles à prévenir ou poursuivre des actes punissables, elles sont transmises à l'autorité de poursuite pénale compétente qui les utilisera, normalement après avoir vérifié qu'elles ont été recueillies légalement. 616

Cinquième partie :
L’exploitation des données recueillies

I. Remarques liminaires

La surveillance ne se limite pas à récolter des données. Les nombreux éléments recueillis doivent ensuite être triés, analysés et exploités. Ils sont transmis ou conservés pour une utilisation ultérieure dans un système structuré de classement de l'information, généralement appelé base de données. Il n'existe pas un gigantesque dossier contenant toutes les informations en Suisse, mais de nombreuses bases de données, parfois divisées en systèmes, registres, et fichiers, tantôt reliées entre elles tantôt séparées. Ces bases de données obéissent à des règles différentes, quoique souvent similaires. 617

On présentera d'abord les principales bases de données utilisées lors d'enquêtes pénales ou en matière de renseignement. L'accès aux données sera ensuite abordé et plus particulièrement le droit de l'individu de connaître les données collectées à son sujet, les conditions à respecter et les moyens mis à sa disposition. L'accent sera mis sur les bases de données fédérales. 618

La publication de données à large échelle, en particulier la publication dans les médias d'images issues d'une vidéosurveillance, constitue un cas particulier qui sera brièvement abordé. 619

II. Les bases de données

A. Les bases de données fédérales

1. Le système informatisé des Offices centraux de police criminelle

620 Le système informatisé des Offices centraux de police criminelle (JANUS) repose sur les art. 10, 11, 13 et 18 LSIP et l'Ordonnance JANUS[929].

621 Il se décompose en quatre sous-systèmes en fonction des différents objectifs que la LSIP lui impose : un système d'appui aux enquêtes de police judiciaire de la Confédération (art. 10 LSIP) ; un système de traitement des données relatives aux infractions fédérales (art. 11 LSIP) qui a pour but de faciliter l'exécution des tâches légales d'information, de coordination et d'analyse de la Police judiciaire fédérale, l'exécution des enquêtes préliminaires dans les domaines de compétence de la Confédération, la coopération de la Police judiciaire fédérale avec les autorités douanières, policières et de poursuite pénale cantonales dans le cadre de leurs compétences en matière de lutte contre le crime intercantonal ou international, ainsi que la collaboration de la Police judiciaire fédérale avec les autorités étrangères dans la lutte contre la criminalité internationale ; un système d'appui aux enquêtes préliminaires et de police menées par les cantons dans leur domaine de compétence en matière de poursuite pénale (art. 13 LSIP) ; un système de gestion des affaires et des dossiers utilisés par l'Office fédéral de la police (fedpol) (art. 18 LSIP).

622 JANUS est également divisé en plusieurs catégories : « Personnes et antécédents » (PV) où sont enregistrées des informations sur des personnes, des organisations et des personnes morales et leurs antécédents provenant d'enquêtes préliminaires, d'enquêtes de police judiciaire ou de sources accessibles au public, « Journaux » (JO) où sont enregistrées par affaire des données provenant d'enquêtes préliminaires, d'enquêtes de police judiciaire ou

[929] Ordonnance du 15 octobre 2008 sur le système informatisé de la Police judiciaire fédérale (RS 360.2).

de sources accessibles au public (notamment surveillances des télécommunications, mains courantes d'observation, mains courantes d'enquête), « Rapports de police » (RP) où sont établis et gérés les rapports et dénonciations nécessaires à l'accomplissement des tâches de la Police judiciaire fédérale, « Gestion des affaires et des dossiers » (GA) où sont enregistrées les données nécessaires au suivi des affaires, « Renseignements généraux » (ER) où sont enregistrées des données utiles à l'accomplissement des tâches telles que répertoires téléphoniques, extraits de presse, descriptifs des compétences de diverses administrations ou informations provenant de sources accessibles au public, « Rapport de situation » (LA) où sont enregistrés des rapports décrivant la situation nationale et internationale, « Analyses » (AN) où sont enregistrés les résultats des mandats d'analyse, « Fausse monnaie » (BL) où sont enregistrés les différents types de fausse monnaie et les techniques de faux monnayage, et finalement les données réunies par la Police judiciaire fédérale dans le cadre d'enquêtes de police judiciaire portant sur des procédures pendantes d'une part et dans le cadre d'enquêtes préliminaires d'autre part[930].

2. Le système de recherche informatisée de police

Le système de recherche informatisée de police (RIPOL) repose sur l'Ordonnance RIPOL[931]. Il est exploité conjointement par les autorités compétentes de la Confédération et des cantons. 623

Le RIPOL comprend une banque de données concernant la recherche de personnes, une banque de données concernant la recherche de véhicules, et une banque de données concernant les infractions non élucidées et la recherche d'objets[932]. Les autorisations de traiter ou de visualiser les données enregistrées dans le RIPOL sont détaillées dans l'annexe à l'Ordonnance RIPOL. 624

[930] Art. 5 à 7 Ordonnance IPAS.

[931] Ordonnance du 15 octobre 2008 sur le système de recherches informatisées de police (RS 361.0).

[932] Au 31 décembre 2009, le RIPOL contenait l'enregistrement de 205 320 personnes, 348 907 véhicules et 1 394 507 infractions non élucidées. Pour plus de détails et les données 2007-2009, voir FEDPOL, *Rapport 2009*, p. 68.

625 Le RIPOL sert principalement à la recherche du lieu de séjour de personnes disparues, à la recherche et à l'éventuelle arrestation de personnes dans le cadre d'une enquête pénale, à l'exécution des mesures d'éloignement et des mesures de contrainte prises à l'égard d'étrangers, à la recherche de véhicules et d'objets perdus ou volés, à la prévention de l'enlèvement international d'enfants, ainsi qu'à la surveillance discrète ou au contrôle ciblé de personnes et de véhicules en vue de poursuivre une infraction pénale ou de prévenir les risques pour la sécurité publique. L'art. 15 al. 5 LSIP permet aux utilisateurs qui en ont l'autorisation d'utiliser l'interface RIPOL pour interroger simultanément d'autres banques de données, comme les systèmes SYMIC, ISA, MOFIS, FABER, PAGIRUS et INFOSTAR[933].

3. L'index national de police

626 L'index national de police repose sur l'art. 17 LSIP et l'Ordonnance sur l'index national de police[934].

627 L'index permet de déterminer si des données se rapportant à une personne déterminée sont traitées ou non dans les systèmes d'information des polices cantonales, JANUS, RIPOL, N-SIS et IPAS (seulement les catégories Interpol, Europol, N-SIS et AFIS-ADN). Il facilite la recherche d'informations sur les personnes et les procédures d'entraide judiciaire et d'assistance administrative[935]. L'index permet seulement d'obtenir l'identité de la personne, l'autorité responsable, la date et le motif de l'inscription, ainsi que le système d'information de provenance des données. Les renseignements supplémentaires doivent être obtenus de la part de l'autorité compétente, en application des principes habituels d'entraide. Chaque police cantonale décide les inscriptions qu'elle souhaite enregistrer, l'échange et la conservation des données policières restant une compétence cantonale. L'absence d'inscription à l'index national de

[933] Ces différents systèmes sont repris en détails dans les pages suivantes.

[934] Ordonnance du 15 octobre 2008 sur l'index national de police (RS 361.4). Sur les fichiers de police en droit français : KORNMAN, *Les fichiers de police*.

[935] Avant l'entrée en vigueur de cet index, l'autorité policière qui avait besoin de renseignements sur un individu devait présenter une demande aux 25 autres cantons ainsi qu'à fedpol pour obtenir un résultat : *Message du CF relatif aux systèmes d'information de police*, p. 4837.

police n'implique donc pas automatiquement l'inexistence de tout dossier en mains cantonales.

4. Le système informatisé de gestion et d'indexation de l'Office fédéral de la police

Le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (IPAS)[936] se fonde sur l'Ordonnance IPAS[937]. 628

IPAS est le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (fedpol). Il doit permettre principalement de traiter des données concernant les affaires de l'office et de gérer le suivi des dossiers. IPAS se compose de trois sous-systèmes : le système de traitement des données relatives à la coopération policière internationale et intercantonale (12 LSIP), le système visant à l'identification de personnes dans le cadre de poursuites pénales et de la recherche de personnes disparues (14 LSIP) et le système de gestion des affaires et des dossiers de fedpol (18 LSIP). IPAS comprend les catégories Interpol, Europol, N-SIS, AFIS-ADN, recherche de personnes disparues et documents d'identité. 629

5. Le système automatisé d'identification des empreintes digitales

Le système automatisé d'identification des empreintes digitales (AFIS)[938] se fonde sur l'Ordonnance sur le traitement des données signalétiques biométriques (RS 361.3)[939]. 630

AFIS contient les empreintes des deux pouces, les empreintes des dix doigts, les empreintes palmaires et les traces relevées sur les lieux de délits. Les images des 631

[936] Das informatisierte Personennachweis, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei (IPAS).

[937] Ordonnance du 15 octobre 2008 sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (RS 361.2).

[938] Automated Fingerprint Identification System (AFIS). Sur le traitement des données dans AFIS : ALBERTINI, *Tableaux synoptiques des enquêtes de police*, pp 203-204.

[939] Ordonnance du 21 novembre 2001 sur le traitement des données signalétiques biométriques (RS 361.3).

empreintes et traces sont enregistrées électroniquement et accompagnées d'un numéro, appelé numéro de contrôle du processus. On y trouve trois catégories d'empreintes : celles des personnes qui accomplissent des tâches dans les domaines de la police technique et scientifique et de la collecte des éléments de preuve, afin de distinguer leurs traces de celles des suspects, les empreintes liées à des affaires pénales et celles liées aux demandes d'asile[940].

632 La deuxième catégorie regroupe les empreintes digitales et palmaires d'auteurs inconnus qui ont été relevées sur les lieux de délits, les empreintes digitales et palmaires de personnes ou de cadavres inconnus ou connus sous une fausse identité. Le numéro de contrôle du processus, ainsi que les données personnelles correspondantes ou les informations sur les lieux de délits, sont traités dans le système IPAS de fedpol[941].

633 La troisième catégorie contient les empreintes digitales de requérants d'asile relevées conformément à la législation en matière d'asile et les empreintes des deux pouces relevées sur les personnes étrangères conformément à la législation sur les étrangers et sur les douanes, notamment lorsqu'elles font usage de faux documents d'identité, ne justifient pas de leur identité ou encore entrent en Suisse, y séjournent ou quittent la Suisse illégalement. Le numéro de contrôle du processus et les données personnelles correspondantes sont traités dans le système SYMIC de l'ODM[942].

634 C'est le service chargé de la gestion d'AFIS qui relie le numéro de contrôle du processus aux autres données personnelles ou relatives à une trace contenues dans IPAS ou SYMIC[943].

[940] Art. 7ss de l'Ordonnance sur le traitement des données signalétiques biométriques.

[941] Voir à ce sujet le chapitre 4. Le système informatisé de gestion et d'indexation de l'Office fédéral de la police, p. 281, ci-dessus.

[942] Voir à ce sujet le chapitre 14. Le système d'information central sur la migration, p. 289 ci-dessous.

[943] Art. 12 de l'Ordonnance sur le traitement des données signalétiques biométriques.

6. Le système d'information fondé sur les profils d'ADN

Le système d'information fondé sur les profils d'ADN (CODIS)[944] est prévu par les art. 10ss de la Loi sur les profils d'ADN et l'Ordonnance sur les profils d'ADN[945]. 635

Le système CODIS permet d'effectuer la comparaison de profils d'ADN à des fins de poursuite pénale et d'identification de personnes inconnues ou disparues. On trouve d'abord dans le système CODIS les profils d'ADN des personnes soupçonnées d'avoir commis un crime ou un délit ou d'y avoir participé, des personnes condamnées, des personnes décédées et des traces. On trouve également les profils d'ADN des personnes non identifiées, vivantes ou décédées, des matériels biologiques attribuables à des personnes disparues, des parents des personnes décédées ou disparues qui doivent être identifiées hors d'une procédure pénale. Le numéro de contrôle de processus, les données relatives à une personne ou à une trace biologique et celles relatives aux lieux de l'infraction sont en revanche traitées dans le Système informatisé IPAS[946]. 636

7. Le système de traitement des données relatives à la protection de l'Etat

Le système de traitement des données relatives à la protection de l'Etat (ISIS)[947] se fonde sur l'Ordonnance sur les systèmes d'information du Service de renseignement de la Confédération[948]. 637

[944] Combined DNA Index System (CODIS). Sur le traitement des données dans le système d'informations de profils d'ADN : ALBERTINI, *Tableaux synoptiques des enquêtes de police*, pp 201-202.

[945] Loi fédérale sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues du 20 juin 2003 (LADN, RS 363) et Ordonnance du 3 décembre 2004 sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues (RS 363.1).

[946] Voir à ce sujet le chapitre 4. Le système informatisé de gestion et d'indexation de l'Office fédéral de la police, p. 281, ci-dessus

[947] ISIS (Staatsschutz-Informations-System) à ne pas confondre avec SIS (Système d'information Schengen).

[948] Ordonnance du 4 décembre 2009 sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC, RS 121.2).

638 ISIS se compose en réalité de sept systèmes — ISIS00 Général, ISIS01 Protection de l'Etat, ISIS02 Administration, ISIS03 Armes, ISIS04 Explosifs, ISIS05 News et ISIS06 Contrôles de sécurité relatifs aux personnes — et dix-huit banques de données — Protection de l'Etat (ST), Police administrative (VP), Documentation (DO), Système numérique (NU), Administration (VE), Acquisition d'armes par des étrangers (DEWA), Acquisition d'armes par des personnes domiciliées dans un autre Etat Schengen (DEWS), Révocation d'autorisations et mise sous séquestre d'armes (DEBBWA), Remise et retrait d'armes de l'armée (DAWA), Exploitation des traces laissées par des armes à feu (ASWA), BARBARA, NEWS, Portail interactif pour Open Sources (IPOS), ELIS, IPIS, Infopress, ISIS-Info et Contrôles de sécurité relatifs aux personnes (PSP) —[949].

639 ISIS est utilisé pour la mise en œuvre de mesures préventives dans le domaine de la protection fédérale de l'Etat, pour les tâches de police de sécurité et de police administrative, ainsi que pour l'exécution de la législation sur les armes.

640 Lorsqu'une information est communiquée, la Section Analyse préliminaire enregistre les personnes, organisations et objets concernés dans les bases de données et les relie à d'autres personnes, organisations, objet ou communications précédentes. C'est également la Section analyse préliminaire qui décide dans quelle banque de données (ISIS01, etc) les informations sont enregistrées. La mention « tiers » est ajoutée lors qu'une personne est enregistrée non pas en tant que telle, mais parce qu'elle est par exemple propriétaire d'un véhicule enregistré ou parce qu'elle a eu un contact avec une personne enregistrée. Les informations sont ensuite contrôlées par la Section Assurance qualité, qui doit effectuer un contrôle formel et matériel. Elle procède également à un tel contrôle cinq ans après la première communication et lors de l'enregistrement de nouvelles communications concernant cette personne. Si la personne ne représente plus une menace pour la sécurité de l'Etat, les informations doivent être détruites[950].

[949] Art. 25 OSI-SRC.

[950] *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, pp 7-9.

La procédure décrite auparavant est celle qui devrait être suivie, mais en pratique le Service analyse et prévention (SAP) semble surtout s'être contenté de procéder aux enregistrements sans procéder sérieusement aux contrôles exigés[951]. 641

8. La partie nationale du Système d'information Schengen

La partie nationale du Système d'information Schengen (N-SIS) se base sur l'art. 16 LSIP et l'Ordonnance N-SIS[952]. 642

N-SIS contient notamment une copie des données figurant dans le système central de l'UE. L'accès aux données N-SIS s'opère par le biais du RIPOL, de SYMIC, ou du système de gestion des affaires et des dossiers du bureau SIRENE[953]. 643

9. Le casier judiciaire

Le casier judiciaire est réglé par les art. 365 à 371 CP et l'Ordonnance VOSTRA[954]. 644

Le casier judiciaire est désormais informatisé. VOSTRA[955] contient des données relatives aux condamnations d'une part et des données relatives aux demandes d'extraits déposées dans le cadre d'enquêtes pénales en cours. Ces données sont traitées séparément. Le casier judiciaire est utilisé essentiellement pour la conduite de procédures pénales, l'exécution des peines et des mesures, les contrôles de sécurité, les décisions en matière de recrutement militaire, les mesures d'éloignement et d'expulsion contre des étrangers, les procédures de naturalisation, les mesures tutélaires, etc. 645

---

951 *Rapport de la DélCdG sur le traitement des données dans le système ISIS*, notamment pp 9-13 et 62-64.

952 Ordonnance du 7 mai 2008 sur la partie nationale du Système d'information Schengen (N-SIS) et sur le bureau SIRENE (362.0).

953 Supplementary Information Request at the National Entry (Service centralisé pour l'échange de toutes les informations supplémentaires). Le bureau SIRENE est l'interlocuteur national unique dans le cadre du système d'informations Schengen (SIS).

954 Ordonnance du 29 septembre 2006 sur le casier judiciaire (RS 331).

955 Vollautomatisiertes Strafregister.

646 VOSTRA contient notamment les condamnations pénales pour lesquelles une peine a été prononcée en raison d'un crime ou d'un délit prévu par le CP, le CPM ou une autre loi fédérale, les acquittements lorsqu'une mesure est prononcée pour les infractions précitées, les condamnations en raison de contraventions prévues par le CP, le CPM ou par une autre loi fédérale lorsqu'une amende de plus de CHF 5000.- ou un travail d'intérêt général de plus de 180 heures est prononcé. En ce qui concerne les mineurs, les condamnations ne sont inscrites que lorsqu'il s'agit d'une privation de liberté ou d'un placement en établissement fermé.

10. Le système d'information en matière de documents d'identité

647 Le système d'information en matière de documents d'identité (ISA)[956] repose sur les art. 10ss de la Loi sur les documents d'identité[957].

648 ISA contient essentiellement les données enregistrées sur les documents d'identité et permet notamment de vérifier l'identité annoncée sur la base du document d'identité présenté ou des données biométriques, de contrôler les documents d'identité valables et invalides, de vérifier l'authenticité des documents, d'empêcher l'établissement et la modification injustifiés de documents d'identité, de décider du retrait des documents d'identité invalides ou utilisés abusivement, etc. Il existe encore une banque de données fédérale sur la carte d'identité 95 (CI-95) et des registres cantonaux. La carte d'identité 95 est valable jusqu'en 2012. Les inscriptions la concernant n'ont pas été reportées dans ISA. Quant à la banque de données ARKILA, elle contient une collection de références de documents d'identité et de légitimation de tous les pays étrangers[958].

[956] Informationssystem Ausweisschriften (ISA).

[957] Loi fédérale du 22 juin 2001 sur les documents d'identité des ressortissants suisses (LDI, 143.1).

[958] L'Union européenne gère un Registre public en ligne de documents d'identité et de voyage librement accessible à l'adresse : http://www.consilium.europa.eu/prado. Il est cependant plus limité que ARKILA qui contient plus de 1800 documents enregistrés : FEDPOL, *Rapport 2009*, p. 71.

ISA est un système d'information administratif qui ne contient pas de signalements et ne permet pas d'effectuer des recherches. Seule la vérification des données personnelles dans le RIPOL permet de découvrir un signalement[959]. 649

11. Le système d'information relatif aux personnes qui ont commis des actes de violence lors de manifestations sportives

Le système électronique d'information relatif aux personnes qui ont commis des actes de violence lors de manifestations sportives (HOOGAN) est fondé sur les art. 24a ss de la LMSI et 8ss de l'Ordonnance sur les mesures de police administrative et les systèmes d'information de l'Office fédéral de la police[960]. 650

HOOGAN contient les données relatives aux personnes qui ont été soumises à des interdictions de stades et qui ont commis des actes de violence lors de manifestations sportives, ou qui sont soumises à des mesures au sens des art. 24b à 24e LMSI, soit une interdiction de périmètre, une interdiction de se rendre dans un pays donné, une obligation de se présenter à la police ou une garde à vue[961]. 651

12. Les registres d'état civil

Les registres d'état civil sont réglés par les art. 39ss CC et 76ss de l'Ordonnance du 28 avril 2004 sur l'état civil[962]. 652

Le système électronique d'enregistrement INFOSTAR est accessible à tous les offices d'état civil de Suisse. Cette banque de données centrale de l'état civil contient les données d'état civil au sens de l'art. 39 al. 2 CC, notamment le numéro d'assuré AVS, les noms, le sexe, les données concernant la naissance, l'état civil, le décès, le domicile, le lieu de séjour, le statut de vie, la tutelle, les 653

[959] *Message du CF concernant la LDI*, p. 4408.

[960] RS 120 et 120.52. Voir à ce sujet le chapitre 5. Les mesures contre la violence lors de manifestations sportives, p. 244 ci-dessus et BICHOVSKY, *Prévention de la violence commise par les spectateurs*, pp 276-291.

[961] STUDER, *Mit Datenbanken gegen Hooliganismus*; VON DÄNIKEN, *Sicherheit bei Sportveranstaltungen*, pp 56-57.

[962] Ordonnance du 28 avril 2004 sur l'état civil (OEC, RS 211.112.2)

parents, les parents adoptifs, le droit de cité et la nationalité, ainsi que les données afférentes aux relations de famille[963].

13. Le système d'information du Bureau de communication en matière de blanchiment

654 Le système d'information du Bureau de communication en matière de blanchiment d'argent (GEWA) est prévu par l'art. 35 de la Loi sur le blanchiment d'argent et les art. 14ss de l'Ordonnance sur le Bureau de communication en matière de blanchiment d'argent[964]. Il contient des données liées à la lutte contre le blanchiment d'argent, la lutte contre la criminalité organisée et le financement du terrorisme[965].

655 En matière de lutte contre le blanchiment d'argent, les données traitées dans GEWA concernent les transactions suspectes, les personnes et les sociétés faisant l'objet de soupçons fondés de blanchir de l'argent ou de tenter de blanchir de l'argent, les personnes et les sociétés faisant l'objet de soupçons fondés de préparer, de commettre ou de faciliter des actes criminels préparatoires au blanchiment d'argent.

656 Quant à la lutte contre la criminalité organisée et le financement du terrorisme, les données traitées dans GEWA concernent les transactions suspectes, les personnes et les sociétés faisant l'objet de soupçons fondés d'appartenance à une organisation criminelle (art. 260ter CP) ou de financement du terrorisme (art. 260^{quinquies} CP) et les personnes faisant l'objet de soupçons fondés de préparer, de faciliter ou de participer à la commission d'actes délictueux dont on peut présumer qu'ils sont le fait d'une organisation criminelle.

[963] Pour le détail des données inscrites, voir l'art. 8 de l'Ordonnance sur l'état civil.

[964] Loi fédérale du 10 octobre 1997 concernant la lutte contre le blanchiment d'argent et le financement du terrorisme dans le secteur financier (LBA, RS 955.0) et Ordonnance du 25 août 2004 sur le Bureau de communication en matière de blanchiment d'argent (OBCBA, RS 955.23).

[965] Art. 16 OBCBA.

14. Le système d'information central sur la migration

Le système d'information central sur la migration (SYMIC) repose sur la Loi sur le système d'information commun aux domaines des étrangers et de l'asile et l'Ordonnance SYMIC[966]. Il a remplacé les anciens systèmes ZAR-3 et AUPER2. 657

Il contient toutes les données liées aux domaines des étrangers et de l'asile. L'annexe 1 à l'Ordonnance SYMIC dresse la liste des données contenues et les différents niveaux d'accès accordés. 658

15. Les bases de données en matière de circulation routière

En matière de circulation routière, les registres cantonaux TRAFFIC concernent les conducteurs et les véhicules. Les données sont reprises au niveau fédéral dans les registres FABER pour les autorisations de conduire et MOFIS pour les véhicules et les détenteurs de véhicules. Les mesures administratives sont enregistrées dans le registre fédéral ADMAS. 659

Le registre FABER[967] est régi par l'Ordonnance sur le registre des autorisations de conduire[968]. Il sert à délivrer les permis d'élève conducteur, de conduire et de moniteur de conduite, à contrôler les autorisations civiles et militaires de conduire ainsi qu'à établir la statistique des autorisations de conduire. Il contient des données relatives à la personne, l'adresse du lieu de domicile, des informations de contrôle, ainsi que les données relatives au permis et à la catégorie. 660

Le registre automatisé des véhicules et des détenteurs de véhicules (MOFIS) est réglé par l'Ordonnance sur le registre MOFIS[969]. Ce registre fait état de tous les véhicules qui sont ou qui ont été immatriculés en Suisse et dans la Principauté 661

[966] Loi fédérale du 20 juin 2003 sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA, RS 142.51) et Ordonnance du 12 avril 2006 sur le système d'information central sur la migration (RS 142.513). En allemand : ZEMIS.

[967] Fahrberechtigungsregister (FABER).

[968] Ordonnance du 23 août 2000 sur le registre des autorisations de conduire (RS 741.53).

[969] Ordonnance du 3 septembre 2003 sur le registre automatisé des véhicules et des détenteurs de véhicules (RS 741.56).

de Liechtenstein ainsi que des données y relatives concernant les détenteurs, l'assurance responsabilité civile, le dédouanement et l'imposition.

662 Le registre ADMAS[970] se fonde sur l'Ordonnance sur le registre ADMAS[971]. Il contient toutes les mesures administratives en matière de circulation routière prononcées par des autorités suisses ou liechtensteinoises.

16. Quelques autres bases de données fédérales

663 Il existe encore un grand nombre de bases de données fédérales. Sans entrer dans le détail, on peut encore citer à titre d'exemples le système d'information VERA (administration en réseau des Suisses de l'étranger) du Département fédéral des affaires étrangères contenant les informations liées aux Suisses de l'étranger et les Suisses séjournant temporairement à l'étranger[972], le système PAGIRUS de gestion de personnes, de dossiers et d'affaires dans le domaine de l'entraide internationale en matière pénale géré par l'Office fédéral de la justice[973], ainsi que le registre foncier fédéral qui donne l'état et la portée des droits privés sur les immeubles[974].

[970] Administrativmassnahmen im Strassenverkehr (ADMAS).

[971] Ordonnance du 18 octobre 2000 sur le registre automatisé des mesures administratives (RS 741.55).

[972] Ordonnance du 7 juin 2004 concernant l'administration en réseau des Suisses à l'étranger (O-VERA, RS 235.22).

[973] Art. 11a de la Loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (EIMP, RS 351.1) et Ordonnance du 16 décembre 2009 sur le système de gestion de personnes, de dossiers et d'affaires (PAGIRUS) de l'Office fédéral de la justice (Ordonnance PAGIRUS, RS351.12).

[974] Art. 942 ss Code civil suisse du 10 décembre 1907 (CC, RS 210) et l'Ordonnance du 22 février 1910 sur le registre foncier (ORF, RS 211.432.1). Voir aussi : STEINAUER, *Les droits réels I*, pp 194-345.

B. Les bases de données cantonales et communales

Le registre du commerce[975] et le registre des poursuites et des faillites[976] existent dans toute la Suisse mais sont gérés au niveau cantonal. Le registre du commerce sert à la constitution et à l'identification des entités juridiques. Il est public et les inscriptions au registre du commerce sont publiées intégralement dans la Feuille officielle suisse du commerce (FOSC). L'Office fédéral du registre du commerce tient un registre central reprenant les informations cantonales. Il est consultable gratuitement en ligne[977]. Le registre des poursuites et des faillites n'est pas public, mais celui qui rend son intérêt vraisemblable peut consulter les procès-verbaux et les registres des offices des poursuites et des offices des faillites. Il peut également s'en faire délivrer des extraits. 664

En plus des registres précités, certains cantons gèrent un registre foncier cantonal. Les cantons et les communes disposent également de bases de données en matière fiscale et de contrôle des habitants, ainsi que dans d'autres domaines de leur compétence. 665

C. Une base de données intercantonale

L'échange et la conservation de données policières ressortent de la législation cantonale[978]. Sur proposition de la Conférence des commandants des polices cantonales de Suisse (CCPCS), la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) a adopté le 2 avril 2009 un Accord intercantonal de la coopération assistée par ordinateur des cantons lors de l'élucidation des délits de violence (Concordat ViCLAS)[979]. ViCLAS était 666

[975] Art. 927ss de la Loi fédérale du 30 mars 1911 complétant le code civil suisse (CO, RS 220) et l'Ordonnance du 17 octobre 2007 sur le registre du commerce (ORC, RS 221.411). Voir aussi : MEIER-HAYOZ / FORSTMOSER, *Schweizerisches Gesellschaftsrecht*, pp 141-163.

[976] Art 8ss de la Loi fédérale du 11 avril 1889 sur la poursuite pour dettes et la faillite (LP, RS 281.1).

[977] http://www.zefix.ch.

[978] La commission juridique du conseil national a refusé l'exigence d'ancrer ViCLAS dans la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP) en raison de la compétence manquante de la Confédération : CCPCS, *Explications relatives au Concordat ViCLAS*, p. 2. C'est pour ce motif également que les cantons peuvent décider des informations qu'ils insèrent dans l'index national de police (art. 17 al. 8 LSIP).

[979] Disponible à l'adresse :
http://www.ccdjp.ch/images/upload/090402%20ViCLAS-Vereinbarung%20f.pdf.

utilisé à titre d'exploitation pilote depuis mai 2003 par la police cantonale de Berne et il comptait déjà environ 7200 ensembles de données en juin 2008[980]. Le Concordat est entré en vigueur le 1er mai 2010.

667 ViCLAS (Violent Crime Linkage Analysis System)[981] est un système d'analyse informatisé développé au Canada par la gendarmerie royale du Canada et utilisé dans de nombreux pays européens[982]. Il permet de déceler des liens éventuels entre des infractions présentant les caractéristiques d'infractions commises en série, notamment lorsque celles-ci impliquent des violences commises pour des raisons sexuelles. Cette banque de données contient non seulement le nom de personnes qui ont été condamnées, mais aussi des informations relatives à des crimes dont l'auteur n'a pas été identifié. L'établissement d'un profil à partir de comportements observés nécessitant la saisie de nombreux détails sur l'affaire, ViCLAS est surtout utilisé en Suisse lorsque des homicides ou des actes d'ordre sexuel sont commis. Il regroupe des données de police de manière supracantonale pour les traiter au sens d'une analyse opérationnelle de cas [983]. Il ne s'agit pas d'un instrument servant à effectuer de nouvelles investigations, mais il permet de traiter et d'analyser des données existantes ressortant d'enquêtes policières cantonales ou communales[984].

D. Les bases de données privées

668 Il existe un très grand nombre de bases de données privées, avec des buts très divers. Il serait illusoire de vouloir en faire ici la présentation, cela d'autant plus que les règles juridiques applicables sont variées et ressortent pour l'essentiel du droit privé (CC et LPD). Les bases de données liées aux opérateurs téléphoniques et autres fournisseurs d'accès en matière de télécommunication ont déjà été abordées, de même que les bases de données détenues par les banques.

[980] CCPCS, *Explications relatives au Concordat ViCLAS*, p. 1.

[981] Système d'analyse des liens entre les crimes de violence (SALVAC).

[982] Pour une présentation du système : http://www.rcmp-grc.gc.ca/tops-opst/bs-sc/viclas-salvac-fra.htm.

[983] CONSEIL FÉDÉRAL, *Réponse du CF à l'interpellation Natalie RICKLI.*

[984] CCPCS, *Explications relatives au Concordat ViCLAS*, p. 5.

Parmi les bases de données privées pouvant servir de manière générale aux autorités policières et judiciaires, il y a celles de clients et d'articles vendus par les magasins (notamment par le biais de cartes fidélité, des stocks de succursales, etc.), celles des détenteurs d'abonnements (qu'il s'agisse de moyens de transports, de location de DVD, de bibliothèques, de centres de sport, ou encore de journaux), ainsi que les annuaires en tous genres. Il faut également ajouter les bases de données alimentées par les utilisateurs eux-mêmes par le biais d'Internet, qu'il s'agisse de blogs, de réseaux sociaux ou autres. 669

E. L'accès aux données

1. La législation applicable

La législation applicable dépend principalement de qui constitue et administre la base de données[985]. 670

S'il s'agit d'une base de données étatique (fédérale, cantonale ou communale), elle repose sur une base légale qui définit également les règles applicables, soit notamment qui a accès à quelles informations et à quelles conditions. En ce qui concerne le droit de l'individu de connaître et consulter les données le concernant, la Loi fédérale sur la protection des données (LPD) trouve également application pour les données traitées par des organes fédéraux. Une législation analogue existe au niveau cantonal. S'il s'agit en revanche d'une base de données privée, les dispositions de la LPD sont les seules à trouver application[986]. 671

2. L'accès de l'autorité aux données

Dans le cadre de l'instruction pénale, la police (et le ministère public à qui elle est subordonnée) a automatiquement accès aux bases de données qu'elle gère elle-même et aux bases de données qui sont conçues dans ce but. Aucune autorisation ou procédure particulière n'est nécessaire. Les autorités pénales, en particulier la police et le ministère public, peuvent également requérir des 672

[985] Nous nous limitons ici aux propos du présent ouvrage. Les questions liées au droit d'auteur ou à la concurrence déloyale ne sont pas abordées. Voir à ce sujet : TISSOT, *Bases de données et droit d'auteur*; TISSOT, *Limites juridiques à l'utilisation des bases de données informatiques*.

[986] Ainsi que les dispositions de droit privé comme les art. 28ss CC et 41 CO par exemple.

rapports officiels relatifs à des faits importants pour la procédure pénale. S'il s'agit d'élucider la situation personnelle du prévenu, seuls le ministère public et les tribunaux peuvent demander des renseignements sur les antécédents judiciaires et la réputation du prévenu, ainsi que d'autres rapports pertinents auprès de services officiels ou de particuliers (art. 195 CPP).[987]

673 Le détenteur d'objets pouvant servir de preuves est soumis à l'obligation de dépôt (art. 265 et 263 al. 1 lit. a CPP), à moins qu'il ne bénéficie d'un droit de refuser de témoigner. C'est par ce biais que peuvent être obtenus les informations contenues dans les bases de données privées. Le plus souvent cela se fera par une demande informelle de la police lors de l'enquête et une collaboration spontanée de la personne concernée, ou par le biais d'une réquisition du ministère public.

674 Chaque loi qui autorise la création et l'utilisation d'une base de données précise normalement qui peut accéder aux informations contenues dans la base de données, et cela en fonction de son but. La loi prévoit aussi dans quelle mesure il y a une transmission d'informations. Par exemple, les services de renseignement doivent transmettre aux autorités pénales compétentes les informations recueillies qui sont utiles à une procédure pénale. Ils transmettent aussi aux autres organes de sûreté de la Confédération et des cantons tous les faits susceptibles de compromettre la sûreté intérieure (art. 10 LMSI). Inversement, le Service de renseignement stratégique, les organes de poursuite pénale et les services de police doivent indiquer au Service d'analyse et de prévention les éléments dont ils ont connaissance en lien avec des menaces concrètes pour la sûreté intérieure ou extérieure (art. 11 et 13 LMSI).

675 Dans le cas d'une base de données privée, les autres personnes ayant accès à la base de données, en plus du maître du fichier, dépendent de la finalité de la base de données.

[987] *Message du CF relatif à l'unification de la procédure pénale*, pp 1195-1196.

3. Le droit d'accès de l'individu dans le cadre d'une procédure pénale

Les parties à la procédure bénéficient du droit d'être entendu, et plus particulièrement du droit de consulter le dossier (art. 107 CPP). Le droit d'accès au sens de la protection des données se distingue du droit procédural de consulter le dossier. Le premier concerne toutes les données liées au requérant, sans qu'il doive faire valoir un intérêt. Le second est plus large et permet de consulter l'intégralité du dossier de la procédure, mais exige un intérêt à la procédure[988]. 676

La Loi fédérale sur la protection des données (LPD), comme les lois cantonales en la matière, ne s'appliquent pas aux procédures pendantes[989]. Celui qui ne participe pas à la procédure doit donc attendre la clôture de celle-ci pour faire valoir son droit d'accès[990]. L'application des art. 13 al. 2 Cst. et 8 CEDH devraient pourtant permettre de faire valoir un droit d'accès aux données personnelles également durant la procédure, même si ce droit pourrait évidemment être limité ou différé par analogie avec l'art. 9 LPD[991]. Les cas où des données personnelles figurant dans un dossier de procédure pénale pendante concernent une personne qui ne participe (et ne participera) pas à la procédure sont plutôt rares et il n'y aura le plus souvent aucune objection à ce qu'une information soit transmise conformément à la LPD. 677

[988] ROSENTHAL / JÖHRI, *Handkommentar zum DSG*, p. 200.

[989] Art. 2 al. 2 lit. c LPD. *Message du CF relatif à l'unification de la procédure pénale*, p. 1137.

[990] *Message du CF relatif à l'unification de la procédure pénale*, p. 1138. On peut d'ailleurs se demander comment il pourra savoir que la procédure est terminée et que la LPD serait à nouveau applicable.

[991] L'exception de la lit. c ne devrait trouver application que si la procédure garantit un droit au moins équivalent à celui de la LPD : MAURER-LAMBROU / KUNZ, *Art. 2 DSG*, p. 52; ROSENTHAL / JÖHRI, *Handkommentar zum DSG*, pp 14-15.

L'art. 95 CPP prévoit également que l'autorité doit en principe informer sans délai la personne au sujet de laquelle des données ont été collectées à son insu. On peut en déduire un droit d'accès.

4. Le droit d'accès de l'individu en dehors de la procédure pénale

a) L'accès direct

678 Les différentes lois autorisant une base de données règlent le droit de la personne concernée de connaître les données la concernant. En plus d'une fonction de contrôle, ce droit d'accès remplit une fonction préventive[992].

679 En l'absence de dispositions spéciales, le droit d'accès prévu par les art. 8 et 9 LPD est applicable. Il permet à toute personne de demander au maître d'un fichier de lui communiquer toutes les données la concernant. La Loi fédérale sur les systèmes d'information de police de la Confédération (LSIP) y renvoie expressément[993]. Sont donc soumis aux art. 8 et 9 LPD, le système de recherche informatisée de police (RIPOL)[994], le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (IPAS)[995], le système d'information fondé sur les profils d'ADN (CODIS)[996], le système d'information en matière de documents d'identité (ISA)[997], le système électronique d'information relatif aux personnes qui ont commis des actes de violence lors de manifestations sportives (HOOGAN)[998], le système d'information central sur la migration (SYMIC)[999], le casier judiciaire[1000].

680 D'autres bases de données ne renvoient pas à la LPD, mais prévoient néanmoins un droit d'accès similaire. Il s'agit du registre des conducteurs FABER[1001], du registre des véhicules et des détenteurs de véhicules MOFIS[1002], du registre des mesures administratives ADMAS[1003], de la partie nationale du Système

[992] ROSENTHAL / JÖHRI, *Handkommentar zum DSG*, p. 199.
[993] Art. 7 LSIP.
[994] Art. 17 Ordonnance RIPOL.
[995] Art. 11 Ordonnance IPAS.
[996] Art. 15 LADN.
[997] Art. 10 LDI.
[998] Art. 24a al. 10 LMSI.
[999] Art. 19 Ordonnance SYMIC.
[1000] Art. 370 CP et 26 Ordonnance VOSTRA.
[1001] Art. 125 al. 3 OAC.
[1002] Art. 10 Ordonnance MOFIS.
[1003] Art. 13 Ordonnance ADMAS

d'information Schengen (N-SIS)[1004], des registres d'état civil[1005]. Quant à l'index national de police, cela dépend du système de provenance des inscriptions : art. 8 et 9 LPD pour les inscriptions provenant des systèmes IPAS et RIPOL, art. 8 LSIP pour les inscriptions provenant des systèmes JANUS, art. 49 Ordonnance N-SIS pour les inscriptions provenant du système N-SIS et droit cantonal pour les inscriptions issues des systèmes d'information de police des cantons (y compris par le biais de JANUS)[1006]. Le registre foncier fédéral est public et des extraits peuvent donc être obtenus, de sorte que la question d'un droit d'accès ne se pose pas[1007].

681 On applique encore un droit d'accès direct pour les données saisies dans le système d'appui aux enquêtes de la police judiciaire fédérale (un des quatre sous-systèmes composant JANUS)[1008], contrairement aux trois autres sous-systèmes de JANUS. C'est le Ministère public de la Confédération qui répond aux demandes de renseignements[1009]. Le Concordat ViCLAS prévoit finalement que l'autorité de police cantonale saisie d'une demande de consultation selon le droit cantonal doit faire suivre d'office la demande pour la base de données ViCLAS s'il y a une indication quant à une mention dans ViCLAS ou si la personne qui forme la demande l'exige. Les renseignements demandés sont fournis en respectant les éventuelles restrictions au droit de consultation de la police qui a enregistré les données[1010]. La loi cantonale bernoise sur la protection des données est applicable au surplus et sa teneur est similaire à la LPD s'agissant du droit de consulter les données[1011].

[1004] Art. 49 Ordonnance N-SIS. Dans ce cas, l'autorité responsable du signalement est préalablement consultée, y compris si le signalement provient d'un Etat Schengen.
[1005] Art. 80 OEC.
[1006] Art. 8 de l'Ordonnance sur l'index national de police.
[1007] Art. 970 CC et 105 ORF.
[1008] Art. 10 LSIP et 2 al. 2 O JANUS.
[1009] Art 7 al. 4 LSIP.
[1010] Art. 10 Concordat ViCLAS.
[1011] Art. 12 Concordat ViCLAS.

b) L'accès direct limité

682 L'art. 8 LSIP déroge au droit d'accès prévu par la LPD en prévoyant un accès limité. Il s'applique aux données saisies dans le système informatisé des Offices centraux de police criminelle (JANUS), à l'exception des données cantonales liées à des infractions n'entrant pas dans la compétence fédérale (art. 3 al. 5 O JANUS) et des données transmises dans le cadre de la coopération avec d'autres Etats Schengen (art. 3 al. 4 O JANUS)[1012]. Le droit d'accès aux premières est soumis aux dispositions cantonales, alors que le droit d'accès aux secondes est régi par l'art. 49 Ordonnance N-SIS. Comme mentionné ci-dessus, les données saisies dans le système d'appui aux enquêtes de la police judiciaire fédérale sont soumises au droit d'accès direct, bien qu'elles soient enregistrées dans JANUS. C'est également un droit d'accès direct limité qui est appliqué au système d'information du Bureau de communication en matière de blanchiment d'argent (GEWA)[1013].

683 L'art. 8 LSIP permet à fedpol de différer la réponse si aucune donnée concernant le requérant n'est traitée ou si les données traitées sont liées à des intérêts prépondérants pour la poursuite pénale, qui exigent le maintien du secret. La communication informant du report de la réponse est toujours libellée de manière identique. Elle n'est ni motivée, ni sujette à recours. La personne concernée peut demander au Préposé fédéral à la protection des données et à la transparence (PFPDT) qu'il vérifie si les éventuelles données la concernant sont traitées conformément au droit et si des intérêts prépondérants liés au maintien du secret justifient le report.

684 Après vérification, le PFPDT indique à la personne concernée, dans une réponse standard, qu'aucune donnée la concernant n'est traitée illégalement ou que s'il a constaté une erreur relative au traitement des données ou au report de la réponse, il a alors adressé à fedpol la recommandation d'y remédier. Il l'informe également de son droit de demander au Tribunal administratif fédéral de vérifier sa communication ou l'exécution de la recommandation qu'il a émise.

[1012] Art. 25 O JANUS.
[1013] Art. 27 OBCBA.

Dès que les intérêts liés au maintien du secret ne peuvent plus être invoqués, mais au plus tard après l'expiration du délai de conservation, fedpol doit transmettre les renseignements demandés. Si aucune donnée n'a été traitée, fedpol doit informer le requérant au plus tard trois ans après réception de la demande. Si le report de la réponse constitue un dommage grave et irréparable, le PFPDT peut recommander que fedpol fournisse immédiatement et à titre exceptionnel le renseignement demandé, pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure. 685

c) L'accès indirect

L'individu ne bénéficie pas d'un droit d'accès aux données qui le concernent dans le système de traitement des données relatives à la protection de l'Etat (ISIS). L'art. 18 LMSI ne prévoit sous la mention « droit d'être renseigné » qu'un accès indirect, ou plus exactement un droit de saisir le Préposé fédéral à la protection des données et à la transparence (PFPDT) pour qu'il vérifie si les données concernant le requérant sont traitées conformément au droit dans le système d'information du Service d'analyse et de prévention (ISIS)[1014]. Le préposé, contrairement au requérant, ne peut pas s'exprimer sur la véracité des informations recueillies. Ce droit d'accès indirect n'est pas conforme aux exigences constitutionnelles et de la CEDH. Une application de la LPD est souhaitable, d'autant plus que l'art. 9 permet de refuser ou différer la communication d'informations si un intérêt public prépondérant l'exige ou si une instruction pénale risque d'être compromise[1015]. 686

[1014] Voir à ce sujet le chapitre E. Le droit d'accès indirect, p. 257 ci-dessus.

[1015] Le Conseil fédéral a répondu favorablement à une motion déposée dans ce sens par la Conseillère nationale Susanne LEUTENEGGER OBERHOLZER : CONSEIL FÉDÉRAL, *Réponse du CF à la motion* LEUTENEGGER OBERHOLZER. Même si cette motion a ensuite été rejetée par le Conseil national le 3 mars 2010 (BO 2010 N 141), le Rapport du Préposé fédéral à la protection des données et à la transparence publié fin juin 2010 metionne qu'il est prévu que le droit d'accès dit indirect au système d'information ISIS soit remplacé par un droit d'accès direct comparable à celui applicable aux fichiers JANUS et GEWA lors d'une révision de la législation sur la sûreté intérieure et extérieure qui aura lieu en 2010 : PFPDT, *17ème rapport*, p. 50.
Ce droit d'accès devrait être intégré dans la future Loi sur le service de service de renseignement de la Confédération (Loi sur le SRC) qui remplacera dans quelques années la LMSI. Il pourrait également, selon les vœux du PFPDT, déjà être ajouté auparavant dans la LMSI.

d) L’absence d’accès

687 Le système automatisé d’identification des empreintes digitales (AFIS) ne prévoit pas de possibilité de faire valoir un droit d’accès. Cela n’est guère surprenant, puisque le système AFIS ne contient aucune donnée nominale en tant que telle. S’il est théoriquement soumis à la LPD, une demande pourrait théoriquement être déposée. En l’absence de données nominales contenues dans AFIS, une telle demande ne ferait guère de sens. Une demande d’accès au système d’information fondé sur les profils d’ADN (CODIS) ou au système d’information central sur la migration (SYMIC) est plus judicieuse.

III. La publication de données à large échelle

Les images provenant de caméras de vidéosurveillance sont souvent utilisées à des fins d'identification. Ces dernières années, et notamment à cause de la qualité croissante des images, elles ont été utilisées pour retrouver des personnes recherchées, y compris en les exposant au grand public. 688

La police genevoise a publié en 2003 déjà les images d'une quarantaine de casseurs présumés prises lors des manifestations intervenues à Genève pendant le sommet du G8 d'Evian[1016]. Ces images provenaient de privés, de médias et de la police[1017]. D'autres corps cantonaux de police ont fait de même à diverses reprises, notamment avec des photos de hooligans[1018]. S'il s'agissait le plus souvent de portraits diffusés durant quelques jours, la police thurgovienne est passée à l'étape suivante en diffusant la vidéo d'une agression survenue à la gare de Kreuzlingen. Cette vidéo a été transmise aux médias suisse et diffusée sur le site de la police avec un lien permettant le téléchargement[1019]. La vidéo, sur laquelle les auteurs sont clairement reconnaissables, était encore disponible sur plusieurs sites Internet une année après sa mise en ligne[1020]. Cette vidéo l'était également sur le site Internet de la police plusieurs mois après l'arrestation des auteurs présumés, qui était pourtant intervenue quelques heures seulement après la diffusion de la vidéo (et vraisemblablement avant même que la presse écrite n'ait pu s'en faire l'écho)[1021]. Cette vidéo n'avait plus le moindre intérêt conforme à son but initial et ne pouvait que satisfaire un appétit voyeur. 689

[1016] CHEVALIER, *G8: La police et la justice persistent et signent.*

[1017] POIRSON, *Le G8 ou l'art qu'ont les images de faire illusion.*

[1018] GIGON, *Le fichage risqué de hooligans sur Internet.*

[1019] ENGELHARD / BÄNZIGER, *Kreuzlinger Schläger-Trio*. Pour le descriptif des faits : SULZER / STRASSMANN / ZUBER, *Internet als zeitgemässes Fahndungsmittel*, pp 3-4.

[1020] Par exemple sur le site du journal alémanique Blick : http://www.blick.ch/news/web-tv?firstProjectID=10949&firstChannelID=52 ou sur le site du journal gratuit 20 minutes : http://www.20min.ch/ro/news/faits_divers/story/17576044, mais également sur le site de vidéo youtube :
http://www.youtube.com/watch?v=nIqA8vQunso ;
http://www.youtube.com/watch?v=DNnqyktx0VU.

[1021] BAERISWYL, *Internet als Fahndungsmittel mit Kollateralschäden*, p. 11.

690 La diffusion de portraits-robots ou d'extraits de vidéosurveillance sur Internet est largement relayée et permet généralement à la police d'obtenir rapidement des informations. Mais cette information est évidemment de nature à porter atteinte à la personnalité de la personne photographiée, ainsi qu'à la présomption d'innocence et à la garantie d'un procès équitable. Il est en est de même pour les personnes figurant sur une vidéo, qu'elles soient auteurs, victimes ou tiers, et cette atteinte est d'autant plus grand qu'une fois les données mises en ligne, leur auteur perd quasi tout contrôle.

691 Le CPP donne la possibilité au ministère public de renseigner le public sur une procédure pendante lorsque la collaboration de la population est nécessaire à l'élucidation d'infractions ou à la recherche de suspects (art. 74 al. 1 lit. a et 211 al. 1 CPP). Les juges d'instructions de Kreuzlingen ont considéré qu'ils pouvaient diffuser la vidéo étant donné qu'ils avaient obtenu l'accord de la victime et qu'il y avait un intérêt public suffisant[1022]. Le CPP ne prévoit pas expressément la possibilité d'informer par le biais d'Internet. L'interprétation de ces articles pour en faire une base légale permettant la diffusion à large échelle de vidéo issue de surveillance est trop large[1023]. Cette interprétation extensive se heurte également à la question du respect de la proportionnalité[1024].

692 Dans le cas de l'agression de la gare de Kreuzlingen, la proportionnalité ne paraît pourtant pas avoir été respectée car le même but aurait pu être atteint avec la diffusion de portraits seulement. Le caractère sensationnel de l'enregistrement vidéo ne devrait pas être utilisé pour augmenter sa diffusion [1025]. L'instruction pénale n'a pas à jouer un rôle dissuasif et ce n'est pas au procureur de prononcer une sanction indirecte en exposant les auteurs, qui bénéficient encore de la présomption d'innocence, à une condamnation par l'opinion publique[1026].

693 La diffusion d'images doit respecter strictement les exigences de proportionnalité. La présentation d'une longue séquence vidéo d'une agression

[1022] SULZER / STRASSMANN / ZUBER, *Internet als zeitgemässes Fahndungsmittel*, pp 4-7.
[1023] BAERISWYL, *Internet als Fahndungsmittel mit Kollateralschäden*, p. 13.
[1024] BAERISWYL, *Internet als Fahndungsmittel mit Kollateralschäden*, pp 13-14.
[1025] Pour un avis contraire :SULZER / STRASSMANN / ZUBER, *Internet als zeitgemässes Fahndungsmittel*, p. 9.
[1026] BAERISWYL, *Internet als Fahndungsmittel mit Kollateralschäden*, pp 14-15.

ne se justifie en principe pas et il convient de privilégier la diffusion de photos d'objets ou de portraits. En raison des dommages importants qu'elle peut causer, la diffusion d'images au public n'est admissible que comme *ultima ratio*. Le respect de la proportionnalité signifie aussi qu'il faut prendre des mesures suffisantes pour assurer le retrait des images lorsqu'elles ne sont plus nécessaires et empêcher par exemple leur indexation dans des moteurs de recherches ou leur conservation sur des sites tiers.

IV. Synthèse et critique de l’exploitation des données

A. Les bases de données

694 Les différentes bases de données fédérales sont difficiles à appréhender. En plus des considérations techniques, des décalages, notamment terminologiques, existent entre les bases de données telles qu’elles sont décrites dans les lois et celles réellement exploitées. Cela ne veut pas pour autant dire que les bases de données existantes sont illégales ou contraires aux buts fixés, mais leurs noms et leurs modes de fonctionnement diffèrent. Les différents services exploitant ces bases de données cultivent aussi une certaine opacité, pas toujours défendable, qui rend difficile la compréhension de la réalité. Certains d’entre eux ne sont pas assez sensibles aux questions liées à la protection des données (qu’ils perçoivent surtout comme des restrictions à leur activité) et leurs responsabilités vis-à-vis du respect de la loi. Pour compliquer encore la situation, plusieurs de ces bases de données sont interconnectées, mais gérées de manières différentes avec des droits d’accès aux données différents selon le type d’utilisateur.

695 Les services concernés et le législateur devraient se concerter de sorte à mettre en conformité les règles légales et les bases de données utilisées. Une plus grande transparence de la part des responsables de ces bases de données est nécessaire et n’empêcherait pas le bon déroulement du travail de la police et de la justice. Il ne s’agit pas de renseigner dans le détail sur le contenu de données personnelles ou des choix de politique criminelle, mais de présenter conformément aux principes démocratiques les moyens à disposition des pouvoirs étatiques et les conditions auxquelles ces moyens peuvent être utilisés. Un respect inconditionnel des lois est finalement nécessaire.

B. L’accès aux données

1. Actuellement

L’accès qu’une personne peut avoir aux données la concernant varie selon les bases de données. Plusieurs d’entre elles reconnaissent un droit usuel, tel que prévu par la Loi fédérale sur la protection des données. Chacun peut donc demander, sans motif particulier, à recevoir les données le concernant. Des exceptions à la transmission des données permettent de protéger les intérêts privés ou publics prépondérants (art. 9 LPD). 696

Un droit d’accès limité existe pour les données saisies dans le système informatisé des Offices centraux de police criminelle (JANUS). Fedpol répond alors dans un libellé standard que la réponse concernant le système de traitement des données concernant les infractions fédérales JANUS sera transmise ultérieurement. La réponse doit intervenir au plus tard dans les trois ans si aucune donnée n’est enregistrée ou dès qu’aucun intérêt prépondérant ne justifie plus qu’il soit renoncé à la transmission des informations. 697

Quant aux données contenues dans le système d’information du service d’analyse et de prévention (ISIS), il n’est pas possible de les consulter directement. Le droit d’être renseigné selon l’art. 18 LMSI est parfois appelé à tort droit d’accès indirect, puisqu’il ne permet pas d’accéder aux données. Il donne seulement le droit pour la personne concernée de demander au Préposé fédéral à la protection des données et à la transparence (PFPDT) de contrôler la légalité de la récolte et du traitement des données. La saisine du PFPDT oblige également le service à vérifier que les données conservées sont encore pertinentes. Elle donne encore le droit au requérant d’être informé d’office par le Service d’analyse et de prévention à l’échéance du délai de conservation des données ou lorsque les intérêts liés au maintien de la sûreté intérieure n’exigent plus le secret. 698

Dans le cas du droit d’accès limité comme dans celui du droit d’accès indirect, il est possible pour le Préposé de recommander la transmission de l’information, voire dans de rares cas de la transmettre lui-même. 699

2. Un droit à élargir

700 Ces réglementations par paliers ne sont ni souhaitables, ni conformes aux exigences de la Cour européenne des droits de l'Homme. S'il est évidemment des cas où l'information ne peut pas être transmise immédiatement et intégralement, la Loi fédérale sur la protection des données prévoit expressément de telles situations, admises également par la CEDH[1027]. L'art. 9 al. 2 LPD permet à un organe fédéral de refuser ou restreindre l'information ou la communication des renseignements demandés, voire d'en différer l'octroi dans la mesure où un intérêt public prépondérant l'exige (en particulier la sûreté intérieure ou extérieure de la Confédération) ou si l'information ou la communication des renseignements risque de compromettre une instruction pénale.

701 Idéalement, c'est donc un droit d'accès uniforme régi par la LPD qui devrait être retenu. Le principe serait la transmission des informations recueillies et la transmission différée resterait l'exception. Le Préposé pourrait conserver un rôle de contrôle et de surveillance général, mais également des pouvoirs pour des cas individuels. L'organe fédéral qui ne souhaite pas transmettre des informations ne devrait pas pouvoir en décider seul sans aucun contrôle. Une voie de recours devrait être ouverte devant une autorité judiciaire telle que le Tribunal administratif fédéral. Lorsqu'une demande est déposée et que l'organe fédéral envisage de ne pas transmettre les données, il serait souhaitable qu'il doive préalablement recueillir l'accord du Préposé ou rendre une décision motivée à son intention.

702 Le droit d'accès doit permettre à chacun de connaître les informations collectées à son insu et cas échéant de faire corriger celles qui seraient fausses. Il permet également d'exercer un contrôle sur l'autorité et oblige ainsi cette dernière à vérifier l'utilité des données encore conservées. Cet aspect est également important car lorsque des données ne sont pas régulièrement contrôlées, elles deviennent obsolètes et parfois fausses, en plus d'être inutiles.

[1027] Art. 8 ch. 2 CEDH.

Le droit d'accès n'a en revanche pas pour but d'empêcher l'exécution d'une mesure de surveillance conforme à la loi ou de permettre à une personne de se comporter différemment selon qu'elle sait qu'elle est ou non l'objet d'une surveillance active. La personne qui s'inquiète des données collectées sur son compte n'est généralement pas un criminel en fuite, mais un simple citoyen curieux ou désireux de s'assurer qu'aucun amalgame n'est fait entre lui et des personnes qu'il a pu côtoyer et qui sont, elles, susceptibles d'être l'objet d'une surveillance. 703

Si l'autorité n'est pas tenue de répondre immédiatement, le droit d'accès ne sera pas un obstacle à son activité. Dans le cadre d'une procédure pénale, le droit d'accès est régi par les règles habituelles de consultation du dossier officiel. Les données utilisées dans une procédure judiciaire ne sont pas accessibles en application des art. 8 et 9 LPD. Ce droit d'accès ne doit donc pas permettre de les consulter par le biais des résultats de la surveillance préventive si l'accès au dossier pénal n'est pas encore complet en raison de l'instruction en cours. La mention automatique dans la réponse d'une réserve des informations utilisées dans une instruction pénale en cours suffit à résoudre cette question. 704

Lorsque les données proviennent d'une surveillance préventive, cela signifie que la personne surveillée n'est soupçonnée d'aucune infraction pénale et que la surveillance n'a pas été contrôlée par une autorité judiciaire[1028]. Le délai imparti à l'autorité pour répondre, par exemple six mois, devrait lui permettre de décider sereinement de l'opportunité d'une poursuite pénale. Si aucune infraction pénale n'est retenue durant cette période, l'intérêt de l'Etat à ne pas transmettre les informations détenues doit céder le pas sur l'intérêt de l'individu à connaître les données récoltées, et, cas échéant, les faire rectifier. Cela ne signifie pas non plus que l'Etat doit mettre un terme à toute mesure de surveillance. Transmettre à une personne des informations enregistrées la concernant n'empêche nullement les services de police de continuer à exercer une surveillance et collecter des données. De plus, à l'expiration du délai de réponse de six mois, un droit de recours effectif pourrait être admis devant une autorité judiciaire. 705

[1028] Contrairement à la surveillance ordonnée sur la base du CPP. Dans le cas d'une surveillance pénale, l'autorité est tenue d'informer spontanément la personne surveillée au plus tard lors de la clôture de l'instruction.

706 Ainsi, lorsque des informations existent et que rien ne s'oppose à ce moment-là à leur transmission, elle doit avoir lieu sans délai. De la même manière, le requérant doit être immédiatement informé s'il n'y a aucune donnée à son sujet et que le fait de différer la réponse lui causerait un préjudice important. Lorsqu'une surveillance est en cours, la transmission des données doit évidemment être différée. Afin d'éviter qu'il ne soit possible de déduire de la réponse l'existence ou l'inexistence d'une surveillance, la réponse peut aussi être différée lorsqu'aucune surveillance n'existe mais qu'une telle mesure pourrait être envisagée.

707 L'accès aux données serait donc régi par les normes générales de la LPD, mais leur application tiendrait compte, comme actuellement, des intérêts particuliers liés aux procédures en cours. Le contrôle exercé par le Préposé se poursuivrait également. L'avantage serait de ne plus voir coexister différents régimes, mais aussi que les données seraient (presque) toujours transmises et cela dans un délai acceptable, alors qu'aujourd'hui une transmission n'intervient que plusieurs années après la demande, quand elle n'est pas simplement oubliée.

C. La publication des données

708 Contrairement à l'exploitation d'une base de données dont les accès sont strictement contrôlables, la diffusion sur Internet ne permet pas de s'assurer que les données sont utilisées conformément à leur but initial et que la proportionnalité est respectée. Pour ces différentes raisons, ce mode de diffusion ne devrait être utilisé que dans de rares cas et comme *ultima ratio*. Les mesures adéquates pour limiter la diffusion des images et assurer la présomption d'innocence doivent être prises.

709 L'accord de la victime à la diffusion des images doit être considéré avec beaucoup de retenue. Si celle-ci souhaite dans un premier temps l'arrestation des auteurs à tout prix, il n'est pas sûr que plusieurs années après elle apprécie de continuer à voir la vidéo de son agression circuler sur Internet.

Sixième partie : Conclusion

Conclusion et propositions

Les mesures techniques de surveillance sont utiles et nécessaires à l'aboutissement de certaines enquêtes pénales. Elles n'en représentent pas moins une atteinte à la sphère privée, d'autant plus grave si la personne visée par la surveillance n'en a pas connaissance et ne peut donc pas défendre ses droits. L'Etat est le garant du respect des règles fondamentales et il doit prendre les mesures nécessaires pour qu'elles soient respectées, même si ces mesures peuvent engendrer certains coûts et compliquer la procédure en obligeant ou permettant un contrôle par une institution indépendante. Le respect des droits individuels et la confiance de l'individu dans les institutions en dépendent. Un strict respect de la procédure par l'Etat permet également au citoyen de savoir que les pouvoirs d'enquête intrusifs sont utilisés à bon escient et qu'il n'est pas nécessaire d'interdire complètement l'utilisation de ces moyens d'investigation au motif de défendre la sphère privée de l'individu. 710

Arrivant au terme de cette étude, il est possible de retenir dix-sept propositions reprenant les principaux éléments discutés : 711

– La surveillance préventive doit être limitée à ce qui est actuellement permis, soit le recours aux sources publiques et librement accessibles. Une surveillance de la correspondance n'est, par exemple, pas souhaitable.

– Une plus grande transparence dans l'activité des services de renseignement est nécessaire et les bases de données utilisées doivent être mises en conformité avec les lois les régissant (ou des adaptations légales apportées). Ces services doivent en outre agir en respectant strictement les lois auxquelles ils sont soumis.

– Il faut assurer un droit d'accès direct pour toutes les bases de données. Il convient d'adapter les lois concernées pour que les art. 8 et 9 LPD puissent être appliqués. Ce devrait aussi être le cas lorsqu'une procédure pénale est pendante et que la personne concernée ne participe pas à la procédure.

– La surveillance de la correspondance, les autres dispositifs de surveillance et la surveillance des relations bancaires doivent suivre la même procédure et

être soumis aux mêmes conditions : le ministère public ordonne la surveillance et le tribunal des mesures de contrainte l'approuve ensuite. Une modification législative est souhaitable et permettrait de donner des compétences au Service SCPT en matière de surveillance des relations bancaires.

– De la même manière, les dispositions concernant le catalogue d'infractions permettant la surveillance, celles relatives aux raccordements de tiers et aux découvertes fortuites devraient être étendues à la surveillance des relations bancaires et aux autres dispositifs de surveillance.

– L'art. 280 CPP doit être considéré comme une base légale pour les (nouveaux) dispositifs de surveillance qui ne sont pas visés par une autre disposition du Code de procédure pénale, l'énumération contenue étant exemplative.

– La personne qui a été l'objet d'une surveillance dans le cadre d'une instruction pénale devrait toujours être informée.

– Une autorité indépendante devrait contrôler que la communication de la surveillance a bien lieu ou que le tribunal des mesures de contrainte a autorisé qu'il y soit renoncé.

– Le recours contre la surveillance (contrôle *a posteriori*) doit être possible déjà avant la communication de la surveillance ou en l'absence de communication.

– Si la surveillance porte sur des éléments protégés par le secret professionnel, une autorité indépendante doit procéder au tri des informations. Des mesures supplémentaires doivent être prises pour s'assurer que les informations obtenues en violation dudit secret ne soient ni utilisées comme preuves, ni à un autre titre, lorsque les données sont transmises immédiatement (en cas de branchement direct par exemple).

– Les preuves illégales ne doivent jamais être exploitées. La personne qui a été l'objet d'une surveillance illégale doit en être informée, de même que son droit à une indemnisation doit lui être rappelé. Les pièces seront conservées séparément et mises sous scellés jusqu'à l'issue de la procédure d'indemnisation.

– La légalité des preuves doit aussi être vérifiée lorsqu'elles sont recueillies par un privé avant d'être remises à l'autorité ou lorsqu'elles proviennent d'une surveillance dissuasive, en particulier d'installations publiques ou privées de vidéosurveillance. Les mesures de surveillance soumises à autorisation doivent rester un monopole étatique et les autres mesures de surveillance doivent être conformes au cadre légal. Elles doivent être strictement inexploitables dans tous les autres cas.

– Le Code de procédure pénale doit préciser que toutes les données originales recueillies doivent être conservées intégralement, puis détruites dans les dix jours suivant l'échéance du dernier délai de recours interne. Sur demande du requérant qui entend saisir la Cour européenne des droits de l'Homme, les données pourraient être conservées durant cette nouvelle procédure.

– L'authenticité des données doit être garantie, ou une réserve mentionnée cas échéant.

– Une haute surveillance devrait exister en matière de surveillance technique, tant pour contrôler la bonne exécution de la surveillance, l'absence de surveillance non autorisée et le respect du cadre de l'autorisation accordée, que l'exploitation des données récoltées ainsi que les questions liées à la communication de la surveillance.

– La diffusion publique de résultats de surveillance, en particulier la diffusion sur Internet d'extraits de vidéosurveillance, doit respecter de manière stricte les exigences en matière de proportionnalité. La diffusion de photos doit être privilégiée à celle de vidéos. Dans tous les cas, les mesures techniques nécessaires doivent être prises pour empêcher une diffusion plus large que ce qui est prévu et supprimer les données lorsqu'elles ne sont plus nécessaires.

– Une bonne formation technique et une meilleure collaboration entre l'autorité judiciaire, la police et les spécialistes techniques sont nécessaires afin d'utiliser correctement les possibilités techniques existantes.

712 De manière plus générale, nous pouvons nous rallier à l'avis de la Cour européenne qui considérait dans l'arrêt S. et MARPER c. Royaume-Uni « que tout Etat qui revendique un rôle de pionnier dans l'évolution de nouvelles technologies porte la responsabilité particulière de trouver le juste équilibre en la matière »[1029].

[1029] Arrêt S. et MARPER c. Royaume-Uni, no 30562/04 et 30566/04, § 112, du 4 décembre 2008.

Table des abréviations

§	Paragraphe
§§	Paragraphes
ACI	Autorité de contrôle indépendante
ADMAS	Administrativmassnahmen im Strassenverkehr (registre des mesures administratives en matière de circulation routière)
ADN	Acide désoxyribonucléique
AFIS	Automatic Fingerprint Identification Systems (système automatique d'identification des empreintes digitales)
AFNES	Automatisches Fahrzeugnummern-Erkennungssystem (système automatisé d'identification de numéros de plaques de véhicules)
al.	Alinéa
AP LSCPT	Avant-projet de révision de la LSCPT du 30 avril 2010
ARKILA	Banque de données des documents d'identité et de légitimation
Art.	Article
ATF	Arrêt du Tribunal fédéral suisse
AVS	Assurance-vieillesse et survivants
Beidou	Projet chinois de système de positionnement par satellites
Bluetooth	Technologie qui permet de relier sans fil plusieurs appareils informatiques
BO	Bulletin officiel (E du Conseil des Etats, N du Conseil National)

BÜPF	Bundesgesetz vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (LSCPT, RS 780.1)
CAI	Commission d'accès à l'information du Québec
CC	Code civil suisse du 10 décembre 1907 (RS 210)
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des Commandants des polices cantonales de Suisse
CCTV	Closed-circuit television (vidéosurveillance)
CDCJ	Comité européen de coopération juridique
CdE	Conseil de l'Europe
CdG	Commissions de gestion (des chambres fédérales)
CE	Communauté européenne
CEDH	Convention de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950 (RS 0.101)
CEP	Commission d'enquête parlementaire
CF	Conseil fédéral
CIA	Central Intelligence Agency (Agence centrale de renseignement américaine)
CJ-PD	Comité d'experts du Conseil de l'Europe sur la protection des données
CMVMS	Concordat instituant des mesures contre la violence lors de manifestations sportives
CN	Conseil national
CNA	Caisse nationale suisse d´assurance en cas d´accident (SUVA)

CNCIS	Commission nationale (française) de contrôle des interceptions de sécurité
CNIL	Commission nationale de l'informatique et des libertés
CO	Loi fédérale du 30 mars 1911 complétant le code civil suisse (Code des obligations, RS 220)
CODIS	Système d'information fondé sur les profils d'ADN
CourEDH	Cour européenne des droits de l'Homme
CP	Code pénal suisse du 21 décembre 1937 (RS 311.0)
CPM	Code pénal militaire du 13 juin 1927 (RS 321.0)
CPP	Code de procédure pénale suisse du 5 octobre 2007 (entrée en vigueur le 1er janvier 2011)
CSI-DFJP	Centre de services informatiques du Département fédéral de justice et police
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS 101)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DECT	Digital Enhanced Cordless Telephone anciennement Digital European Cordless Telephone (Téléphone sans-fil numérique amélioré)
DélCdG	Délégation des commissions de gestion des Chambres fédérales
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFJP	Département fédéral de justice et police
DPA	Loi fédérale du 22 mars 1974 sur le droit pénal administratif (RS 313.0)
DVD	Digital versatile disc (disque numérique polyvalent) ou Digital video disc (disque vidéo numérique

EIMP	Loi fédérale du 20 mars 1981 sur l'entraide internationale en matière pénale (RS 351.1)
ETSI	Institut européen des normes de télécommunication (European Telecommunications Standards Institute)
FABER	Fahrberechtigungsregister (registre des autorisations de conduire)
FBI	Federal Bureau of Investigation (Bureau fédéral d'investigation américain)
fedpol	Office fédéral de la police
FF	Feuille fédérale
FMR	False Match Rate (taux de fausses acceptations ou fausses comparaissons)
FNMR	False Non Match Rate (taux de faux rejets)
FOSC	Feuille officielle suisse du commerce
FR	Taux de faux rejets
FTE	Failure To Enroll (défaillance à l'enregistrement)
G8	Groupe des huit (Etats-Unis, Japon, Allemagne, France, Royaume-Uni, Italie, Canada et Russie)
Galileo	Projet européen de système de positionnement par satellites
GC	Grande chambre (de la CourEDH)
GEWA	Bureau de communication en matière de blanchiment d'argent
GLONASS	Système global de navigation par satellites (système russe de positionnement par satellites)
GNSS	Global Navigation Satellite System (système de positionnement par satellites)

GPRS	General Packet Radio Service (norme pour la téléphonie mobile dérivée du GSM)
GPS	Global Positioning System (système de positionnement mondial, système américain de positionnement par satellites)
GSM	Global System for Mobile Communications (norme numérique de seconde génération pour la téléphonie mobile)
HOOGAN	Système électronique d'information relatif aux personnes qui ont commis des actes de violence lors de manifestations sportives
IMEI	International Mobile Equipment Identity (numéro de 15 chiffres qui permet d'identifier de manière unique un téléphone mobile).
IMSI	International Mobile Subscriber Identity (numéro stocké dans la carte SIM qui permet à un réseau d'identifier un usager)
INFOSTAR	Banque de données centrale de l'état civil
IP (adresse IP)	Internet Protocol (numéro qui identifie chaque ordinateur connecté à Internet)
IPAS	Système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police
IRNSS	Indian Regional Navigational Satellite System (Projet indien de système de positionnement par satellites)
IRSN	Institut (français) de radioprotection et sûreté nucléaire
ISA	Informationssystem Ausweisschriften (système d'information en matière de documents d'identité)
ISDN	Integrated Services Digital Network (réseau numérique à intégration de services ou RNIS)

ISIS	Staatsschutz-Informations-System (système de traitement des données relatives à la protection de l'Etat)
JAAC	Jurisprudence des autorités administratives de la Confédération
JANUS	Système informatisé des Offices centraux de police criminelle
LA	Loi fédérale du 21 décembre 1948 sur l'aviation (RS 748.0)
LAAM	Loi fédérale du 3 février 1995 sur l'armée et l'administration militaire (RS 510.10)
LADN	Loi fédérale du 20 juin 2003 sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues (RS 363)
LAVI	Loi fédérale du 4 octobre 1991 sur l'aide aux victimes d'infractions (RS 312.5)
LBA	Loi fédérale du 10 octobre 1997 concernant la lutte contre le blanchiment d'argent et le financement du terrorisme dans le secteur financier (RS 955.0)
LCdF	Loi fédérale du 20 décembre 1957 sur les chemins de fer (RS 742.101)
LD	Loi sur les douanes du 18 mars 2005 (RS 631)
LENu	Loi du 21 mars 2003 sur l'énergie nucléaire (RS 732.1)
LEtr	Loi fédérale du 16 décembre 2005 sur les étrangers (RS 142.20)
LF-CLaH	Loi fédérale du 22 juin 2001 relative à la Convention de La Haye sur l'adoption et aux mesures de protection de l'enfant en cas d'adoption internationale (RS 211.221.31)
LFIS	Loi fédérale du 20 juin 2003 sur l'investigation secrète (RS 312.8)

LFMG	Loi fédérale du 13 décembre 1996 sur le matériel de guerre (RS 514.51)
LFRC	Loi fédérale du 3 octobre 2008 sur le renseignement civil entrée en vigueur le 1er janvier 2010 (RS 121)
LIPAD	Loi genevoise du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles
lit.	Littera
LMJ	Loi fédérale du 18 décembre 1998 sur les jeux de hasard et les maisons de jeu (RS 935.52)
LMSI	Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (RS 120)
LOAP	Loi fédérale du 19 mars 2010 sur l'organisation des autorités pénales de la Confédération
LPCO	Loi fédérale sur le programme de consolidation 2011-2013 (projet)
LPD	Loi fédérale sur la protection des données du 19 juin 1992 (RS 235.1)
LPO	Loi fédérale du 30 avril 1997 sur la poste (RS 783.0)
LSCPT	Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (RS 780.1)
LSIP	Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (RS 361)
LSRC	Loi sur le service de service de renseignement de la Confédération (l'avant-projet n'a pas encore été publié)
LTC	Loi fédérale du 30 avril 1997 sur les télécommunications (RS 784.10)
LTF	Loi du 17 juin 2005 sur le Tribunal fédéral (RS 173.110)

LTV	Loi fédérale du 20 mars 2009 sur le transport de voyageurs (RS 745.1)
MMS	Multimedia messaging service (service de messagerie multimédia pour la téléphonie mobile)
MOFIS	Registre automatisé des véhicules et des détenteurs de véhicules
MSISDN	Mobile Station Number (numéro d'appel)
NSA	National security agency (Agence de sécurité nationale américaine)
N-SIS	Partie nationale du Système d'information Schengen
OACI	Organisation de l'aviation civile internationale
OAR	Operational and Administrative Requirements
OBCBA	Ordonnance du 25 août 2004 sur le Bureau de communication en matière de blanchiment d'argent (RS 955.23).
OCDE	Organisation de coopération et de développement économiques
OCSP	Ordonnance du 19 décembre 2001 sur les contrôles de sécurité relatifs aux personnes (RS 120.4)
ODM	Office fédéral des migrations
OEC	Ordonnance du 28 avril 2004 sur l'état civil (RS 211.112.2)
OEV	Ordonnance du 22 octobre 2008 sur l'entrée et l'octroi de visas (RS 142.204)
OFJ	Office fédéral de la justice
OGE	Ordonnance du 15 octobre 2003 sur la guerre électronique (RS 510.292)
OLMJ	Ordonnance sur les jeux de hasard et les maisons de jeu (RS 935.521)

OLT 3	Ordonnance 3 du 18 août 1993 relative à la Loi sur le travail (RS 822.113)
OMSA	Ordonnance du DETEC sur les mesures de sûreté dans l'aviation du 31 mars 1993 (RS 748.122)
OMSI	Ordonnance sur les mesures visant au maintien de la sûreté intérieure (RO 2001 1829, abrogée par l'OSRC)
ONU	Organisation des Nations unies
OPO	Ordonnance du 26 novembre 2003 sur la poste (RS 783.01)
ORC	Ordonnance du 17 octobre 2007 sur le registre du commerce (RS 221.411)
Ordonnance ADNS	Ordonnance du Conseil fédéral sur le système d'information fondé sur les profils d'ADN (RO 2000 1715)
ORF	Ordonnance du 22 février 1910 sur le registre foncier (RS 211.432.1).
OSAv	Ordonnance du 14 novembre 1973 sur l'aviation (RS 748.01)
OSF	Ordonnance du 27 juin 2001 sur la sécurité relevant de la compétence fédérale (RS 120.72)
OSI-SRC	Ordonnance du 4 décembre 2009 sur les systèmes d'information du Service de renseignement de la Confédération (RS 121.2)
OSRA	Ordonnance du 4 décembre 2009 concernant le Service de renseignement de l'armée RS 510.291)
OSRC	Ordonnance du 4 décembre 2009 sur le Service de renseignement de la Confédération (RS 121.1)
O-VERA	Ordonnance du 7 juin 2004 concernant l'administration en réseau des Suisses à l'étranger (RS 235.22).

OVid-TP	Ordonnance du 4 novembre 2009 sur la vidéosurveillance dans les transports publics (RS 742.147.2)
p.	Page
PAGIRUS	Système de gestion de personnes, de dossiers et d'affaires dans le domaine de l'EIMP
PCO	Programme de consolidation
PC-TI	Comité d'experts du Conseil de l'Europe sur les techniques spéciales d'investigation en relation avec les actes de terrorisme
PDA	Personal data assistant (assistant numérique personnel)
PFPD	Préposé fédéral à la protection des données (deviendra PFPDT avec l'introduction de la Loi fédérale sur la transparence)
PFPDT	Préposé fédéral à la protection des données et à la transparence (anciennement PFPD)
P-LMSI II	Projet de révision de la LMSI visant à ajouter des moyens de surveillance
pp	Pages
PPF	Loi du 15 juin 1934 sur la procédure pénale fédérale (RO 50 709)
PPM	Procédure pénale militaire du 23 mars 1979 (RS 322.1)
PRIVATIM	Association des commissaires suisses à la protection des données
PTT	Postes, téléphones, télégraphes (ancienne administration publique suisse des postes et des télécommunications, remplacée par La Poste et Swisscom).
RFA	Renseignement des forces aériennes
RFID	Radio Frequency Identification (système d'identification par radiofréquences)

RIPOL	Système de recherche informatisée de police
RM	Renseignement militaire
RO	Recueil officiel du droit fédéral
RS	Recueil systématique du droit fédéral
RSB	Recueil systématique des lois bernoises
RSBS	Recueil systématique des lois du canton de Bâle-Ville
RSG	Recueil systématique genevois
RSN	Recueil systématique de la législation neuchâteloise
SAP	Service d'analyse et de prévention
Service SCPT	Service de surveillance de la correspondance par poste et télécommunication (parfois SSCPT)
SIM (carte SIM)	Subscriber Identity Module (carte à puce que l'on insère dans un téléphone mobile)
SIRENE	Supplementary Information Request at the National Entry (Service centralisé pour l'échange de toutes les informations supplémentaires)
SIS	Système d'information Schengen
SMS	Short Message Service (système de messagerie proposé par la téléphonie mobile)
SRC	Service de renseignement de la Confédération
SRS	Service de renseignement stratégique (SRS)
STIC	Système (français) de traitement des infractions constatées
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (CPP)
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SYMIC	Système d'information central sur la migration (en allemand ZEMIS)

TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TR	Technical Requirements
TRAFFIC	Registres cantonaux des conducteurs et des véhicules
UE	Union européenne
UMTS	Universal Mobile Telecommunications System (technologie de téléphonie mobile de troisième génération (3G))
VERA	Système d'administration en réseau des Suisses de l'étranger
ViCLAS	Violent Crime Linkage Analysis System (Système d'analyse des liens entre les crimes de violence, SALVAC)
VoIP	Voice over IP (voix sur réseau IP, technique qui permet de communiquer par la voix via l'Internet ou tout autre réseau acceptant le protocole TCP/IP)
VOSTRA	Vollautomatisiertes Strafregister (casier judiciaire informatisé)
VÜPF	Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (OSCPT, 780.11)
Wifi	Wireless Fidelity (technologie qui permet de relier sans fil plusieurs appareils informatiques)
WWW	World Wide Web (système hypertexte public fonctionnant sur Internet qui permet de consulter, avec un navigateur, des pages accessibles sur des sites)

Bibliographie

AEBI-MÜLLER REGINA E., *Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes unter besonderer Berücksichtigung der Rechtslage in der Schweiz und in Deutschland*, Berne 2005 (cité: AEBI-MÜLLER, *Personenbezogene Informationen*).

AEBI-MÜLLER REGINA E. / EICKER ANDREAS / VERDE MICHEL, *Verfolgung von Versicherungsmissbrauch mittels Observation: Grenzen aus Sicht des Privat-, des öffentlichen und des Strafrechts*, 2010, disponible à l'adresse: http://jusletter.weblaw.ch/article/de/_8338?lang=fr (cité: AEBI-MÜLLER / EICKER / VERDE, *Verfolgung von Versicherungsmissbrauch mittels Observation*).

AELLEN LAURENCE / HAINARD FRÉDÉRIC, *Secret professionnel et surveillance des télécommunications*, 2009, disponible à l'adresse: http://jusletter.weblaw.ch/article/fr/_7271?lang=fr (cité: AELLEN / HAINARD, *Secret professionnel et surveillance des télécommunications*).

AEPLI MICHAEL, *Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich*, Zurich 2004 (cité: AEPLI, *Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten*).

AGENCE FRANCE-PRESSE (AFP), *Terrorisme: UE et Etats-Unis s'accordent pour partager les données bancaires*, in: Le Monde du 8 juillet 2010, disponible à l'adresse: http://www.lemonde.fr/europe/article/2010/07/08/terrorisme-ue-et-etats-unis-s-accordent-pour-partager-les-donnees-bancaires_1385350_3214.html (cité: AFP, *Terrorisme: UE et Etats-Unis s'accordent pour partager les données bancaires*).

ALBERTINI GIANFRANCO, *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 (cité: ALBERTINI, *Tableaux synoptiques des enquêtes de police*).

ALBERTINI GIANFRANCO / FEHR BRUNO / VOSER BEAT, *Polizeiliche Ermittlung: ein Handbuch der Vereinigung der Schweizerischen Kriminalpolizeichefs zum polizeilichen Ermittlungsverfahren gemäss der Schweizerischen Strafprozessordnung*, Zurich 2008 (cité: ALBERTINI / FEHR / VOSER, *VSKC-Handbuch*).

ALBRECHT HANS-JÖRG / DORSCH CLAUDIA / KRÜPE CHRISTIANE, *Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmassnahmen*, Fribourg en Brisgau 2003, disponible à l'adresse: http://www.mpicc.de/shared/data/pdf/k115.pdf (cité: ALBRECHT / DORSCH / KRÜPE, *Rechtswirklichkeit und Effizienz der TKÜ*).

ANDRES HERBERT, *Die Internet-Überwachung in der Praxis*, in: CASSANI U. / DITTMANN V. / MAAG R. / STEINER S. (Eds.), *Mehr Sicherheit – weniger Freiheit? Ermittlungs- und Beweistechniken hinterfragt = Plus de sécurité – moins de liberté? Les techniques d'investigation et de preuve en question*, pp 239-253, Zurich; Coire 2003 (cité: ANDRES, *Die Internet-Überwachung in der Praxis*).

APSIS ANALIA, *RFID and Consumers' Privacy Rights*, Final These for ML in Legal Issues, Crime and Security of New Technologies, s. l. 2008 (cité: ASPIS, *RFID and Consumers' Privacy Rights*).

ARNAUD ELODIE / LEIN EVA / MATHÉ NICOLE / ROMANO GIAN-PAOLO, *L'insertion de données biométriques dans les documents d'identité: le cadre européen - les exemples allemand, français et italien*, www.isdc.ch, 2005, disponible à l'adresse: http://www.isdc.ch/d2wfiles/document/4138/4017/0/Article%20biom%E9trie.pdf (cité: ARNAUD / LEIN / MATHÉ / ROMANO, *L'insertion de données biométriques dans les documents d'identité*).

ARZT CLEMENS, *Polizeiliche Überwachungsmassnahmen in den USA: Grundrechtseinschränkungen durch moderne Überwachungstechniken und im War on Terrorism*, Frankfurt am Main 2004 (cité: ARZT, *Polizeiliche Überwachungsmassnahmen in den USA*).

ASSOCIATED PRESS, *Photocopiers with disk drives may lead to ID theft*, in: The Boston Globe 2007, disponible à l'adresse: http://www.boston.com/business/technology/articles/2007/03/14/photocopiers_with_disk_drives_may_lead_to_id_theft (cité: ASSOCIATED PRESS, *The Boston Globe*).

AUBERT JEAN-FRANÇOIS, *Traité de droit constitutionnel suisse*, Neuchâtel 1993 (cité: AUBERT, *Traité de droit constitutionnel*).

AUBERT JEAN-FRANÇOIS / MAHON PASCAL, *Petit commentaire de la Constitution fédérale de la Confédération suisse du 18 avril 1999*, Zurich ; Bâle ; Genève 2003 (cité: AUBERT / MAHON, *Petit commentaire*).

AUER ANDREAS / MALINVERNI GIORGIO / HOTTELIER MICHEL, *Droit constitutionnel suisse I*, 2ème éd., Berne 2006 (cité: AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse I*).

AUER ANDREAS / MALINVERNI GIORGIO / HOTTELIER MICHEL, *Droit constitutionnel suisse II*, 2ème éd., Berne 2006 (cité: AUER / MALINVERNI / HOTTELIER, *Droit constitutionnel suisse II*).

AUER CHRISTOPH, *Auswirkungen der Reorganisation der Bundesrechtspflege auf die Kantone*, in: Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht 2006, Vol. 107 (3), pp 121-140 (cité: AUER, *Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht*).

BACHER JEAN-LUC, *Commentaire ad art. 277 CPP*, in: KUHN ANDRÉ / JEANNERET YVAN (Eds.), *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: BACHER, *Art. 277 CPP*).

BACHER JEAN-LUC / ZUFFEREY NATHALIE, *Commentaire ad art. 270 CPP*, in: KUHN ANDRÉ / JEANNERET YVAN (Eds.), *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: BACHER / ZUFFEREY, *Art. 270 CPP*).

BACHER JEAN-LUC / ZUFFEREY NATHALIE, *Commentaire ad art. 279 CPP*, in: KUHN ANDRÉ / JEANNERET YVAN (Eds.), *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: BACHER / ZUFFEREY, *Art. 279 CPP*).

BAERISWYL BRUNO, *Videoüberwachung - im rechtsfreien Raum?, Datenschutzrechtliche Aspekte moderner Überwachung mittels optischen Geräten*, in: digma 2002 (1), pp 26-28 (cité: BAERISWYL, *Videoüberwachung - im rechtsfreien Raum?*).

BAERISWYL BRUNO, *Internet als Fahndungsmittel mit Kollateralschäden*, in: Sécurité & Droit 2010 (1), pp 11-15 (cité: BAERISWYL, *Internet als Fahndungsmittel mit Kollateralschäden*).

BÄNZIGER FELIX / BURKHARD CHRISTOPH / HAENNI CHARLES, *Der Strafprozess im Kanton Bern*, Berne 2010 (cité: BÄNZIGER / BURKHARD / HAENNI, *Der Strafprozess im Kanton Bern*).

BARRELET, DENIS, *Une nouvelle liberté: la liberté des télécommunications*, in: COTTIER, BERTIL (Ed.), *Le droit des télécommunications en mutation*, pp 35-48, Fribourg 2001 (cité: BARRELET, *Une nouvelle liberté*).

BARTHET ELISE, *Quelles technologies alternatives aux scanners corporels ?*, in: Le Monde du 5 janvier 2010, disponible à l'adresse: http://www.lemonde.fr/technologies/article/2010/01/05/quelles-technologies-alternatives-aux-scanners-corporels_1287790_651865.html (cité: BARTHET, *Quelles technologies alternatives aux scanners corporels ?*).

BARTSCH, VERENA, *Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und in den USA*, Berlin 2004 (cité: BARTSCH, *Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen*).

BAUER ALAIN / CORNU PIERRE, *Code de procédure pénale neuchâtelois annoté*, Neuchâtel 2003 (cité: BAUER / CORNU, *CPPN annoté*).

BAUER ALAIN / VENTRE ANDRÉ MICHEL, *Les polices en France: sécurité publique et opérateurs privés*, 2ème éd., Paris 2002 (cité: BAUER / VENTRE, *Les polices en France*).

BAUM, OLIVIER, *Rechtliche Fragestellungen im Zusammenhang mit dem kriminalpräventiven Einsatz von Videoüberwachungsanlagen im öffentlichen Raum*, 2007, disponible à l'adresse: http://jusletter.weblaw.ch/article/fr/_5970?lang=fr (cité: BAUM, *Der kriminalpräventive Einsatz von Videoüberwachungsanlagen*).

BAUMGARTNER HANS, *Zum V-Mann-Einsatz unter besonderer Berücksichtigung des Scheinkaufs im Betäubungsmittelverfahren und des Zürcher Strafprozesses*, Zurich 1990 (cité: BAUMGARTNER, *Zum V-Mann-Einsatz*).

BAUSCH STEPHAN, *Videoüberwachung als präventives Mittel der Kriminalitätsbekämpfung in Deutschland und in Frankreich*, Marburg 2004 (cité: BAUSCH, STEPHAN, *Videoüberwachung*).

BEDDIAF LACÈNE, *Vidéosurveillance, principes et technologies*, Paris 2008 (cité: BEDDIAF, *Vidéosurveillance*).

BÉNÉDICT JÉRÔME, *Le sort des preuves illégales dans le procès pénal*, Lausanne 1994 (cité: BÉNÉDICT, *Le sort des preuves illégales*).

BÉNÉDICT JÉRÔME, *Internet et le respect du secret professionnel de l'avocat*, in: CHAUDET FRANÇOIS / RODONDI OLIVIER (Eds.), *L'avocat moderne*, pp 267-286, Bâle, Genève, Munich 1998 (cité: BÉNÉDICT, *Internet*).

BENOÎT ANNE, *Le partage vertical des compétences en tant que garant de l'autonomie des Etats fédérés en droit suisse et en droit américain*, Genève; Zurich 2009 (cité: BENOÎT, *Le partage vertical des compétences*).

BERGER VINCENT, *Jurisprudence de la Cour européenne des droits de l'homme*, 11ème éd., Paris 2009 (cité: BERGER, *Jurisprudence de la CourEDH*).

BIAGGINI GIOVANNI, *BV: Bundesverfassung der Schweizerischen Eidgenossenschaft und Auszüge aus der EMRK, den UNO-Pakten sowie dem BGG*, Zurich 2007 (cité: BIAGGINI, *BV Kommentar*).

BIAGGINI GIOVANNI, *Kommentar zu Art. 113-119 BGG*, in: NIGGLI MARCEL ALEXANDER / UEBERSAX PETER / WIPRÄCHTIGER HANS (Eds.), *Basler Kommentar zur Bundesgerichtsgesetz*, pp 1111-1166, Bâle 2008 (cité: BIAGGINI, *Art. 113-119 BGG*).

BICHOVSKY AUDE, *Guantanamo, le camp de la honte?*, Grolley 2006 (cité: BICHOVSKY, *Guantanamo*).

BICHOVSKY AUDE, *Prévention de la violence commise par les spectateurs lors de manifestations sportives*, Bâle 2009 (cité: BICHOVSKY, *Prévention de la violence commise par les spectateurs*).

BIEDERMANN AUGUST, *Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000*, in: Revue pénale suisse 2002, Vol. 120 (1), pp 77-106 (cité: BIEDERMANN, *BÜPF*).

BLOSS WILLIAM, *Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects*, in: Surveillance & Society 2007, Vol. 4 (3), pp 208-228, disponible à l'adresse: http://www.surveillance-and-society.org/articles4(3)/escalating.pdf (cité: BLOSS, *Escalating U.S. Police Surveillance after 9/11*).

BOGGAN STEVE, *Cracked it!*, in: The Guardian du 17 novembre 2006, disponible à l'adresse: http://www.guardian.co.uk/idcards/story/0,,1950226,00.html (cité: BOGGAN, *Cracked it*).

BOGGAN STEVE, *New ID cards are supposed to be "unforgeable", but it took our expert 12 minutes to clone one, and programme it with false data*, in: Daily Mail du 6 août 2009, disponible à l'adresse: http://www.dailymail.co.uk/news/article-1204641/New-ID-cards-supposed-unforgeable--took-expert-12-minutes-clone-programme-false-data.html (cité: BOGGAN, *New ID cards are supposed to be unforgeable*).

BOMMER FELIX, *DNA-Analyse zu Identifizierungszwecken im Strafverfahren*, in: Revue pénale suisse 2000, Vol. 118, pp 131-160 (cité: BOMMER, *DNA-Analyse*).

BONDALLAZ STÉPHANE, *La protection des personnes et de leurs données dans les télécommunications*, Zurich 2007 (cité: BONDALLAZ, *La protection des personnes et de leurs données dans les télécommunications*).

BONDALLAZ STÉPHANE, *Le «droit à une télécommunication protégée» ou la nécessité de reconsidérer la protection de la vie privée dans les environnements numériques*, 2008, disponible à l'adresse: http://jusletter.weblaw.ch/article/fr/_6256?lang=fr (cité: BONDALLAZ, *Le droit à une télécommunication protégée*).

BOSONNET MARCEL, *In der Dunkelkammer geheimer Polizeimethoden*, in: plädoyer 2006, Vol. Beilage 6, pp 6-14 (cité: BOSONNET, *In der Dunkelkammer geheimer Polizeimethoden*).

BRAFMAN NATHALIE, *Nous savons combien vous êtes !*, in: Le Monde du 1er juillet 2007, disponible à l'adresse: http://www.lemonde.fr/web/article/0,1-0@2-651865,36-930042@51-913526,0.html (cité: BRAFMAN, *Nous savons combien vous êtes !*).

BREITENMOSER STEPHAN, *Kommentar zu Art. 13 BV*, in: EHRENZELLER BERNHARD / MASTRONARDI PHILIPPE / SCHWEIZER RAINER J. / VALLENDER KLAUS A. (Eds.), *Die schweizerische Bundesverfassung Kommentar*, pp 306-334, Zurich 2008 (cité: BREITENMOSER, *Art. 13 BV*).

BRENNER HARALD, *Die strafprozessuale Überwachung des Fernmeldeverkehrs mit Verteidigern: zugleich ein Beitrag zu den Beweisverboten, auch im Zusammenhang mit neuen Formen der Telekommunikation*, Tübingen 1994 (cité: BRENNER, *Die strafprozessuale Überwachung des Fernmeldeverkehrs*).

BRODEUR JEAN-PAUL, *Le renseignement I: concepts et distinctions préliminaires*, in: CUSSON MAURICE / DUPONT BENOÎT / LEMIEUX FRÉDÉRIC (Eds.), *Traité de sécurité intérieure*, pp 263-277, Lausanne 2008 (cité: BRODEUR, *Le renseignement*).

BRÖNNIMANN PHILIPPE, *Datenbanken als Arbeitserleichterung der Polizei*, in: CIMICHELLA SANDRO / KUHN ANDRÉ / NIGGLI MARCEL ALEXANDER (Eds.), *Neue Technologie und Kriminalität: Neue Kriminologie? = Nouvelles techonologies et criminalité: nouvelle criminologie?*, pp 121-133, Zurich ; Coire 2006 (cité: BRÖNNIMANN, *Datenbanken*).

BUCHER ANDREAS, *Personnes physiques et protection de la personnalité*, 4ème éd., Bâle 1999 (cité: BUCHER, *Personnes physiques et protection de la personnalité*).

BÜCKING HANS-JÖRG, *Polizeiliche Videoüberwachung öffentlicher Räume*, Berlin 2007 (cité: BÜCKING, *Polizeiliche Videoüberwachung öffentlicher Räume*).

BUERGENTHAL THOMAS / THÜRER DANIEL, *Menschenrechte: Ideale, Instrumente, Institutionen*, Zürich (cité: BUERGENTHAL / THÜRER, *Menschenrechte*).

BÜLLESFELD DIRK, *Polizeiliche Videoüberwachung öffentlicher Strassen und Plätze zur Kriminalitätsvorsorge*, Stuttgart 2002 (cité: BÜLLESFELD, *Polizeiliche Videoüberwachung öffentlicher Strassen und Plätze zur Kriminalitätsvorsorge*).

BUSCH HEINER, *Frei Bahn für den Staatsschutz*, in: plädoyer 2007, Vol. 3, pp 16-18 (cité: BUSCH, *Freie Bahn für den Staatsschutz*).

BUSCH HEINER, *DNA-Profile nicht über alle Zweifel erhaben*, in: plädoyer 2008, Vol. 3, pp 13-15 (cité: BUSCH, *DNA-Profile*).

BUTTARELLI GIOVANNI, *Principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données à caractère personnel au moyen de la vidéo-surveillance* 2000, disponible à l'adresse: http://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/rapport_et_etudes_experts/y-rapportbutarelli_2000.asp#P414_75963(cité: BUTTARELLI, *Principes directeurs*).

BUTTARELLI GIOVANNI, *Rapport sur la protection des données en relation avec la surveillance* 2000, disponible à l'adresse: http://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/rapports_et_etudes_des_experts/Y_Report_Butarelli_2000_fr.asp#TopOfPage (cité: BUTTARELLI, *Rapport sur la protection des données*).

CARNIEL VIRGINIE, *Protection de la sphère privée et vidéo surveillance*, in: Flash informatique 2006 (FI-spécial été), pp 17-19, disponible à l'adresse: http://sewww.epfl.ch/SIC/SA/SPIP/Publications/IMG/pdf/sp-06-page17.pdf (cité: CARNIEL, *Protection de la sphère privée*).

CARTIER JULIEN, *Localisation des téléphones portables*, in: CIMICHELLA SANDRO / KUHN ANDRÉ / NIGGLI MARCEL ALEXANDER (Eds.), *Neue Technologie und Kriminalität: Neue Kriminologie? = Nouvelles technologies et criminalité: nouvelle criminologie?*, pp 196-224, Zurich; Coire 2006 (cité: CARTIER, *Localisation des téléphones portables*).

CASSANI URSULA / DITTMANN VOLKER / MAAG RENIE / STEINER SILVIA, *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 (cité: CASSANI / DITTMANN / MAAG / STEINER, *Plus de sécurité – moins de liberté?*).

CASSANI URSULA / OURAL MIGUEL, *Commentaire ad art. 284-285 CPP*, in: KUHN ANDRÉ / JEANNERET YVAN (Eds.), *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: CASSANI / OURAL, *Art. 284-285 CPP*).

CASTEX LUCIEN / ACCARDO CHRISTOPHE, *Encadrement et risques de la biométrie*, www.e-juristes.org, 2004, disponible à l'adresse: http://60gp.ovh.net/~ejuriste/Encadrement-et-risques-de-la (cité: CASTEX / ACCARDO, *Encadrement et risques de la biométrie*).

CESONI MARIA LUISA, *Droit pénal européen et dérives de l'antiterrorisme*, in: plädoyer 2008, Vol. 5, pp 56-61 (cité: CESONI, *Dérives de l'antiterrorisme*).

CEYHAN AYSE, *La biométrie: une technologie pour gérer les incertitudes de la modernité contemporaine*, in: WUILLEUMIER ANNE / ETZIONI AMITAI (Eds.), *Police et identification: enjeux, pratiques, techniques*, pp 61-89, Paris 2005 (cité: CEYHAN, *La biométrie*).

CHAMPOD CHRISTOPHE / LENNARD CHRIS J. / MARGOT PIERRE / STOILOVIC MILUTIN, *Fingerprints and other ridge skin impressions*, International forensic science and investigation series, Boca Raton, London, New York, Washington 2004 (cité: CHAMPOD / LENNARD / MARGOT / STOILOVIC, *Fingerprints*).

CHARLES GILBERT, *Votre portable vous espionne*, in: L'Express du 6 février 2008, disponible à l'adresse: http://www.lexpress.fr/actualite/high-tech/votre-portable-vous-espionne_473495.html (cité: CHARLES, GILBERT, *Votre portable vous espionne*).

CHECOLA LAURENT, *Le scanner corporel, dernier-né des techniques de contrôle dans les aéroports*, in: Le Monde du 24 octobre 2008, disponible à l'adresse: http://www.lemonde.fr/europe/article/2008/10/24/les-scanners-corporels-une-technique-securitaire-parmi-d-autres_1110897_3214.html (cité: CHECOLA, *Le scanner corporel*).

CHEVALIER PHILIPPE, *G8: La police et la justice persistent et signent*, in: Le Courrier du 31 août 2003, disponible à l'adresse: http://lecourrier.programmers.ch/index.php?name=News&file=article&sid=2609 (cité: CHEVALIER, *G8: La police et la justice persistent et signent*).

CIMICHELLA SANDRO / KUHN ANDRÉ / NIGGLI MARCEL ALEXANDER, *Neue Technologie und Kriminalität: Neue Kriminologie? = Nouvelles techonologies et criminalité: nouvelle criminologie?*, Zurich; Coire 2006.

CLERC FRANÇOIS, *Initiation à la justice pénale en Suisse*, Neuchâtel 1975 (cité: CLERC, *Initiation à la justice pénale*).

COLL SAMI, *Consommation sous surveillance: le cas des cartes de fidélité*, à paraître (cité: COLL, *Consommation sous surveillance*).

COMITÉ D'EXPERTS SUR LES TECHNIQUES SPÉCIALES D'INVESTIGATION EN RELATION AVEC DES ACTES DE TERRORISME (PC-TI), *Rapport final d'activités sur les techniques spéciales d'investigation en relation avec des actes de terrorisme*, Conseil de l'Europe, Strasbourg 2003 (cité: PC-TI, *Rapport final d'activités sur les techniques spéciales d'investigation*).

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC (CAI), *La biométrie au Québec: les enjeux*, Québec 2002, disponible à l'adresse: http://www.cai.gouv.qc.ca/ 06_documentation/01_pdf/biom_enj.pdf (cité: CAI, *La biométrie*).

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC (CAI), *La technologie d'identification par radiofréquence (RFID), doit-on s'en méfier?* , Québec 2006, disponible à l'adresse: http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Analyse_RFID.pdf (cité: CAI, *La technologie d'identification par radiofréquence*).

COMMISSION D'ENQUÊTE PARLEMENTAIRE (CEP DFJP), Rapport complémentaire sur les événements survenus au DFJP du 31 juillet 1990, publié in FF 1990 1469-1513 (cité: *Rapport complémentaire de la CEP DFJP*).

COMMISSION D'ENQUÊTE PARLEMENTAIRE (CEP DFJP), Rapport sur les événements survenus au DFJP du 22 novembre 1989, publié in FF 1990 593-847 (cité: *Rapport de la CEP DFJP*).

COMMISSION EUROPÉENNE POUR LA DÉMOCARATIE PAR LE DROIT (COMMISSION DE VENISE), *Avis sur la vidéosurveillance dans les lieux publics par les autorités publiques et la protection des droits de l'homme*, Venise 2007, disponible à l'adresse: http://www.venice.coe.int/docs/2007/CDL-AD%282007%29014-f.asp (cité: COMMISSION DE VENISE, *Avis sur la vidéosurveillance dans les lieux publics par les autorités publiques (CDL-AD[2007]014)*).

COMMISSION EUROPÉENNE POUR LA DÉMOCARATIE PAR LE DROIT (COMMISSION DE VENISE), *Avis sur la vidéosurveillance dans les sphères publiques et privées par des opérateurs privés et dans la sphère privée par les autorités publiques et la protection des droits de l'homme*, Venise 2007, disponible à l'adresse: http://www.venice.coe.int/docs/2007/CDL-AD%282007%29027-f.asp
(cité: COMMISSION DE VENISE, *Avis sur la vidéosurveillance par des opérateurs privés (CDL-AD[2007]027)*).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *Vie privée, Droit de l'homme*, 23ème conférence internationale des commissaires à la protection des données, Paris 2002 (cité: CNIL, *23ème conférence internationale des commissaires à la protection des données*).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *Communiqué de presse du 13 juin 2007*, Paris 2007, disponible à l'adresse: http://www.cnil.fr/index.php?id=2231 (cité: CNIL, *Communiqué de presse du 13 juin 2007*).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *21ème rapport d'activité 2000 de la Commission nationale de l'informatique et des libertés*, La documentation française, Paris 2001, disponible à l'adresse: http://www.ladocumentationfrancaise.fr/rapports-publics/014000460/index.shtml (cité: CNIL, *21ème rapport*).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *22ème rapport d'activité 2001 de la Commission nationale de l'informatique et des libertés*, La documentation française, Paris 2002, disponible à l'adresse: http://www.ladocumentationfrancaise.fr/rapports-publics/024000377/index.shtml (cité: CNIL, *22ème rapport*).

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *Conclusions du contrôle du système de traitement des infractions constatées (STIC)*, Paris 2009, disponible à l'adresse: http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Controles_Sanctions/CNIL-Conclusions_des_controles_STIC.pdf (cité: CNIL, *Conclusions du contrôle du STIC*).

COMMISSIONS DE GESTION (CDG) / DÉLÉGATION DES COMMISSIONS DE GESTION DES CHAMBRES FÉDÉRALES (DÉLCDG), Rapport annuel 2007 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales du 25 janvier 2008, publié in FF 2008 4579-4688 (cité: *Rapport annuel 2007 des CdG et de la DélCdG*).

COMMISSIONS DE GESTION (CDG) / DÉLÉGATION DES COMMISSIONS DE GESTION DES CHAMBRES FÉDÉRALES (DÉLCDG), Rapport annuel 2009 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales du 22 janvier 2010, publié in FF 2010 2429-2530 (cité: *Rapport annuel 2009 des CdG et de la DélCdG*).

CONFÉRENCE DES COMMANDANTS DES POLICES CANTONALES DE SUISSE (CCPCS), *Explications relatives à l'accord intercantonal de la coopération assistée par ordinateur des cantons lors de l'élucidation des délits de violence (Concordat ViCLAS)* Berne 2009, disponible à l'adresse: http://www.kkjpd.ch/images/upload/090522%20ViCLAS-Erl%C3%A4uterungen%20f%20def.pdf (cité: CCPCS, *Explications relatives au Concordat ViCLAS*).

CONSEIL D'ETAT NEUCHÂTELOIS, *Rapport du Conseil d'Etat au Grand Conseil à l'appui d'un projet de loi portant adaptation de la loi sur la protection des données (LCPD)*, Neuchâtel 2008, disponible à l'adresse: http://www.ne.ch/neat/documents/Autorites/ConseilEtat_1487/Consultations_6230/procedures_5466/rapportLCPDVIdeoConsulat.pdf (cité: CONSEIL D'ETAT NEUCHÂTELOIS, *Rapport vidéosurveillance*).

CONSEIL FÉDÉRAL, Message concernant la Loi fédérale sur la protection des données du 23 mars 1988, publié in FF 1988 II 421-539 (cité: *Message du CF concernant la LPD*).

CONSEIL FÉDÉRAL, Message concernant la Loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire «S. o. S. - pour une Suisse sans police fouineuse» du 7 mars 1994, publié in FF 1994 1123-1216 (cité: *Message du CF concernant la LMSI*).

CONSEIL FÉDÉRAL, Message concernant les lois fédérales sur la surveillance de la correspondance postale et des télécommunications et sur l'investigation secrète du 1er juillet 1998, publié in FF 1998 3689-3771 (cité: *Message du CF concernant la LSCPT*).

CONSEIL FÉDÉRAL, Message concernant la Loi fédérale sur les documents d'identité des ressortissants suisses du 28 juin 2000, publié in FF 2000 4391-4415 (cité: *Message du CF concernant la LDI*).

CONSEIL FÉDÉRAL, Message concernant la révision totale de l'organisation judiciaire fédérale du 28 février 2001, publié in FF 2001 4000-4280 (cité: *Message du CF concernant la révision totale de l'organisation judiciaire*).

CONSEIL FÉDÉRAL, Message relatif à la Loi fédérale sur l'utilisation de profils d'ADN dans le cadre d'une procédure pénale et sur l'identification de personnes inconnues ou disparues du 8 novembre 2000, publié in FF 2001 19-48 (cité: *Message du CF relatif à la Loi fédérale sur l'utilisation de profils d'ADN*).

CONSEIL FÉDÉRAL, Analyse de la situation et des menaces pour la Suisse à la suite des attentats terroristes du 11 septembre 2001, rapport du Conseil fédéral à l'intention du Parlement du 26 juin 2002, publié in FF 2003 1674-1749 (cité: *Rapport du CF à la suite des attentats terroristes du 11 septembre 2001*).

CONSEIL FÉDÉRAL, Message relatif à la révision de la Loi fédérale sur la protection des données du 19 février 2003, publié in FF 2003 1915-1966 (cité: *Message du CF relatif à la révision de la LPD*).

CONSEIL FÉDÉRAL, Message relatif à la modification de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (Mesures contre la propagande incitant à la violence et contre la violence lors de manifestations sportives) du 17 août 2005, publié in FF 2005 5285-5314 (cité: *Message du CF relatif à la violence lors de manifestations sportives*).

CONSEIL FÉDÉRAL, Message concernant la Loi fédérale sur les systèmes d'information de police de la Confédération du 24 mai 2006 publié in FF 2006 4819-4848 (cité: *Message du CF relatif aux systèmes d'information de police*).

CONSEIL FÉDÉRAL, Message relatif à l'unification du droit de la procédure pénale du 21 décembre 2005, publié in FF 2006 1057-1372 (cité: *Message du CF relatif à l'unification de la procédure pénale*).

CONSEIL FÉDÉRAL, Rapport donnant suite au postulat du 21 février 2005 de la Commission de la politique de sécurité du Conseil des Etats (05.3006) du 9 juin 2006, publié in FF 2006 5421-5470 (cité: *Rapport du CF relatif à la lutte contre le terrorisme*).

CONSEIL FÉDÉRAL, Message relatif à l'arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'Union européenne concernant le Règlement (CE) 2252/2004 relatif aux passeports biométriques et aux documents de voyage du 8 juin 2007 publié in FF 2007 4893-4934 (cité: *Message du CF concernant le passeport biométrique*).

CONSEIL FÉDÉRAL, Message relatif à la modification de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure du 15 juin 2007, publié in FF 2007 4773-4872 (cité: *Message du CF relatif à la LMSI II*).

CONSEIL FÉDÉRAL, Message relatif à la Loi fédérale sur l'organisation des autorités pénales de la Confédération du 10 septembre 2008, publié in FF 2008 7371-7430, (cité: *Message du CF relatif à la LOAP*).

CONSEIL FÉDÉRAL, *Réponse à l'interpellation 08.3462 déposée par la Conseillère nationale Natalie RICKLI*, BO 2008 N 1970, disponible à l'adresse: http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20083462 (cité: *Réponse du CF à l'interpellation Natalie RICKLI*).

CONSEIL FÉDÉRAL, *Réponse à l'interpellation 08.3455 déposée par la Conseillère aux Etats Anita FETZ*, BO 2008 E 1033, disponible à l'adresse: http://www.parlament.ch/F/Suche/Pages/geschaefte.aspx?gesch_id=20083455 (cité: *Réponse du Conseil fédéral à l'interpellation FETZ*).

CONSEIL FÉDÉRAL, *Réponse à la motion 08.3732 déposée par le Conseiller national Peter MALAMA*, disponible à l'adresse: http://www.parlament.ch/F/Suche/Pages/geschaefte.aspx?gesch_id=20083732 (cité: *Réponse du Conseil fédéral à la motion MALAMA*).

CONSEIL FÉDÉRAL, *Réponse à la motion 08.3852 déposée par la Conseillère nationale LEUTENEGGER OBERHOLZER*, BO 2009 N 575 disponible à l'adresse: http://www.parlament.ch/f/suche/pages/geschaefte.aspx?gesch_id=20083852 (cité: *Réponse du CF à la motion LEUTENEGGER OBERHOLZER*).

CONSEIL FÉDÉRAL, Avant-projet de révision de la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 30 avril 2010, disponible à l'adresse: http://www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/entw-f.pdf (cité: *AP LSCPT*).

CONSEIL FÉDÉRAL, Rapport explicatif relatif à la modification de la Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 19 mai 201051, disponible à l'adresse: http://www.ejpd.admin.ch/content/dam/data/sicherheit/gesetzgebung/fernmeldeueberwachung/vn-ber-f.pdf (cité: *Rapport du CF relatif à l'AP LSCPT*).

CONSEIL FÉDÉRAL, Rapport sur le programme de consolidation 2011-2013 des finances fédérales (PCO 2011-2013) du 14 avril 2010 166, disponible à l'adresse: http://www.efd.admin.ch/dokumentation/gesetzgebung/00571/01674/index.html?lang=fr&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ae2IZn4Z2qZpnO2Yuq2Z6gpJCDeYR5hGym162epYbg2c_JjKbNoKSn6A (cité: *Rapport du CF sur le programme de consolidation 2011-2013 des finances fédérales*).

COQUOZ CHRISTIAN, *Le tribunal des mesures de contrainte, l'autorité de recours, la juridiction d'appel*, in: PFISTER-LIECHTI, RENATE (Ed.), *La procédure pénale fédérale*, pp 107-136, Berne 2010 (cité: COQUOZ, *Le tribunal des mesures de contrainte*).

COQUOZ RAPHAËL, *Profils ADN: matière d'expertise ou élément d'enquête préliminaire?*, in: Revue pénale suisse 2000, Vol. 118, pp 223-235 (cité: COQUOZ, *Profils ADN*).

COQUOZ RAPHAËL / TARONI FRANCO, *Preuve par l'ADN: la génétique au service de la justice*, 2ème éd., Lausanne 2006 (cité: COQUOZ / TARONI, *Preuve par l'ADN*).

CORBOZ BERNARD, *Les infractions en droit suisse, volume I*, Berne 2002 (cité: CORBOZ, *Les infractions en droit suisse I*).

CORBOZ BERNARD, *Les infractions en droit suisse, volume II*, Berne 2002 (cité: CORBOZ, *Les infractions en droit suisse II*).

CORNU PIERRE, *L'enquête selon la procédure pénale unifiée, Recueil de jurisprudence neuchâteloise 2008*, pp 45-80, Neuchâtel 2009 (cité: CORNU, *L'enquête selon le CPP*).

CORNU PIERRE, *Le nouveau ministère public - son fonctionnement et ses compétences*, in: PFISTER-LIECHTI, RENATE (Ed.), *La procédure pénale fédérale*, pp 51-78, Berne 2010 (cité: CORNU, *Le nouveau ministère public*).

COUSSIRAT-COUSTERE VINCENT, *Commentaire ad art. 8 § 2 CEDH*, in: PETTITI LOUIS-EDMOND / DECAUX EMMANUEL / IMBERT PIERRE-HENRI (Eds.), *La Convention européenne des droits de l'homme: commentaire article par article*, pp 323-351, Paris 1999 (cité: COUSSIRAT-COUSTERE, *art. 8 § 2 CEDH*).

CUSSON, MAURICE, *De l'action de sécurité*, in: CUSSON, MAURICE / DUPONT, BENOÎT / LEMIEUX, FRÉDÉRIC (Eds.), *Traité de sécurité intérieure*, pp 43-57, Lausanne 2008 (cité: CUSSON, *De l'action de sécurité*).

CUSSON,MAURICE, *La surveillance et la contre-surveillance*, in: CUSSON MAURICE / DUPONT BENOÎT / LEMIEUX FRÉDÉRIC (Eds.), *Traité de sécurité intérieure*, pp 429-436, Lausanne 2008 (cité: CUSSON, *La surveillance et la contre-surveillance*).

CUSSON MAURICE, *La télésurveillance*, in: CUSSON MAURICE / DUPONT, BENOÎT / LEMIEUX FRÉDÉRIC (Eds.), *Traité de sécurité intérieure*, pp 452-460, Lausanne 2008 (cité: CUSSON, *La télésurveillance*).

CUSSON MAURICE / DUPONT BENOÎT / LEMIEUX FRÉDÉRIC, *Traité de sécurité intérieure*, Collection Sciences forensiques, Lausanne 2008.

DE GRAFFENRIED PHILIPPE, *Actes de la police judiciaire*, Lausanne 1981 (cité: GRAFFENRIED, *Actes de la police judiciaire*).

DE SALVIA MICHELE, *Compendium de la CEDH: les principes directeurs de la jurisprudence relative à la Convention européenne des droits de l'homme. Jurisprudence 1960 à 2002*, Kehl, Strasbourg, Arlington 2003 (cité: DE SALVIA, *Compendium de la CEDH 1960 à 2002*).

DE SAUSSURE SOPHIE, *Le IMSI-Catcher: fonctions, applications pratiques et légalité*, 2009, disponible à l'adresse: http://jusletter.weblaw.ch/article/fr/_7875?lang=fr (cité: DE SAUSSURE, *Le IMSI-Catcher*).

DE VALKENEER CHRISTIAN / BRULIN HUGUES, *Manuel de l'enquête pénale*, Bruxelles 2005 (cité: DE VALKENEER / BRULIN, *Manuel*).

DÉLÉGATION DES COMMISSIONS DE GESTION DES CHAMBRES FÉDÉRALES (DÉLCDG), Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet «Onyx») du 10 novembre 2003 publié in FF 2004 1377-1422 (cité: *Rapport de la DélCdG du 10 novembre 2003 sur le projet Onyx*).

DÉLÉGATION DES COMMISSIONS DE GESTION DES CHAMBRES FÉDÉRALES (DÉLCDG), Légalité et efficacité du système d'exploration radio «Onyx», du 9 novembre 2007, publié in FF 2008 2293-2318 (cité: *Rapport de la DélCdG du 9 novembre 2007 sur le projet Onyx*).

DÉLÉGATION DES COMMISSIONS DE GESTION DES CHAMBRES FÉDÉRALES (DÉLCDG), Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS) du 21 juin 2010, disponible à l'adresse: http://www.parlament.ch/f/organe-mitglieder/delegationen/geschaeftspruefungsdelegation/isis-inspektion/Documents/bericht-gpdel-isis-2010-06-21-f.pdf (cité: *Rapport de la DélCdG sur le traitement des données dans le système ISIS*).

DELESSERT DANIEL A., *Les méthodes techniques de surveillance des personnes suspectes dans le procès pénal*, in: Revue pénale suisse 1975, Vol. 91, pp 182-207 (cité: DELESSERT, *Les méthodes techniques de surveillance*).

DELMAS-MARTY MIREILLE, *Le flou du droit: du code pénal aux droits de l'homme*, Paris 2004 (cité: DELMAS-MARTY, *Le flou du droit*).

DELNON VERA / RÜDY BERNHARD, *Kommentar zu Art. 186 StrGB*, in: NIGGLI MARCEL ALEXANDER / WIPRÄCHTIGER HANS (Eds.), *Strafrecht II*, pp 1071-1086, Bâle 2007 (cité: DELNON / RÜDY, *Art. 186 StrGB*).

DÉPARTEMENT FÉDÉRAL DE JUSTICE ET POLICE (DFJP), *Vidéosurveillance exercée en vue d'assurer la sécurité dans les gares, les aéroports et les autres espaces publics* 2007, disponible à l'adresse: http://www.ejpd.admin.ch/etc/medialib/data/pressemitteilung/2007/pm_2007-09-28__bericht.Par.0002.File.tmp/070926_Bericht_ Videoueberwachung_publ_f.pdf (cité: DFJP, *Rapport sur la vidéosurveillance*).

DESCHENAUX HENRI / STEINAUER PAUL-HENRI, *Personnes physiques et tutelle*, 4ème éd., Berne 2001 (cité: DESCHENAUX HENRI / STEINAUER PAUL-HENRI, *Personnes physiques et tutelle*).

DIDIER BERNARD, *Biométries*, in: OCDE (Ed.), *L'économie de la sécurité*, pp 39-60, Paris 2004 (cité: DIDIER, *Biométries*).

DIJK PIETER VAN / HOOF GODEFRIDUS J. H. VAN, *Theory and practice of the European Convention on Human Rights*, 4ème éd., Antwerpen 2006 (cité: DIJK / HOOF, *Theory and practice of the ECHR*).

DONATSCH ANDREAS / HANSJAKOB THOMAS / LIEBER VIKTOR, *Kommentar zur Schweizerischen Strafprozessordnung (StPO)*, Zurich à paraître.

DONATSCH ANDREAS / SCHWARZENEGGER CHRISTIAN / WOHLERS WOLFGANG, *Lehrbuch zum Eidgenössichen Strafprozessrecht* 2010 (à paraître).

DONATSCH ANDREAS / SCHWARZENEGGER CHRISTIAN / WOHLERS WOLFGANG, *Lehrbuch zum Eidgenössichen Strafprozessrecht* à paraître.

DONZALLAZ YVES, *Loi sur le Tribunal féréral, commentaire*, Berne 2008 (cité: DONZALLAZ, *Commentaire LTF*).

DOUTREMEPUICH CHRISTIAN, *Les fichiers des empreintes génétiques en pratique judiciaire*, INSTITUT NATIONAL DES HAUTES ÉTUDES DE SÉCURITÉ (INHES) (Ed.), La Sécurité aujourd'hui, Paris 2007 (cité: DOUTREMEPUICH, *Les fichiers des empreintes génétiques*).

DRZEMCZEWSKI ANDREW, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance tel que le garantit l'article 8 de la Convention européenne des Droits de l'Homme*, Dossiers sur les droits de l'homme no 7, Strasbourg 1995 (cité: DRZEMCZEWSKI, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance*).

DUBUIS NICOLAS, *Note sur les mesures de surveillance optique par caméra en procédure pénale*, in: Revue valaisanne de jurisprudence (RVJ) 2009, pp 207-212 (cité: DUBUIS, NICOLAS, *Note sur les mesures de surveillance optique par caméra*).

DUFOUR ARNAUD / GHERNAOUTI-HÉLIE SOLANGE, *Internet*, 10ème éd., Que sais-je?, Paris 2006 (cité: DUFOUR / GHERNAOUTI-HÉLIE, *Internet*).

DUNAND JEAN-PHILIPPE / MAHON PASCAL, *« Le droit décloisonné », interférences et interdépendances entre droit privé et droit public*, Enseignement de 3ème cycle de droit 2008, Genève; Zurich; Bâle 2009 (cité: DUNAND / MAHON, *Le droit décloisonné*).

DUPUIS MICHEL / GELLER BERNARD, *et al.*, *Code pénal I: partie générale, art. 1-110 et DPMin*, Bâle 2008 (cité: DUPUIS / GELLER, *et al.*, *Petit commentaire CP I*).

DUTERTRE GILLES, *Extraits clés de jurisprudence, Cour européenne des droits de l'homme*, Strasbourg 2003 (cité: DUTERTRE, *Extraits clés de jurisprudence*).

EGLI PATRICIA, *Drittwirkung von Grundrechten: zugleich ein Beitrag zur Dogmatik der grundrechtlichen Schutzpflichten im Schweizer Recht*, Zurich; Bâle; Genève 2002 (cité: EGLI, *Drittwirkung von Grundrechten*).

EHRENZELLER BERNHARD, *Die subsidiäre Verfassungsbeschwerde*, in: Revue de l'avocat 2007 (3), pp 103-109 (cité: EHRENZELLER, *Die subsidiäre Verfassungsbeschwerde*).

EHRENZELLER BERNHARD / MASTRONARDI PHILIPPE / SCHWEIZER RAINER J. / VALLENDER KLAUS A., *Die schweizerische Bundesverfassung Kommentar*, Zurich 2008 (cité: EHRENZELLER, *Bundesverfassung*).

EICHENBERGER ISABELLE, *La Suisse n'échappera pas aux scanners corporels*, www.swissinfo.ch, 2010, disponible à l'adresse: http://www.swissinfo.ch/fre/politique_suisse/La_Suisse_n_echappera_pas_aux_scanners_corporels.html?cid=8018940&rss=true (cité: EICHENBERGER, *La Suisse n'échappera pas aux scanners corporels*).

EISENBERG ULRICH, *Beweisrecht der StPO Spezialkommentar*, 6ème éd., Munich 2008 (cité: EISENBERG, *Beweisrecht der StPO*).

ENGELHARD MARC / BÄNZIGER MARTIN, *Kreuzlinger Schläger-Trio: Polizei verfolgt heisse Spur*, in: Thurgauer Zeitung du 29 mai 2009, disponible à l'adresse: http://www.thurgauerzeitung.ch/thurgau/kreuzlingen/Kreuzlinger-SchlaegerTrio-Polizei-verfolgt-heisse-Spur/story/3012536 (cité: ENGELHARD / BÄNZIGER, *Kreuzlinger Schläger-Trio*).

EPINEY ASTRID / FEIERMUTH MARIANNE, *Datenschutz in der Schweiz und in Europa = La protection des données en Suisse et en Europe*, Colloque "Datenschutz in der Schweiz und in Europa" Fribourg 1999 (cité: EPINEY / FEIERMUTH, *La protection des données*).

ETZIONI AMITAÏ, *Big Brother ou Big Benefits? Identification biométrique et encartement*, in: WUILLEUMIER ANNE / ETZIONI AMITAI (Eds.), *Police et identification: enjeux, pratiques, techniques*, pp 9-59, Paris 2005 (cité: ETZIONI, *Big Brother*).

EYMANN STEPHANIE, *Die strafprozessuale Kontosperre*, Bâle 2009 (cité: EYMANN, *Die strafprozessuale Kontosperre*).

FANTI SÉBASTIEN, *Alc@tr@z numérique*, Vevey 2009 (cité: FANTI, *Alcatraz numérique*).

FASSBIND OLIVIER, *Les incidences de la Convention européenne des droits de l'homme sur les lois suisses de procédure pénale*, s. l. 1984 (cité: FASSBIND, *Les incidences de la CEDH*).

FAVRE ERIC / DIRECTION GENEVOISE DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION (DSIC), *Quid de la vidéosurveillance en Ville de Genève ? Rapport à l'attention du Conseil administratif*, Ville de Genève, Genève 2008 (cité: FAVRE / DSIC, *Rapport à l'attention du Conseil administratif*).

FICKERT SEBASTIAN, *Die Behandlung von Zufallserkenntnissen im Ermittlungsverfahren: unter Berücksichtigung der allgemeinen Grundsätze über Verwertungsverbote*, Frankfurt am Main ; Berne etc. 2002 (cité: FICKERT, *Die Behandlung von Zufallserkenntnissen*).

FINKENZELLER KLAUS, *RFID-Handbuch*, 4ème éd., Munich 2006 (cité: FINKENZELLER, *RFID-Handbuch*).

FLEXILIS, *RFID e-Passport Vulnerability*, www.flexilis.com, 2006, disponible à l'adresse: http://www.flexilis.com/epassport.php (cité: FLEXILIS, *RFID e-Passport Vulnerability*).

FLÜCKIGER ALEXANDRE, *La preuve juridique à l'épreuve du principe de précaution*, in: Revue européenne des sciences sociales 2003, Vol. 41 (128), pp 107-127 (cité: FLÜCKIGER, *La preuve juridique à l'épreuve du principe de précaution*).

FLÜCKIGER ALEXANDRE, *Le conflit entre le principe de transparence et la protection de la sphère privée*, in: Medialex 2003 (4), pp 225-233 (cité: FLÜCKIGER, *Le conflit entre le principe de transparence et la protection de la sphère privée*).

FLÜCKIGER, ALEXANDRE, *Droits fondamentaux et vidéosurveillance par les particuliers et les autorités des espaces ouverts au public* in: SCHWARZENEGGER, CHRISTIAN / NÄGELI, ROLF (Eds.), *Drittes Zürcher Präventionsforum: Videoüberwachung als Prävention?* à paraître (cité: FLÜCKIGER, *Droits fondamentaux et vidéosurveillance*).

FLÜCKIGER ALEXANDRE, *Droits fondamentaux et vidéosurveillance par les particuliers et les autorités des espaces ouverts au public* in: SCHWARZENEGGER CHRISTIAN / NÄGELI ROLF (Eds.), *Drittes Zürcher Präventionsforum: Videoüberwachung als Prävention?* à paraître (cité: FLÜCKIGER, *Droits fondamentaux et vidéosurveillance*).

FLÜCKIGER ALEXANDRE / AUER ANDREAS, *La vidéosurveillance dans l'œil de la constitution*, in: AJP/PJA 2006 (8), pp 924-942 (cité: FLÜCKIGER / AUER, *La vidéosurveillance dans l'œil de la constitution*).

FORNITO ROBERTO, *Beweisverbote im schweizerischen Strafprozess*, St-Gall 2000 (cité: FORNITO, *Beweisverbote im schweizerischen Strafprozess*).

FORTIER FRANÇOIS, *Citoyens sous surveillance: la face cachée d'Internet*, Montréal 2002 (cité: FORTIER, *Citoyens sous surveillance*).

GAILLARD LOUIS, *Le sort des preuves illicites dans le procès civil*, in: La Semaine Judiciaire 1998, Vol. II (37), pp 649-670 (cité: GAILLARD, *Le sort des preuves illicites dans le procès civil*).

GANI CYNTHIA, *«Sans cadre légal, 120 caméras surveillent déjà la ville de Genève»*, in: Le Temps du 1er mars 2008, (cité: GANI, *Sans cadre légal, 120 caméras surveillent déjà la ville de Genève*).

GARBADE JEAN-PIERRE, *Vos droits face à la police et au juge d'instruction*, Lausanne 1995 (cité: GARBADE, *Vos droits*).

GARSTKA HANS-JÜRGEN, *Der "nackte" Automobilist im Visier?*, in: digma 2007 (3), pp 90-93 (cité: GARSTKA, *Der "nackte" Automobilist*).

GAUTHIER JEAN, *Enregistrement clandestin d'une conversation téléphonique et preuve pénale*, in: HAUSER ROBERT / REHBERG JÖRG / STRATENWERTH GÜNTER (Eds.), *Gedächtnisschrift für Peter Noll*, pp 333-340, Zurich 1984 (cité: GAUTHIER, *Enregistrement clandestin*).

GAUTHIER JEAN, *Les résultats de l'audio-surveillance comme preuve pénale en droit suisse, Rapports suisses présentés au XIIème Congrès international de droit comparé*, pp 75-91, Zurich 1987 (cité: GAUTHIER, *Les résultats de l'audio-surveillance*).

GEIGER, ANDREAS, *Verfassungsfragen zur polizeilichen Anwendung der Video-Überwachungstechnologie bei der Straftatbekämpfung*, Berlin 1994 (cité: GEIGER, *Verfassungsfragen zur polizeilichen Video-Überwachung*).

GEORGEL JACQUES, *Les libertés de communication: contrôle d'identité, écoute téléphonique, vidéosurveillance*, Paris 1996 (cité: GEORGEL, *Les libertés de communication*).

GHERNAOUTI-HÉLIE SOLANGE, *La cybercriminalité: le visible et l'invisible*, Lausanne 2009 (cité: GHERNAOUTI-HÉLIE, *La cybercriminalité*).

GIGON ARIANE, *Le fichage risqué de hooligans sur Internet*, www.swissinfo.ch, 2009, disponible à l'adresse: http://www.swissinfo.ch/fre/politique_suisse/Le_fichage_risque_de_hooligans_sur_Internet.html?cid=7175412 (cité: GIGON, *Le fichage risqué de hooligans sur Internet*).

GILL MARTIN / SPRIGGS ANGELA, *Assessing the impact of CCTV*, Home Office Research, Development and Statistics Directorate n° 292, Londres 2005, disponible à l'adresse: http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf (cité: GILL / SPRIGGS, *Assessing the impact of CCTV*).

GILLARD NICOLAS, *La nouvelle loi fédérale sur la protection des données: travaux de la Journée d'étude organisée par le Centre du droit de l'entreprise le 6 octobre 1993 à l'Université de Lausanne*, Lausanne 1994 (cité: GILLARD, *La nouvelle loi fédérale sur la protection des données*).

GISLER FRÉDÉRIC, *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 (cité: GISLER, *La coopération policière*).

GOLDSCHMID PETER, *Der Einsatz technischer Überwachungsgeräte im Strafprozess: unter besonderer Berücksichtigung der Regelung im Strafverfahren des Kantons Bern*, Berne 2001 (cité: GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess*).

GOLDSCHMID PETER, *Geheime Überwachungsmassnahmen im Entwurf zu einer eidgenössischen Strafprozessordnung*, in: CIMICHELLA, SANDRO / KUHN ANDRÉ / NIGGLI MARCEL ALEXANDER (Eds.), *Neue Technologie und Kriminalität: neue Kriminologie ?*, pp 157-172, Zurich 2006 (cité: GOLDSCHMID, *Geheime Überwachungsmassnahmen*).

GOLDSCHMID PETER / MAURER THOMAS / SOLLBERGER JÜRG, *Kommentierte Textausgabe zur schweizerischen Strafprozessordnung*, Berne 2008 (cité: GOLDSCHMID / MAURER / SOLLBERGER, *Kommentierte Textausgabe zur StPO*).

GRAVEN JEAN *L'emploi du magnétophone dans la procédure pénale*, in: Revue pénale suisse 1958, Vol. 73 (4), pp 361-381 (cité: GRAVEN, *L'emploi du magnétophone*).

GRAVEN PHILIPPE, *Le cautionnement préventif: (l'article 57 du code pénal suisse): étude de législation comparée*, Bâle 1963 (cité: GRAVEN, *Le cautionnement préventif*).

GRIMM THOMAS, *"Pay as you drive" - die Technik*, in: digma 2007 (3), pp 94-97 (cité: GRIMM, *Pay as you drive*).

GRISEL ETIENNE / NEUENSCHWANDER, ANOUK, *Droits fondamentaux, libertés idéales*, Berne 2008 (cité: GRISEL / NEUENSCHWANDER, *Droits fondamentaux*).

GROUPE DE TRAVAIL «ARTICLE 29», *Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT)*, Bruxelles 2006, disponible à l'adresse: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_fr.pdf (cité: GROUPE 29, *Avis 10/2006 (SWIFT)*).

GUÉNIAT OLIVIER / HAINARD FRÉDÉRIC, *Commentaire ad art. 282-283 CPP*, in: KUHN ANDRÉ / JEANNERET YVAN (Eds.), *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: GUÉNIAT / HAINARD, *Art. 282-283 CPP*).

GUERRIER CLAUDINE, *Les écoutes téléphoniques*, Paris 2000 (cité: GUERRIER, *Les écoutes téléphoniques*).

GUERRIER CLAUDINE / MONGET MARIE-CHRISTINE, *Droit et sécurité des télécommunications*, Paris 2000 (cité: GUERRIER / MONGET, *Droit et sécurité des télécommunications*).

GUILLEMIN CHRISTOPHE, *Le photocopieur, gardien des grands et petits secrets des entreprises*, in: ZDNet France 2003, disponible à l'adresse: http://www.zdnet.fr/entreprise/service-informatique/poste-client/0,50007192,39133986,00.htm (cité: GUILLEMIN, *Le photocopieur*).

HÄFELIN ULRICH / HALLER WALTER / KELLER HELEN, *Schweizerisches Bundesstaatsrecht*, 7ème éd., Zurich 2008 (cité: HÄFELIN / HALLER / KELLER, *Schweizerisches Bundesstaatsrecht*).

HALLER WALTER, *The Swiss Constitution in a comparative context*, Zurich 2009 (cité: HALLER, *The Swiss Constitution*).

HALLER WALTER, *La liberté personnelle*, in: AUBERT JEAN-FRANÇOIS / EICHENBERGER KURT / BOIS PHILIPPE / KOLLER HEINRICH (Eds.), *Commentaire de la Constitution fédérale de la Confédération suisse du 29 mai 1874*, Bâle, Zurich 1987 (cité: HALLER, *La liberté personnelle*).

HANSJAKOB THOMAS, *Die ersten Erfahrungen mit dem Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)*, in: Revue pénale suisse 2002, Vol. 120 (3), pp 265-283 (cité: HANSJAKOB, *Die ersten Erfahrungen mit dem BÜPF*).

HANSJAKOB, THOMAS, *Das neue Bundesgesetz über die verdeckte Ermittlung*, in: Revue pénale suisse 2004, Vol. 122 (2), pp 97-114 (cité: HANSJAKOB, *Das neue BVE*).

HANSJAKOB THOMAS, *BÜPF/VÜPF: Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*, 2ème éd., St. Gallen 2006 (cité: HANSJAKOB, *BÜPF und VÜPF Kommentar*).

HANSJAKOB THOMAS, *Bemerkungen zur BGE 133 IV 329 (6B_170/2007)*, in: Forum poenale 2008 (4), pp 212-215 (cité: HANSJAKOB, *Bemerkungen zur BGE 133 IV 329*).

HANSJAKOB THOMAS, *Verdeckte Ermittlung - Gesetz und Rechtsprechung*, in: Forum poenale 2008 (6), pp 361-366 (cité: HANSJAKOB, *Verdeckte Ermittlung*).

HANSJAKOB THOMAS, *Zwangsmassnahmen in der neuen Eidg. StPO*, in: Revue pénale suisse 2008, Vol. 126 (1), pp 90-114 (cité: HANSJAKOB, *Zwangsmassnahmen in der neuen Eidg. StPO*).

HÄRING DANIEL, *Verwertbarkeit rechtswidrig erlangter Beweise gemäss Schweizerischer Strafprozessordnung – alte Zöpfe oder substanzielle Neuerungen?*, in: Revue pénale suisse 2009, Vol. 127 (3), pp 225-257 (cité: HÄRING, *Verwertbarkeit rechtswidrig erlangter Beweise*).

HARKIN JAMES, *"Big Brother" may be over but we still love watching ourselves*, in: The Independent du 28 août 2009, disponible à l'adresse: http://www.independent.co.uk/opinion/commentators/james-harkin-big-brother-may-be-over-but-we-still-love-watching-ourselves-1778284.html (cité: HARKIN, *"Big Brother" may be over but we still love watching ourselves*).

HAUSER ROBERT / SCHWERI ERHARD / HARTMANN KARL, *Schweizerisches Strafprozessrecht*, 6ème éd., Bâle 2005 (cité: HAUSER / SCHWERI / HARTMANN, *Schweizerisches Strafprozessrecht*).

HAUSHEER HEINZ, *Die Genanalyse zu Identifizierungszwecken im Straf-, Zivil- und Verwaltungsrecht*, in: Zeitschrift für schweizerisches Recht 1998, Vol. 117 (5), pp 449-472 (cité: HAUSHEER, *Die Genanalyse*).

HEILMANN ÉRIC, *La vidéosurveillance, une réponse efficace à la criminalité ?*, in: Criminologie 2003, Vol. 36 (1), pp 89-102, disponible à l'adresse: http://www.erudit.org/revue/crimino/2003/v36/n1/006554ar.pdf
(cité: HEILMANN, *La vidéosurveillance, une réponse efficace à la criminalité*).

HODGES STEVE / MCFARLANE DUNCAN, *RFID: le concept et l'incidence* in: OCDE (Ed.), *L'économie de la sécurité*, pp 61-86, Paris 2004 (cité: HODGES / MCFARLANE, *RFID*).

HOTTELIER MICHEL, *Les droits de l'homme et la procédure pénale en Suisse*, in: Revue suisse de droit international et européen 2007, Vol. 17 (3), pp 493-506 (cité: HOTTELIER, *Les droits de l'homme et la procédure pénale en Suisse*).

HOTTELIER MICHEL / MOCK HANSPETER / PUECHAVY MICHEL, *La Suisse devant la Cour européenne des droits de l'homme*, Bruxelles 2005 (cité: HOTTELIER / MOCK / PUECHAVY, *La Suisse devant la CEDH*).

HÜPPI DAVID, *Zufallsfunde aus genehmigten Telephonüberwachungen: ihre Verwertbarkeit als Beweismittel gemäss Art. 104d Abs. 3 der Strafprozessordnung des Kantons Zürich und de lege ferenda*, in: Schweizerische Juristen-Zeitung 1990 (23), pp 394-399 (cité: HÜPPI, *Zufallsfunde aus genehmigten Telephonüberwachungen*).

HURTADO POZO JOSÉ, *Droit pénal / Partie générale*, 3ème éd., Genève 2008 (cité: HURTADO POZO, *Partie générale*).

HYDE MARINA, *This surveillance onslaught is draconian and creepy*, in: The Guardian du 28 juin 2008, disponible à l'adresse: http://www.guardian.co.uk/commentisfree/2008/jun/28/civilliberties.privacy (cité: HYDE, *This surveillance onslaught is draconian and creepy*).

INSTITUT DE RADIOPROTECTION ET SÛRETÉ NUCLÉAIRE (IRSN), *Evaluation du risque sanitaire des scanners corporels à rayons X «backscatter»*, Fontenay-aux-Roses 2010, disponible à l'adresse: http://www.irsn.fr/FR/Actualites_presse/Communiques_et_dossiers_de_presse/Documents/IRSN_Rapport_Evaluation_Scanner_backscatter_201002.pdf (cité: IRSN, *Evaluation du risque sanitaire des scanners corporels*).

IQBAL YASMIN, *Zugriff auf elektronische Post*, in: Revue de l'avocat 2004 (1), pp 7-13 (cité: IQBAL, *Zugriff auf elektronische Post*).

JACOBS FRANCIS GEOFFREY / OVEY CLARE / WHITE ROBIN C. A., *Jacobs and White, the European Convention on human rights*, 4ème éd., Oxford 2006 (cité: JACOBS / OVEY / WHITE, *Jacobs and White, the ECHR*).

JACQUARD NICOLAS, *Quand espionner les téléphones portables devient un jeu d'enfant*, in: Le Parisien du 8 mars 2010, disponible à l'adresse: http://www.leparisien.fr/ faits-divers/quand-espionner-les-telephones-portables-devient-un-jeu-d-enfant-08-03-2010-839610.php (cité: JACQUARD, *Quand espionner les téléphones portables devient un jeu d'enfant*).

JACQUARD NICOLAS, *Quatre questions sur un «mouchard»*, in: Le Parisien du 8 mars 2010, disponible à l'adresse: http://www.leparisien.fr/faits-divers/quatre-questions-sur-un-mouchard-08-03-2010-839602.php (cité: JACQUARD, *Quatre questions sur un «mouchard»*).

JEAN-RICHARD-DIT-BRESSEL MARC THÉODORE, *Ist ein Millionendiebstahl ein Bagatelldelikt: Fragen zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000*, in: Revue pénale suisse 2001 (119), pp 40-70 (cité: JEAN-RICHARD-DIT-BRESSEL, *Ist ein Millionendiebstahl ein Bagatelldelikt*).

JEANNERET YVAN, *Le recours en matière pénale*, Journée de formation continue pour les avocats, notaires, magistrats et juristes de l'administration: la nouvelle loi sur le Tribunal fédéral et questions choisies de droit privé, Neuchâtel 2006 (cité: JEANNERET, *Le recours en matière pénale*).

JENDLY MANON, *La coexistence des secrets en exécution de peine privative de liberté: vers un modèle de partage des informations confidentielles en milieu carcéral*, Neuchâtel 2005,(cité: JENDLY, *La coexistence des secrets*).

JOBARD FABIEN / SCHULZE-ICKING NIKLAS, *Preuves hybrides, L'administration de la preuve pénale sous l'influence des techniques et des technologies (France, Allemagne, Grande-Bretagne)*, Guyancourt 2004, disponible à l'adresse: http://www.cesdip.org/IMG/pdf/ EDP_no_96.pdf (cité: JOBARD / SCHULZE-ICKING, *Preuves hybrides*).

JOHNER STEPHAN / VIREDAZ BAPTISTE, *Commentaire ad art. 198-200 CPP*, in: KUHN ANDRÉ / JEANNERET YVAN (Eds.), *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: JOHNER / VIREDAZ, *Art. 198-200 CPP*).

JOSET PIERRE / RUCKSTUHL NIKLAUS, *V-Mann-Problematik aus der Sicht der Verteidigung*, in: Revue pénale suisse 1993, Vol. 111, pp 355-374 (cité: JOSET / RUCKSTUHL, *V-Mann-Problematik*).

JOSITSCH DANIEL, *Grundriss des schweizerischen Strafprozessrechts*, Zurich 2009 (cité: JOSITSCH, *Grundriss des schweizerischen Strafprozessrechts*).

KÄLIN WALTER / MALINVERNI GIORGIO / NOWAK MANFRED, *Die Schweiz und die UNO-Menschenrechtspakte = La Suisse et les Pactes des Nations Unies relatifs aux droits de l'homme*, 2ème éd., Bâle, Francfort-sur-le-Main, Bruxelles 1997 (cité: KÄLIN / MALINVERNI / NOWAK, *La Suisse et les Pactes des Nations Unies*).

KAUFMANN MARTIN, *Beweisführung und Beweiswürdigung: Tatsachenfeststellung im schweizerischen Zivil-, Straf- und Verwaltungsprozess*, Zurich 2009 (cité: KAUFMANN, *Beweisführung und Beweiswürdigung*).

KELLER ANDREAS, *Die politische Polizei im Rahmen des schweizerischen Staatsschutzes: dargestellt am Beispiel des Kantons Basel-Stadt*, Bâle ; Frankfurt am Main 1996 (cité: KELLER, *Die politische Polizei*).

KELLER HELEN, *Grundrechtliche Schranken von geheimen Überwachungsmassnahmen*, in: SCHMID NIKLAUS / ACKERMAN JÜRG-BEAT (Ed.), *Strafrecht als Herausforderung: Analysen und Perspektiven von Assistierenden des Rechtswissenschaftlichen Instituts der Universität Zürich: zur Emeritierung von Professor Niklaus Schmid / Jürg-Beat Ackermann*, pp 405-422, Zurich 1999 (cité: KELLER, *Grundrechtliche Schranken*).

KERN FRANÇOIS, *Les écoutes au regard du droit répressif français et de la Convention européenne des droits de l'homme*, Thèse de doctorat, Paris 1992 (cité: KERN, *Les écoutes au regard du droit répressif français et de la CEDH*).

KIENER REGINA / KÄLIN WALTER, *Grundrechte*, Berne 2007 (cité: KIENER / KÄLIN, *Grundrechte*).

KILLIAS MARTIN / KUHN ANDRÉ / DONGOIS NATHALIE / AEBI MARCELO F., *Précis de droit pénal général*, 3ème éd., Précis de droit Stämpfli, Berne 2008 (cité: KILLIAS / KUHN / DONGOIS / AEBI, *Précis de droit pénal général*).

KLAUSER FRANCISCO, *Die Videoüberwachung öffentlicher Räume, Zur Ambivalenz eines Instruments sozialer Kontrolle*, Frankfurt am Main 2006 (cité: KLAUSER, *Die Videoüberwachung öffentlicher Räume*).

KLEY ANDREAS / TOPHINKE ESTHER, *Kommentar zu Art. 16 BV*, in: EHRENZELLER BERNHARD / MASTRONARDI PHILIPPE / SCHWEIZER RAINER J. / VALLENDER KLAUS A. (Eds.), *Die schweizerische Bundesverfassung Kommentar*, pp 366-384, Zurich 2008 (cité: KLEY / TOPHINKE, *Art. 16 BV*).

KÖNIG ROBERT, *Videoüberwachung; Fakten, Rechtslage und Ethik*, Wien 2001 (cité: KÖNIG, *Videoüberwachung*).

KORNMAN MAUDE, *Les fichiers de police: au cœur de la dérive policière*, www.droit-tic.com, 2004, disponible à l'adresse: http://www.droit-tic.com/pdf/fichier_police.pdf (cité: KORNMAN, *Les fichiers de police*).

KREIS GEORG, *Staatsschutz im Laufe der Zeit*, in: digma 2009 (2), pp 54-59 (cité: GEORG, *Staatsschutz im Laufe der Zeit*).

KREIS GEORG / DELLEY JEAN-DANIEL / KAUFMANN OTTO KONSTANTIN / WIGGER OTMAR, *La protection politique de l'Etat en Suisse: l'évolution de 1935 à 1990; étude pluridisciplinaire effectuée et éditée sur mandat du Conseil fédéral*, Berne, Stuttgart, etc. 1993 (cité: KREIS / DELLEY / KAUFMANN / WIGGER, *La protection politique de l'Etat en Suisse*).

KREMPL STEFAN, 25C3: Serious security vulnerabilities in DECT wireless telephony, in: The H Security, disponible à l'adresse: http://www.h-online.com/security/25C3-Serious-security-vulnerabilities-in-DECT-wireless-telephony--/news/112326.

KUHN ANDRÉ, *Sanctions pénales: est-ce bien la peine ? et dans quelle mesure ?*, Grolley 2005 (cité: KUHN, *Sanctions pénales*).

KUHN ANDRÉ, *Procédure pénale unifiée: reformatio in pejus aut in melius?*, Charmey 2008 (cité: KUHN, *Procédure pénale unifiée*).

KUHN ANDRÉ, *La procédure pénale suisse selon le futur CPP unifié*, in: Revue de droit suisse 2009, Vol. 128 (1), pp 125-184 (cité: KUHN, *La procédure pénale suisse selon le futur CPP unifié*).

KUHN ANDRÉ, *La procédure pénale fédérale: choix du modèle et droit transitoire*, in: PFISTER-LIECHTI RENATE (Ed.), *La procédure pénale fédérale*, pp 11-50, Berne 2010 (cité: KUHN, *Choix du modèle et droit transitoire*).

KUHN ANDRÉ, *Sommes-nous tous des criminels?*, 3ème éd., Grolley 2010 (cité: KUHN, *Sommes-nous tous des criminels*).

KUHN ANDRÉ / JEANNERET YVAN, *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: KUHN / JEANNERET, *CR-CPP*).

KUHN ANDRÉ / PERRIER CAMILLE , *Quelques points problématiques du Code de procédure pénale suisse*, 2008, disponible à l'adresse: http://jusletter.weblaw.ch/article/fr/_6769?lang=fr (cité: KUHN / PERRIER, *Quelques points problématiques du CPP*).

KÜNZLI BEAT, *Praktische Probleme bei der Umsetzung des Bundesgesetzes betreffend die Überwachung des Post- und Fernemeldeverkehrs*, in: CASSANI U. / DITTMANN V. / MAAG R. / STEINER S. (Eds.), *Mehr Sicherheit – weniger Freiheit? Ermittlungs- und Beweistechniken hinterfragt = Plus de sécurité – moins de liberté? Les techniques d'investigation et de preuve en question*, pp 95-216, Zurich; Coire 2003 (cité: KÜNZLI, *Praktische Probleme bei der Umsetzung des BÜPF*).

LECHNER STEPHAN, *RFID: Sicherheitsprobleme und -lösungen*, in: digma 2005 (4), pp 172-175 (cité: LECHNER, *RFID*).

LEGLER THOMAS, *Vie privée, image volée: la protection pénale de la personnalité contre les prises de vues*, Berne 1997 (cité: LEGLER, *Vie privée, image volée*).

LEMAN-LANGLOIS STÉPHANE / LEMIEUX FRÉDÉRIC, *Renseignement de sécurité et renseignement criminel*, in: CUSSON MAURICE / DUPONT BENOÎT / LEMIEUX FRÉDÉRIC (Eds.), *Traité de sécurité intérieure*, pp 335-352, Lausanne 2008 (cité: LEMAN-LANGLOIS / LEMIEUX, *Renseignement de sécurité et renseignement criminel*).

LEMIEUX FRÉDÉRIC, *Vers un renseignement criminel de qualité*, in: CUSSON, MAURICE / DUPONT, BENOÎT / LEMIEUX, FRÉDÉRIC (Eds.), *Traité de sécurité intérieure*, pp 291-299, Lausanne 2008 (cité: LEMIEUX, *Vers un renseignement criminel de qualité*).

LHUILLIE JEAN-BAPTISTE, *«Attention, cet appel pourra être enregistré.» De la loyauté de la preuve*, Droit du procès et de la preuve judiciaire, 2009, disponible à l'adresse: http://m2bde.u-paris10.fr/blogs/dpj/index.php/post/2009/06/08/%C2%AB-Attention%2C-cet-appel-pourra-%C3%AAtre-enregistr%C3%A9.-%C2%BB-De-la-loyaut%C3%A9-de-la-preuve-%E2%80%93-par-Jean-Baptiste-Lhuillier (cité: LHUILLIE, *De la loyauté de la preuve*).

LÜTZNER AXEL, *Strafprozessuale Zwangs- und Überwachungsmassnahmen im Recht der USA und der Bundesrepublik Deutschland*, Leipzig 1999 (cité: LÜTZNER, *Strafprozessuale Zwangs- und Überwachungsmassnahmen*).

LYON DAVID, *Les technologies de la surveillance: tendances et répercussions sociales*, in: OCDE (Ed.), *L'économie de la sécurité*, pp 141-166, Paris 2004 (cité: LYON, *Les technologies de la surveillance*).

MAHON PASCAL, *Un «droit à l'oubli»?*, *Le temps et le droit*, pp 195-221, Bâle 2008 (cité: MAHON, *Un «droit à l'oubli»?*).

MAISL HERBERT, *Communications mobiles, secret des correspondances et protection des données personnelles*, in: Droit de l'informatique et des télécoms 1995 (2), pp 13-20 (cité: MAISL, *Communications mobiles*).

MALINGRE VIRGINIE, *Caméras de surveillance: tous voyeurs, tous délateurs*, in: Le Monde du 10 octobre 2009, disponible à l'adresse: http://www.lemonde.fr/europe/article/2009/10/10/cameras-de-surveillance-tous-voyeurs-tous-delateurs_1252130_3214.html (cité: MALINGRE, *Caméras de surveillance*).

MALLIÉ EDDIE, *La vidéosurveillance: réglementation et pratique*, Dossier d'experts, Voiron 2000 (cité: MALLIÉ, *La vidéosurveillance*).

MASTRONARDI PHILIPPE, *Kommentar zu Art. 7 BV*, in: EHRENZELLER BERNHARD / MASTRONARDI PHILIPPE / SCHWEIZER RAINER J. / VALLENDER KLAUS A. (Eds.), *Die schweizerische Bundesverfassung Kommentar*, pp 164-178, Zurich 2008 (cité: MASTRONARDI, *Art. 7 BV*).

MATHIEU BERTRAND, *Génome humain et droits fondamentaux*, Paris 2000 (cité: MATHIEU, *Génome humain et droits fondamentaux*).

MATT PETRA JULIA, *Die Überwachung des Fernmeldeverkehrs im liechtensteinischen Strafverfahren*, Zurich 1990.

MAURER-LAMBROU URS / KUNZ SIMON, *Kommentar zu Art. 2 DSG*, in: MAURER-LAMBROU URS / VOGT NEDIM PETER (Eds.), *Basler Kommentar zur Datenschutzgesetz*, pp 43-61, Bâle 2008 (cité: MAURER-LAMBROU / KUNZ, *Art. 2 DSG*).

MAURER-LAMBROU URS / VOGT NEDIM PETER, *Basler Kommentar zur Datenschutzgesetz*, Bâle 2008 (cité: MAURER-LAMBROU / VOGT, *Basler Kommentar DSG*).

MEIER-HAYOZ ARTHUR / FORSTMOSER PETER, *Schweizerisches Gesellschaftsrecht*, 10ème éd., Berne 2007 (cité: MEIER-HAYOZ / FORSTMOSER, *Schweizerisches Gesellschaftsrecht*).

MEIER PHILIPPE / STAEGER ALEXANDRE , *La surveillance des assurés (assurances sociales et assurances privées), état des lieux*, 2009, disponible à l'adresse: http://jusletter.weblaw.ch/article/fr/_7970?lang=fr (cité: MEIER / STAEGER, *La surveillance des assurés*).

MEIER VERENA, *Forensische DNA-Analysen – Wo liegen die technischen Grenzen?*, in: CASSANI U. / DITTMANN V. / MAAG R. / STEINER S. (Eds.), *Mehr Sicherheit – weniger Freiheit? Ermittlungs- und Beweistechniken hinterfragt = Plus de sécurité – moins de liberté? Les techniques d'investigation et de preuve en question*, pp 257-272, Zurich; Coire 2003 (cité: MEIER, *Forensische DNA-Analysen*).

MÉTILLE SYLVAIN, *L'utilisation privée de moyens techniques de surveillance et la procédure pénale*, in: DUNAND JEAN-PHILIPPE / MAHON PASCAL (Eds.), *«Le droit décloisonné», interférences et interdépendances entre droit privé et droit public, Enseignements de 3ème cycle de droit*, pp 179-198, Genève; Zurich; Bâle 2009 (cité: MÉTILLE, *L'utilisation privée de moyens techniques de surveillance*).

MÉTILLE SYLVAIN, *Les mesures techniques de surveillance: des risques évités et des risques créés*, in: MEIER PHILIPPE / PAPAUX ALAIN (Eds.), *Risque(s) et droit, Enseignements de 3ème cycle de droit*, Genève; Zurich; Bâle à paraître (cité: MÉTILLE, *Des risques évités et des risques créés*).

METZGER, HUBERT ANDREAS, *Der strafrechtliche Schutz des persönlichen Geheimbereichs gegen Verletzungen durch Ton- und Bildaufnahme- sowie Abhörgeräte*, Winterthur 1972, disponible à l'adresse: http://www.stub.unibe.ch/html/haupt/datenbanken/diss/bestell.html (cité: METZGER, *Der strafrechtliche Schutz des persönlichen Geheimbereich*).

MEUWLY DIDIER, *L'Ordonnance sur le service de surveillance de la correspondance postale et des télécommunications: une loi en retard d'une guerre technologique?*, in: COTTIER BERTIL (Ed.), *Le droit des télécommunications en mutation*, pp 105-119, Fribourg 2001 (cité: MEUWLY, *L'Ordonnance sur le service de surveillance de la correspondance postale et des télécommunications*).

MEUWLY DIDIER, *Reconnaissance de locuteurs en sciences forensiques: l'apport d'une approche automatique*, Lausanne 2001 (cité: MEUWLY, *Reconnaissance de locuteurs*).

MEUWLY DIDIER, *Le mythe de "l'empreinte vocale" (I)*, in: Revue internationale de criminologie et de police technique et scientifique 2003, Vol. 56 (2), pp 219-236 (cité: MEUWLY, *Le mythe de "l'empreinte vocale" (I)*).

MEUWLY DIDIER, *Le mythe de "l'empreinte vocale" (II)*, in: Revue internationale de criminologie et de police technique et scientifique 2003, Vol. 56 (3), pp 361-374 (cité: MEUWLY, *Le mythe de "l'empreinte vocale" (II)*).

MEYER-LADEWIG JENS, *EMRK Konvention zum Schutz der Menschenrechte und Grundfreiheiten Handkommentar*, 2ème éd., Baden-Baden 2006 (cité: MEYER-LADEWIG, *EMRK Handkommentar*).

MOCK HANSPETER, *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 237-246 (cité: MOCK, *Le droit au respect de la vie privée et familiale, du domicile et de la correspondance*).

MÖHLENBECK MICHAELA, *Das absolute Folterverbot: Seine Grundlagen und die strafrechtlichen sowie strafprozessualen Folgen seiner Verletzung*, Francfort-sur-le-Main 2008 (cité: MÖHLENBECK, *Das absolute Folterverbot*).

MONTBEYRE RICHARD, *Le transfert de données bancaires à caractère personnel vers les Etats-Unis: aspects juridiques de l'Affaire SWIFT*, www.droit-tic.com, 2008, disponible à l'adresse: http://www.droit-tic.com/pdf/Aspects-juridiques-Swift.pdf (cité: MONTBEYERE, *Aspects juridiques de l'Affaire SWIFT*).

MOREILLON LAURENT, *Le suivi des mouvements de la personne: l'entraide policière et judiciaire au sein de l'Union européenne, L'individu face aux nouvelles technologies*, pp 69-92, Genève ; Zurich ; Bâle 2005 (cité: MOREILLON, *Le suivi des mouvements de la personne*).

MOREILLON LAURENT / BLANK SANDRA, *La surveillance policière et judiciaire des communications par Internet*, in: Medialex 2004 (2), pp 81-90 (cité: MOREILLON / BLANK, *La surveillance policière et judiciaire des communications par Internet*).

MORNET MARIE-NOËLLE, *La vidéosurveillance et la preuve*, Travaux et Mémoires de la Faculté de Droit et de Science Politique d'Aix-Marseille, Aix-en-Provence 2004 (cité: MORNET, *La vidéosurveillance et la preuve*).

MÜLLER JÖRG PAUL / SCHEFER MARKUS, *Grundrechte in der Schweiz im Rahmen der Bundesverfassung, der EMRK und der Uno-Pakte*, 4ème éd., Berne 2008 (cité: MÜLLER JÖRG PAUL / SCHEFER MARKUS, *Grundrechte in der Schweiz*).

MÜLLER MARKUS / WYSSMANN URSULA, *Polizeiliche Videoüberwachung: Rechtssetzungszuständigkeit nach bernischem Polizeigesetz* in: BVR/JAB 2005 (12), pp 529-554 (cité: MÜLLER / WYSSMANN, *Rechtssetzungszuständigkeit*).

MÜLLER RETO PATRICK, *Innere Sicherheit Schweiz: rechtliche und tatsächliche Entwicklungen im Bund seit 1848*, Egg bei Einsiedeln 2009 (cité: MÜLLER, *Innere Sicherheit Schweiz*).

NATTERER JUDITH, *Die Verwertbarkeit von Zufallsfunden aus der Telefonüberwachung im Strafverfahren: eine kritische Betrachtung des schweizerischen und deutschen Umgangs mit Ergebnissen heimlicher strafprozessualer Überwachungsmassnahmen*, Berne 2001 (cité: NATTERER, *Die Verwertbarkeit von Zufallsfunden*).

NIGGLI MARCEL ALEXANDER / HEER, MARIANNE / WIPRÄCHTIGER, HANS, *Schweizerische Strafprozessordnung / Schweizerische Jugendstrafprozessordung*, Bâle à paraître (cité: NIGGLI / HEER / WIPRÄCHTIGER, *Basler Kommentar StPO/JStPO*).

NIGGLI MARCEL ALEXANDER / UEBERSAX PETER / WIPRÄCHTIGER HANS, *Basler Kommentar zur Bundesgerichtsgesetz*, Bâle 2008 (cité: NIGGLI / UEBERSAX / WIPRÄCHTIGER, *Basler Kommentar BGG*).

OBERHOLZER NIKLAUS, *Grundzüge des Strafprozessrechts: dargestellt am Beispiel des Kantons St. Gallen*, 2ème éd., Berne 2005 (cité: OBERHOLZER, *Grundzüge des Strafprozessrechts*).

OBERHOLZER NIKLAUS, *Die Regeln bei polizeilich erhobenen Daten sind unklar*, in: plädoyer 2006, Vol. Beilage 6, pp 23-26 (cité: OBERHOLZER, *Die Regeln bei polizeilich erhobenen Daten sind unklar*).

OBERHOLZER NIKLAUS, *Strafprozessrecht*, Berne à paraître (cité: OBERHOLZER, *Strafprozessrecht*).

OFFICE FÉDÉRAL DE LA JUSTICE (OFJ), *Avis du 15 juin 1993*, in: JAAC 1993 (58.75) (cité: OFJ, *Avis du 15 juin 1993*).

OFFICE FÉDÉRAL DE LA JUSTICE (OFJ), *Rapport explicatif relatif à l'avant-projet de disposition constitutionnelle sur les mesures de lutte contre la violence dans le cadre des manifestations sportives* 2006, disponible à l'adresse: http://www.admin.ch/ch/f/gg/pc/documents/1469/Bericht_f.pdf (cité: OFJ, *Rapport relatif à la disposition constitutionnelle sur la violence dans le cadre des manifestations sportives*).

OFFICE FÉDÉRAL DE LA POLICE (FEDPOL), *Rapport d'activité 2008*, Berne 2009, (cité: FEDPOL, *Rapport 2008*).

OFFICE FÉDÉRAL DE LA POLICE (FEDPOL), *Rapport d'activité 2009*, Berne 2010, (cité: FEDPOL, *Rapport 2009*).

OFFICE FÉDÉRAL DE LA POLICE (FEDPOL), *Rapport explicatif à l'avant-projet de révision de la Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI)*, Berne 2006 disponible à l'adresse: http://www.ejpd.admin.ch/etc/medialib/data/sicherheit/bwis.Par.0023.File.tmp/Erlaeuterungen_BWIS_II_f.pdf (cité: FEDPOL, *Rapport explicatif à l'avant-projet de LMSI II*).

OFFICE FÉDÉRAL DES MIGRATIONS (ODM), *Commentaire explicatif relatif à l'adaptation d'ordonnances en raison de l'introduction de données biométriques dans le titre de séjour*, Berne 2010, disponible à l'adresse: http://www.ejpd.admin.ch/etc/medialib/data/migration/rechtsgrundlagen/gesetzgebung/biometrie_auslaenderausweis/anpassung_verordnungen.Par.0005.File.tmp/ber-f.pdf (cité: ODM, *Commentaire relatif à l'introduction de données biométriques dans le titre de séjour*).

OOSTERLINCK RENÉ, *Localisation par satellite: GALILEO*, in: OCDE (Ed.), *L'économie de la sécurité*, pp 87-102, Paris 2004 (cité: OOSTERLINCK, *Localisation par satellite*).

ORDOLLI GENEVIÈVE, *Les systèmes de surveillance des travailleurs: aspects de droit individuel et collectif*, in: DUNAND JEAN-PHILIPPE / MAHON PASCAL (Eds.), *«Le droit décloisonné», interférences et interdépendances entre droit privé et droit public, Enseignements de 3ème cycle de droit*, pp 199-224, Genève; Zurich; Bâle 2009 (cité: ORDOLLI, *Les systèmes de surveillance des travailleurs*).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *L'économie de la sécurité*, Paris 2004 (cité: OCDE, *L'économie de la sécurité*).

OTTINGER LUCIE, *L'exploitation des moyens de preuve obtenus illégalement: de la situation actuelle à celle du CPP unifié*, 2009, disponible à l'adresse: http://jusletter.weblaw.ch/article/fr/_7623?lang=fr (cité: OTTINGER, *L'exploitation des moyens de preuve obtenus illégalement*).

PAGE GÉRALD, *Le droit d'accès et de contestation dans le traitement des données personnelles: étude de base en droit privé suisse et américain*, Computer und Recht, Zurich 1983 (cité: PAGE, *Le droit d'accès en droit privé suisse et américain*).

PÉCLET JEAN-CLAUDE, *Ayant mis un pied à New York, VisioWave regarde la Chine*, in: Le Temps du 27 avril 2005, disponible à l'adresse: http://www.letemps.ch/dossiers/dossiersarticle.asp?ID=154605 (cité: PÉCLET, *Ayant mis un pied à New York, VisioWave regarde la Chine*).

PELTIER VIRGINIE, *Le secret des correspondances*, Aix-en-Provence 1999 (cité: PELTIER, *Le secret des correspondances*).

PETTITI LOUIS-EDMOND / DECAUX EMMANUEL / IMBERT PIERRE-HENRI, *La Convention européenne des droits de l'homme: commentaire article par article*, 2ème éd., Paris 1999 (cité: PETTITI / DECAUX / IMBERT, *La CEDH : commentaire article par article*).

PFISTER-LIECHTI RENATE, *La procédure pénale fédérale*, Berne 2010 (cité: PFISTER-LIECHTI, *La procédure pénale fédérale*).

PIETH MARK, *Schweizerisches Strafprozessrecht: Grundriss für Studium und Praxis*, Bâle 2009 (cité: PIETH, *Schweizerisches Strafprozessrecht*).

PIQUEREZ GÉRARD, *La preuve pénale: présentation générale*, *Revue jurassienne de jurisprudence*, pp 7-23, Porrentruy 2004 (cité: PIQUEREZ, *La preuve pénale*).

PIQUEREZ GÉRARD, *Traité de procédure pénale suisse*, 2ème éd., Genève, Zurich 2006 (cité: PIQUEREZ, *Traité*).

PLATTNER TITUS, *L'œil de Swisscom pour échapper aux bouchons*, in: L'Hebdo 2008 (42), pp 32-33 (cité: PLATTNER, TITUS, *L'œil de Swisscom*).

POIRSON, PHILIPPE, *Le G8 ou l'art qu'ont les images de faire illusion*, in: Le Courrier du 24 avril 2007, disponible à l'adresse: http://lecourrier.programmers.ch/index.php?name=News&file=article&sid=436286 (cité: POIRSON, *Le G8 ou l'art qu'ont les images de faire illusion*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES (PFPD), *Explications relatives aux webbugs (pixels espions) et aux bulletins d'information personnalisés* 2006, disponible à l'adresse: http://www.edoeb.admin.ch/dokumentation/00445/00471/00530/00999/index.html?lang=fr&download=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnqWfVp7Yhmfhnapmmc7Zi6rZnqCkkIN0f398bKbXrZ2lhtTN34al3p6YrY7P1oah162apo3X1cjYh2+hoJVn6w== (cité: PFPD, *Explications relatives aux webbugs*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES (PFPD), *11ème rapport d'activités 2003/2004*, Berne 2004 (cité: PFPD, *11ème rapport*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES (PFPD), *13ème rapport d'activités 2005/2006*, Berne 2006 (cité: PFPD, *13ème rapport*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Vidéosurveillance effectuée par des personnes privées*, Berne 2003, disponible à l'adresse: http://www.edoeb.admin.ch/dokumentation/00445/00507/00603/index.html?lang=fr (cité: PFPDT, *Vidéosurveillance effectuée par des personnes privées*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *14ème rapport d'activités 2006/2007*, Berne 2007 (cité: PFPDT, *14ème rapport*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail*, Berne 2007, disponible à l'adresse: http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=fr&download=M3wBPgDB/8ull6Du36WenojQ1NTTjaXZnqWfVp7Yhmfhnapmmc7Zi6rZnqCkkIN0e3x+bKbXrZ6lhuDZz8mMps2gpKfo (cité: PFPDT, *Surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *15ème rapport d'activités 2007/2008*, Berne 2008 (cité: PFPDT, *15ème rapport*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *16ème rapport d'activités 2008/2009*, Berne 2009 (cité: PFPDT, *16ème rapport*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Guide relatif aux systèmes de reconnaissance biométrique*, Berne 2009, disponible à l'adresse: http://www.edoeb.admin.ch/dokumentation/00445/00472/01369/index.html?lang=fr&download=M3wBPgDB/8ull6Du36WenojQ1NTTjaXZnqWfVp7Yhmfhnapmmc7Zi6rZnqCkkIN1gHh+bKbXrZ6lhuDZz8mMps2gpKfo (cité: PFPDT, *Systèmes de reconnaissance biométrique*).

PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *17ème rapport d'activités 2009/2010*, Berne 2010 (cité: PFPDT, *17ème rapport*).

PRIVATIM, *Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données*, Zurich 2006 (cité: PRIVATIM, *Guide pour l'évaluation de procédés biométriques sur le plan de la protection des données*).

PRIVATIM, *Communiqué de presse du 14 juin 2007*, Zurich 2007, disponible à l'adresse: http://www.privatim.ch/content/pdf/Medienmitteilung_Videoueberwachung_20070614.pdf (cité: PRIVATIM, *Communiqué de presse du 14 juin 2007*).

RAUBER PHILIPP, *Rechtliche Grundlagen der Erfüllung sicherheitspolizeilicher Aufgaben durch Private*, Bâle 2006 (cité: RAUBER, *Sicherheitspolizeiliche Aufgaben durch Private*).

RÉMY MARC, *Droit des mesures policières*, Genève, Zürich, Bâle 2008 (cité: RÉMY, *Droit des mesures policières*).

RHINOW RENÉ, *Grundzüge des schweizerischen Verfassungsrechts*, Bâle ; Genève ; Munich 2003 (cité: RHINOW, *Grundzüge*).

RHINOW RENÉ A. / SCHEFER MARKUS, *Schweizerisches Verfassungsrecht*, 2ème éd., Bâle 2009 (cité: RHINOW / SCHEFER, *Schweizerisches Verfassungsrecht*).

RHYNER BEAT, *Kommentar zu Art. 95-99 StPO*, in: ALBERTINI GIANFRANCO / FEHR BRUNO / VOSER BEAT (Eds.), *VSKC-Handbuch*, pp 135-154, Zurich 2008 (cité: RHYNER, *Kommentar zu Art. 95-99 StPO*).

RHYNER BEAT / STÜSSI DIETER, *Kommentar zu Art. 269-279 StPO*, in: ALBERTINI GIANFRANCO / FEHR BRUNO / VOSER BEAT (Eds.), *VSKC-Handbuch*, pp 432-461, Zurich 2008 (cité: RHYNER / STÜSSI, *Kommentar zu Art. 269-279 StPO*).

RHYNER BEAT / STÜSSI DIETER, *Kommentar zu Art. 280-281 StPO*, in: ALBERTINI GIANFRANCO / FEHR BRUNO / VOSER BEAT (Eds.), *VSKC-Handbuch*, pp 462-470, Zurich 2008 (cité: RHYNER / STÜSSI, *Kommentar zu Art. 280-281 StPO*).

RHYNER BEAT / STÜSSI DIETER, *Kommentar zu Art. 282-283 StPO*, in: ALBERTINI GIANFRANCO / FEHR BRUNO / VOSER BEAT (Eds.), *VSKC-Handbuch*, pp 471-483, Zurich 2008 (cité: RHYNER / STÜSSI, *Kommentar zu Art. 282-283 StPO*).

RHYNER BEAT / STÜSSI DIETER, *Kommentar zu Art. 284-285 StPO*, in: ALBERTINI GIANFRANCO / FEHR BRUNO / VOSER BEAT (Eds.), *VSKC-Handbuch*, pp 484-485, Zurich 2008 (cité: RHYNER / STÜSSI, *Kommentar zu Art. 284-285 StPO*).

RHYNER BEAT / STÜSSI DIETER, *Kommentar zu Art. 286-298 StPO*, in: ALBERTINI GIANFRANCO / FEHR BRUNO / VOSER BEAT (Eds.), *VSKC-Handbuch*, pp 488-530, Zurich 2008 (cité: RHYNER / STÜSSI, *Kommentar zu Art. 286-298 StPO*).

RIBAUX OLIVIER, *Les outils informatisés du renseignement criminel*, in: CIMICHELLA SANDRO / KUHN ANDRÉ / NIGGLI MARCEL ALEXANDER (Eds.), *Neue Technologie und Kriminalität: Neue Kriminologie? = Nouvelles technologies et criminalité: nouvelle criminologie?*, pp 135-156, Zurich; Coire 2006 (cité: RIBAUX, *Les outils informatisés du renseignement criminel*).

RIBAUX OLIVIER / GITZ PHILIPPE / CARTIER JULIEN, *L'analyse criminelle face à la complexité des données: risque pour la sphère privée ou moyen de la protéger?*, in: BOLLE PIERRE-HENRI / STEFFEN HEINZ (Eds.), *La criminalité financière, actes du 60ème Congrès international de criminologie*, pp 109-124, Bâle 2002 (cité: RIBAUX / GITZ / CARTIER, *L'analyse criminelle face à la complexité des données*).

RIEDO CHRISTOF / FIOLKA GERHARD / NIGGLI MARCEL ALEXANDER, *Schweizerisches Strafprozessrecht: eine Einführung*, Bâle à paraître (cité: RIEDO / FIOLKA / NIGGLI, *Schweizerisches Strafprozessrecht (Einführung)*).

RIGHETTI FABIO, *Kommentar zu Art. 196-240 StPO*, in: GOLDSCHMID PETER / MAURER THOMAS / SOLLBERGER JÜRG (Eds.), *Kommentierte Textausgabe zur StPO*, pp 185-228, Berne 2008 (cité: RIGHETTI, *Kommentar zu Art. 196-240 StPO*).

RIKLIN FRANZ, *Vollzugsdefizite noch und noch*, in: plädoyer 2009, Vol. 3, pp 18-22 (cité: RIKLIN, *Vollzugsdefizite noch und noch*).

RIKLIN FRANZ, *StPO Kommentar*, Zurich à paraître (cité: RIKLIN, *StPO Kommentar*).

RIPPE KLAUS PETER, *Der menschliche Körper als Datenträger*, in: digma 2005 (4), pp 150-151 (cité: RIPPE, *Der menschliche Körper als Datenträger*).

ROBERT CHRISTIAN-NILS, *Les mensonges du détecteur*, 2008, disponible à l'adresse: http://jusletter.weblaw.ch/article/fr/_6696?lang=fr (cité: ROBERT, *Les mensonges du détecteur*).

ROGGAN FREDRIK / KUTSCHA MARTIN, *Handbuch zum Recht der Inneren Sicherheit*, 2ème éd., Berlin 2006 (cité: ROGGAN / KUTSCHA, *Handbuch zum Recht der Inneren Sicherheit*).

ROHMER SANDRINE, *Les enquêtes de grande envergure dans le cadre de la nouvelle loi fédérale sur les profils d'ADN: une proportionnalité douteuse*, in: Revue pénale suisse 2006, Vol. 124 (1), pp 96-103 (cité: ROHMER, *Les enquêtes de grande envergure*).

ROHMER SANDRINE, *Spécificité des données génétiques et protection de la sphère privée: les exemples des profils d'ADN dans la procédure pénale et du diagnostic génétique*, Genève; Zurich; Bâle 2006 (cité: ROHMER, *Spécificité des données génétiques*).

ROHMER SANDRINE, *Commentaire ad art. 255-262 CPP*, in: KUHN ANDRÉ / JEANNERET YVAN (Eds.), *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: ROHMER, *Art. 255-262 CPP*).

ROHNER CHRISTOPH, *Kommentar zu Art. 22 BV*, in: EHRENZELLER BERNHARD / MASTRONARDI PHILIPPE / SCHWEIZER RAINER J. / VALLENDER KLAUS A. (Eds.), *Die schweizerische Bundesverfassung Kommentar*, pp 453-463, Zurich 2008 (cité: ROHNER, *Art. 22 BV*).

ROSENTHAL DAVID / JÖHRI YVONNE, *Handkommentar zum Datenschutzgesetz*, Zurich 2008 (cité: ROSENTHAL / JÖHRI, *Handkommentar zum DSG*).

ROUSELLE PIERRE-MARIE, *Le droit à la preuve*, Lausanne 1981 (cité: ROUSELLE, *Le droit à la preuve*).

RUCKSTUHL NIKLAUS, *Technische Überwachungen aus anwaltlicher Sicht*, in: Pratique juridique actuelle 2005 (2), pp 150-158 (cité: RUCKSTUHL, *Technische Überwachungen*).

RUCKSTUHL, NIKLAUS *Rechtswidrige Beweise erlaubt*, in: plädoyer 2006, Vol. Beilage 6, pp 15-22 (cité: RUCKSTUHL, *Rechtswidrige Beweise erlaubt*).

RUDIN BEAT, *"Indirekte Auskunft" nach art. 18 BWIS*, in: digma 2006 (4), pp 184-189 (cité: RUDIN, *Indirekte Auskunft*).

RUDIN BEAT, *Auf der Suche nach dem "Bodensatz" - Datenrechtliche Aspekte der präventiven Rasterfahndung*, in: Revue de l'avocat 2007 (6-7), pp 276-283 (cité: RUDIN, *Auf der Suche nach dem "Bodensatz"*).

RUDIN BEAT, *Datenschutzgesetze - fit für Europa*, Zürich 2007 (cité: RUDIN, *Datenschutzgesetze*).

RUDIN BEAT, *Videoüberwachung: Aufbewahrungsfrist*, in: digma 2007 (1), pp 34-36 (cité: RUDIN, *Videoüberwachung*).

RUDIN BEAT, *Das Recht auf Anonymität*, in: digma 2008 (1), pp 6-13 (cité: RUDIN, *Das Recht auf Anonymität*).

RUEDIN XAVIER-BAPTISTE, *Exécution des arrêts de la Cour européenne des droits de l'homme: procédure, obligations des Etats, pratique et réforme*, Collection de droit international public, Bâle 2009 (cité: RUEDIN, *Exécution des arrêts de la Cour européenne des droits de l'homme*).

RUEGG JEAN / FLÜCKIGER ALEXANDRE / NOVEMBER VALÉRIE / KLAUSER FRANCISCO, *Vidéosurveillance et risques dans l'espace à usage public: représentations des risques, régulation sociale et liberté de mouvement*, Travaux du CETEL 2006, disponible à l'adresse: http://www.unige.ch/droit/cetel/videosurveillance/travauxCETEL55.pdf (cité: RUEGG / FLÜCKIGER / NOVEMBER / KLAUSER, *Vidéosurveillance et risques dans l'espace à usage public*).

SALLAZ JEAN-PIERRE / DEBROSSE PHILIPPE / HAN DOMINIQUE, *Rapport sur l'efficacité de la vidéoprotection*, Ministère de l'intérieur, de l'outre-mer et des collectivités territoriales, Paris 2009, disponible à l'adresse: http://www.videoprotection.interieur.gouv.fr/admcontent/downloadDocuments/id/282 (cité: SALLAZ / DEBROSSE / HAN, *Rapport sur l'efficacité de la vidéoprotection*).

SAUER BARBARA, *Das Recht der Vollzugspolizeien von Bund und Kantonen in der Schweiz: eine vergleichende Untersuchung aus der Perspektive der bundesdeutschen Polizeirechtsordnung*, Würzburg 2007 (cité: SAUER, *Das Recht der Vollzugspolizeien*).

SCHEFER MARKUS, *Grundrechte in der Schweiz: Ergänzungsband zur dritten Auflage des gleichnamigen Werks von* JÖRG PAUL MÜLLER, Berne 2005 (cité: SCHEFER, *Grundrechte, Ergänzungsband*).

SCHMID GERHARD / COMMISSION TEMPORAIRE DU PARLEMENT EUROPÉEN SUR LE SYSTÈME D'INTERCEPTION ECHELON, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception Echelon)* 2001, disponible à l'adresse: http://www.europarl.europa.eucomparl/tempcom/echelon/pdf/rapport_echelon_fr.pdf (cité: SCHMID, *Rapport Echelon*).

SCHMID NIKLAUS, *Die nachträgliche Mitteilung von technischen Überwachungsmassnahmen im Strafprozess, insbesondere bei der Überwachung des Telefonsverkehrs*, in: Revue suisse de jurisprudence 1986, Vol. 82 (1), pp 37-46 (cité: SCHMID, NIKLAUS, *Die nachträgliche Mitteilung (1)*).

SCHMID NIKLAUS, *Verwertung von Zufallsfunden sowie Verwertungsverbote nach dem neuen Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)*, in: Revue pénale suisse 2002, Vol. 120 (3), pp 284-320 (cité: SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote*).

SCHMID NIKLAUS, *Strafprozessrecht eine Einführung auf der Grundlage des Strafprozessrechtes des Kantons Zürich und des Bundes*, 4ème éd., Zurich 2004 (cité: SCHMID, *Strafprozessrecht*).

SCHMID NIKLAUS, *Die Strafrechtsbeschwerde nach dem Bundesgesetzt über das Bundesgericht*, in: Revue pénale suisse 2006, Vol. 124, pp 160-207 (cité: SCHMID, *Die Strafrechtsbeschwerde*).

SCHMID NIKLAUS, *Handbuch des schweizerischen Strafprozessrechts*, Zurich 2009 (cité: SCHMID, *Handbuch*).

SCHMID NIKLAUS, *Schweizerische Strafprozessordnung, Praxiskommentar*, Zurich 2009 (cité: SCHMID, *Praxiskommentar*).

SCHNEIDER JÜRG, *Internet Service Provider im Spannungsfeld zwischen Fernmeldegeheimnis und Mitwirkungspflichten bei der Überwachung des E-Mail-Verkehrs über das Internet*, in: AJP/PJA 2005 (2), pp 179-192 (cité: SCHNEIDER, *Internet Service Provider im Spannungsfeld*).

SCHNEIER BRUCE , *Hackers Clone RFID Passports*, www.schneier.com, 2006, disponible à l'adresse: http://www.schneier.com/blog/archives/2006/08/hackers_clone_r.html (cité: SCHNEIER, *Hackers Clone RFID Passports*).

SCHNEIER BRUCE, *RFID Cards and Man-in-the-Middle Attacks*, www.schneier.com, 2006, disponible à l'adresse: http://www.schneier.com/blog/archives/2006/04/rfid_cards_and.html (cité: SCHNEIER, *RFID Cards and Man-in-the-Middle Attacks*).

SCHOTT MARKUS, *Kommentar zu Art. 95-98 BGG*, in: NIGGLI MARCEL ALEXANDER / UEBERSAX PETER / WIPRÄCHTIGER HANS (Eds.), *Basler Kommentar zur Bundesgerichtsgesetz*, pp 927-967, Bâle 2008 (cité: THOMMEN, *Art. 95-98 BGG*).

SCHWARTZ PAUL M., *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance* in: Hastings Law Journal 2003, Vol. 54 (751), pp 751-800 (cité: SCHWARTZ, *German and U.S. Telecommunications Privacy Law*).

SCHWARTZ PAUL M. / SOLOVE DANIEL J., *Information Privacy Law*, 3ème éd., New York 2009 (cité: SCHWARTZ / SOLOVE, *Information Privacy Law*).

SCHWARTZ PAUL M. / SOLOVE DANIEL J., *Privacy, Information, and Technology*, 2ème éd., New York 2009 (cité: SCHWARTZ / SOLOVE, *Privacy, Information, and Technology*).

SCHWARZENEGGER CHRISTIAN / NÄGELI ROLF, *Drittes Zürcher Präventionsforum: Videoüberwachung als Prävention?*, Zurich à paraître (cité: SCHWARZENEGGER / NÄGELI, *Drittes Zürcher Präventionsforum: Videoüberwachung als Prävention?*).

SCHWEGLER IVO, *Datenschutz im Polizeiwesen von Bund und Kantonen*, Berne 2001 (cité: SCHWEGLER, *Datenschutz im Polizeiwesen*).

SCHWEIZER RAINER J., *Kommentar zu Art. 3 BV*, in: EHRENZELLER BERNHARD / MASTRONARDI PHILIPPE / SCHWEIZER RAINER J. / VALLENDER KLAUS A. (Eds.), *Die schweizerische Bundesverfassung Kommentar*, pp 79-91, Zurich 2008 (cité: SCHWEIZER, *Art. 3 BV*).

SCHWEIZER RAINER J. *Kommentar zu Art. 10 BV*, in: EHRENZELLER BERNHARD / MASTRONARDI PHILIPPE / SCHWEIZER RAINER J. / VALLENDER KLAUS A. (Eds.), *Die schweizerische Bundesverfassung Kommentar*, pp 250-272, Zurich 2008 (cité: SCHWEIZER, *Art. 10 BV*).

SCHWEIZER RAINER J., *Kommentar zu Art. 36 BV*, in: EHRENZELLER BERNHARD / MASTRONARDI PHILIPPE / SCHWEIZER RAINER J. / VALLENDER KLAUS A. (Eds.), *Die schweizerische Bundesverfassung Kommentar*, pp 727-742, Zurich 2008 (cité: SCHWEIZER, *Art. 36 BV*).

SCHWOB RENATE, *Die nachträgliche Mitteilung von technischen Überwachungsmassnahmen im Strafprozess, insbesondere bei der Ueberwachung des Telefonsverkehrs*, in: Revue suisse de jurisprudence 1987, Vol. 83 (10), pp 166-169 (cité: SCHWOB, RENATE, *Die nachträgliche Mitteilung (2)*).

SEILER HANSJÖRG / VON WERDT NICOLAS / GÜNGERICH ANDREAS, *Bundesgerichtsgesetz (BGG)*, Berne 2007 (cité: SEILER / WERDT / GÜNGERICH, *BGG*).

SERVICE DE RENSEIGNEMENT DE LA CONFÉDÉRATION (SRC), *La sécurité de la Suisse 2009*, Berne 2010, disponible à l'adresse: http://www.news.admin.ch/NSBSubscriber/message/attachments/19841.pdf (cité: SRC, *Rapport annuel 2009*).

SERVICE DE RENSEIGNEMENT STRATÉGIQUE (SRS), *Le service de renseignement stratégique de la Suisse* 2008, disponible à l'adresse: http://www.vbs.admin.ch/internet/vbs/fr/home/documentation/publication/snd_publ.parsys.9918.downloadList.51103.DownloadFile.tmp/broschueresndwebf.pdf (cité: SRS, *Le service de renseignement stratégique de la Suisse*).

SHARANDIN YURI, *Rapport de la Commission des questions juridiques et des droits de l'homme du Conseil de l'Europe sur la vidéosurveillance des lieux publics* 2008, disponible à l'adresse: http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc08/FDOC11478.pdf (cité: SHARANDIN, *Rapport sur la vidéosurveillance des lieux publics*).

SIGRIST GABRIEL, *Géolocalisation, écoutes et cyberenquêtes*, in: Reflex 2007 (1), pp 35-36 (cité: SIGRIST, *Reflex*).

SIMON STÉPHANIE, *Les preuves illicites: le cas des écoutes téléphoniques*, Droit du procès et de la preuve judiciaire, 2009, disponible à l'adresse: http://m2bde.u-paris10.fr/blogs/dpj/index.php/post/2009/02/26/Les-preuves-illicites-%3A-le-cas-des-ecoutes-telephoniques-par-Stephanie-SIMON (cité: SIMON, *Les preuves illicites*).

SOÒS ROBERT / VÖGELI CHRISTOPH, *BWIS-Massnahmen gegen Gewalt an Sportveranstaltungen: Top oder Flop?*, in: Sécurité & Droit 2008 (3), pp 156-161 (cité: SOÒS / VÖGELI, *Top oder Flop?*).

SPENLÉ CHRISTOPH ANDRÉ / MATTLI ARTHUR / SCHENK NOËMI, *Kompendium zum Schutz der Menschenrechte: Quellensammlung für die Schweiz*, Berne 2009 (cité: SPENLÉ / MATTLI / SCHENK, *Kompendium*).

STAUB LEO, *Tonaufnahmen als Mittel zur Aufdeckung von Straftaten insbesondere im Kanton St.Gallen*, Zurich 1986 (cité: STAUB, *Tonaufnahmen*).

STEINAUER PAUL-HENRI, *Les droits réels I*, 4ème éd., Précis de droit Staempfli, Berne 2007 (cité: STEINAUER, *Les droits réels I*).

STEINER HEINRICH, *Das Grundrecht der Unverletzlichkeit der Wohnung*, Zürich 1959 (cité: STEINER, *Das Grundrecht der Unverletzlichkeit der Wohnung*).

STEVENS BARRIE, *Les facteurs de la demande de biens et services de sécurité*, in: OCDE (Ed.), *L'économie de la sécurité*, pp 19-38, Paris 2004 (cité: STEVENS, *Les facteurs de la demande de biens et services de sécurité*).

STRASSER OTHMAR, *Polizeiliche Zwangsmassnahmen*, Zurich 1981 (cité: STRASSER, *Polizeiliche Zwangsmassnahmen*).

STRÄULI BERNHARD, *La surveillance de la correspondance par poste et télécommunication: aperçu du nouveau droit*, in: CASSANI U. / DITTMANN V. / MAAG R. / STEINER S. (Eds.), *Mehr Sicherheit – weniger Freiheit? Ermittlungs- und Beweistechniken hinterfragt = Plus de sécurité – moins de liberté? Les techniques d'investigation et de preuve en question*, pp 93-194, Zurich ; Coire 2003 (cité: STRÄULI, *La surveillance de la correspondance par poste et télécommunication*).

STROBEL DAEHYUN, *IMSI Catcher*, Bochum 2007, disponible à l'adresse: http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/seminare/itsss07/imsi_catcher.pdf (cité: STROBEL, *IMSI Catcher*).

STUDER MARCEL, *Mit Datenbanken gegen Hooliganismus*, in: digma 2006 (2), pp 66-69 (cité: STUDER, *Mit Datenbanken gegen Hooliganismus*).

SUDRE FRÉDÉRIC, *Droit européen et international des droits de l'homme*, 6ème éd., Paris 2003 (cité: SUDRE, *Droit européen et international des droits de l'homme*).

SUDRE FRÉDÉRIC / MARGUENAUD JEAN-PIERRE, *et al.*, *Les grands arrêts de la Cour européenne des droits de l'homme*, 3ème éd., Paris 2005 (cité: SUDRE / MARGUENAUD, *et al.*, *Les grands arrêts de la CourEDH*).

SULZER LINDA / STRASSMANN JASMIN / ZUBER ANDREAS, *Internet als zeitgemässes Fahndungsmittel* in: Sécurité & Droit 2010 (1), pp 3-10 (cité: SULZER / STRASSMANN / ZUBER, *Internet als zeitgemässes Fahndungsmittel*).

TABATONI PIERRE / GROUPE D'ÉTUDES SOCIÉTÉ D'INFORMATION ET VIE PRIVÉE (PARIS), *La protection de la vie privée dans la société d'information: l'impact des systèmes électroniques d'information*, Paris 2000 (cité: TABATONI, *La protection de la vie privée dans la société d'information*).

TARONI F. / CASTELLA V. / RIBAUX O. / HICKS T., *Statistical foundations and ethical considerations on partial DNA profiles and familial searching using the swiss DNA database (projet FNSRS n°100011-113881)*, Lausanne 2008 (cité: TARONI / CASTELLA / RIBAUX / HICKS, *Partial DNA profiles and familial searching*).

TARONI FRANCO, *Interprétation de la preuve ADN: le juriste, le scientifique et les probabilités*, in: CASSANI U. / DITTMANN V. / MAAG R. / STEINER S. (Eds.), *Mehr Sicherheit – weniger Freiheit? Ermittlungs- und Beweistechniken hinterfragt = Plus de sécurité – moins de liberté? Les techniques d'investigation et de preuve en question*, pp 273-294, Zurich; Coire 2003 (cité: TARONI, *Interprétation de la preuve ADN*).

TARONI FRANCO / AITKEN COLIN, *Probabilités et preuve par l'ADN dans les affaires civiles et criminelles. Questions de la cour et réponses fallacieuses des experts*, in: Revue pénale suisse 1998, Vol. 116, pp 291-313 (cité: TARONI / AITKEN, *Probabilités et preuve par l'ADN*).

TARONI FRANCO / MANGIN PATRICE, *La preuve ADN, les probabilités, les experts et les juristes: nécessité de développement et de communication*, Lausanne 1999 (cité: TARONI / MANGIN, *La preuve ADN, les probabilités, les experts et les juristes*).

THOMMEN MARC, *Kommentar zu Art. 78-81 BGG*, in: NIGGLI MARCEL ALEXANDER / UEBERSAX PETER / WIPRÄCHTIGER HANS (Eds.), *Basler Kommentar zur Bundesgerichtsgesetz*, pp 662-697, Bâle 2008 (cité: THOMMEN, *Art. 78-81 BGG*).

TISSOT NATHALIE, *Limites juridiques à l'utilisation des bases de données informatiques*, 3e Journée de droit des ingénieurs, Neuchâtel 1996 (cité: TISSOT, *Limites juridiques à l'utilisation des bases de données informatiques*).

TISSOT NATHALIE, *Bases de données et droit d'auteur*, *Internet 2003*, pp 185-213, Lausanne 2004 (cité: TISSOT, *Bases de données et droit d'auteur*).

TRECCANI JEAN, *Interceptions électroniques*, in: CASSANI U. / DITTMANN V. / MAAG R. / STEINER S. (Eds.), *Mehr Sicherheit – weniger Freiheit? Ermittlungs- und Beweistechniken hinterfragt = Plus de sécurité – moins de liberté? Les techniques d'investigation et de preuve en question*, pp 217-238, Zurich; Coire 2003 (cité: TRECCANI, *Interceptions électroniques*).

VADROT CLAUDE-MARIE, *La grande surveillance: caméras, ADN, portables, Internet*, L'histoire immédiate, Paris 2007 (cité: VADROT, *La grande surveillance*).

VERDONNET JEAN-FRANÇOIS, *Les internautes britanniques invités à dénoncer les crimes et les délits*, in: La Tribune de Genève du 8 octobre 2009, disponible à l'adresse: http://www.tdg.ch/actu/monde/internautes-britanniques-invites-denoncer-crimes-delits-2009-10-07 (cité: VERDONNET, *Les internautes britanniques invités à dénoncer les crimes et les délits*).

VERNIORY JEAN-MARC, *Les droits de la défense dans les phases préliminaires du procès pénal*, Etudes de droit suisse, Berne 2005 (cité: VERNIORY, *Les droits de la défense*).

VERNIORY JEAN-MARC, *L'accès au dossier en procédure pénale*, in: La Semaine Judiciaire 2007, Vol. II (4), pp 125-151 (cité: VERNIORY, *L'accès au dossier*).

VEST HANS / HÖHENER ANDREA, *Beweisverwertungsverbote: quo vadis Bundesgericht?*, in: Revue pénale suisse 2009, Vol. 127 (1), pp 95-108 (cité: VEST / HÖHENER, *Beweisverwertungsverbote*).

VETTERLI LUZIA, *Bemerkungen zur BGE 1P.51/2007*, in: Forum poenale 2008 (2), pp 82-86 (cité: VETTERLI, *Bemerkungen zur BGE 1P.51/2007*).

VETTERLI LUZIA, *Verdeckte Ermittlung und Grundrechtsschutz*, in: Forum poenale 2008 (6), pp 367-373 (cité: VETTERLI, *Verdeckte Ermittlung und Grundrechtsschutz*).

VETTERLI LUZIA, *Gesetzesbindung im Strafprozess zur Geltung von Verwertungsverboten und ihrer Fernwirkung nach illegalen Zwangsmassnahmen*, Zurich 2010 (cité: VETTERLI, *Geltung von Verwertungsverboten und ihrer Fernwirkung*).

VIENNE ROGER, *Les écoutes téléphoniques au regard de la Cour européenne des droits de l'homme, Mélanges offerts à Georges Levasseur*, pp 263-285, Paris 1992 (cité: VIENNE, *Les écoutes téléphoniques au regard de la Cour*).

VILLIGER MARK EUGEN, *Handbuch der Europäischen Menschenrechtskonvention (EMRK): unter besonderer Berücksichtigung der schweizerischen Rechtslage*, 2ème éd., Zurich 1999 (cité: VILLIGER, *Handbuch der EMRK*).

VILLIGER MARK EUGEN, *Das Urteil des Europäischen Gerichtshofs für Menschenrechte*, in: Revue de droit suisse 2008, Vol. 127 (5), pp 453-474 (cité: VILLIGER, *Das Urteil des EGMR*).

VIREDAZ BAPTISTE, *Le sentiment d'insécurité: devons-nous avoir peur ?*, la question, Grolley 2005 (cité: VIREDAZ, *Le sentiment d'insécurité*).

VOGGENAUER-VON BOTHMER ROLAND, *Welche Daten werden wirklich gebraucht?*, in: digma 2007 (3), pp 102-104 (cité: VOGGENAUER-VON BOTHMER, *Welche Daten*).

VON BENTIVEGNI ASTRID, *Les mesures officielles de surveillance en procédure pénale*, Lausanne 1986 (cité: VON BENTIVEGNI, *Les mesures officielles de surveillance*).

VON DÄNIKEN URS, *Sicherheit bei Sportveranstaltungen*, in: digma 2006 (2), pp 54-58 (cité: VON DÄNIKEN, *Sicherheit bei Sportveranstaltungen*).

VON GUNTEN JEAN-MARC, *Das Grundrecht auf Unverletzlichkeit der Wohnung*, Zurich 1992 (cité: VON GUNTEN, *Das Grundrecht auf Unverletzlichkeit der Wohnung*).

VOSER BEAT, *Kommentar zu Art. 255-259 StPO*, in: ALBERTINI, GIANFRANCO / FEHR, BRUNO / VOSER, BEAT (Eds.), *VSKC-Handbuch*, pp 370-391, Zurich 2008 (cité: VOSER, *Kommentar zu Art. 255-259 StPO*).

VUCHER-BONDET AURÉLIE, *La recevabilité d'un témoignage sous hypnose en tant que moyen de preuve: approche comparée Etats-Unis / France*, Droit du procès et de la preuve judiciaire, 2009, disponible à l'adresse: http://m2bde.u-paris10.fr/blogs/dpj/index.php/post/2009/04/07/La-recevabilite-dun-temoignage-sous-hypnose-en-tant-que-moyen-de-preuve-%3A-approche-comparee-Etats-Unis-/-France-par-Aurelie-VUCHER-BONDET (cité: VUCHER-BONDET, *La recevabilité d'un témoignage sous hypnose*).

WALTER JEAN-PHILIPPE, *La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données*, *La protection des données en Suisse et en Europe*, pp 83-118, Fribourg 1999 (cité: WALTER, *La Convention pour la protection des personnes à l'égard du traitement automatisé des données*).

WALTER JEAN-PHILIPPE, *Le droit de l'individu à l'autoprotection lors du traitement de données personnelles dans le domaine des télécommunications*, in: COTTIER, BERTIL (Ed.), *Le droit des télécommunications en mutation*, pp 459-482, Fribourg 2001 (cité: WALTER, *Le droit de l'individu à l'autoprotection lors du traitement de données personnelles*).

WEICHERT THILO, *Überwachung: Einblick in die Praxis, Gängige Überwachungspraktiken im Bereich des öffentlichen und privaten Lebens*, in: digma 2002 (1), pp 4-9 (cité: WEICHERT, *Überwachung: Einblick in die Praxis*).

WEISSEN ROMAIN, *Les services de renseignement suisses*, Berne 2004 (cité: WEISSEN, *Les services de renseignement suisses*).

WELP, JÜRGEN, *Auf dem Weg zum Überwachungsstaat ?, Aktuelle Entwicklungen in der staatlichen Überwachung von Bürgerinnen und Bürgern*, in: digma 2002 (1), pp 18-22 (cité: WELP, *Auf dem Weg zum Überwachungsstaat*).

WELSH BRANDON C. / FARRINGTON DAVID P., *Crime prevention effects of closed circuit television: a systematic review*, Home Office Research, Development and Statistics Directorate n° 252, Londres 2002, disponible à l'adresse: http://www.homeoffice.gov.uk/rds/pdfs2/hors252.pdf (cité: WELSH / FARRINGTON, *Crime prevention effects of CCTV*).

WINZAP PIERRE-HENRI, *La procédure de première instance (CPP 328 à CPP 351)*, in: PFISTER-LIECHTI RENATE (Ed.), *La procédure pénale fédérale*, pp 95-106, Berne 2010 (cité: WINZAP, *La procédure de première instance*).

WOHLERS WOLFGANG, *Das Bundesgesetz über die verdeckte Ermittlung (BVE)*, in: Revue de droit suisse 2005, Vol. 124 (3), pp 219-241 (cité: WOHLERS, *Revue de droit suisse*).

WOLTER, ROLAND, *Kommentar zu Art. 269-281 StPO*, in: GOLDSCHMID PETER / MAURER THOMAS / SOLLBERGER JÜRG (Eds.), *Kommentierte Textausgabe zur StPO*, pp 254-272, Berne 2008 (cité: WOLTER, *Kommentar zu Art. 269-281 StPO*).

YON MARCEL, *Etude sur la biométrie: rapport à l'attention du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD)*, Bochum 2004, disponible à l'adresse: http://www.coe.int/T/F/Affaires_juridiques/Coopération_juridique/Protection_des_données/Documents/ (cité: YON, *Etude sur la biométrie*).

ZALUNARDO-WALSER ROBERTO, *Verdeckte kriminalpolizeiliche Ermittlungsmassnahmen unter besonderer Berücksichtigung der Observation*, S.l. 1998 (cité: ZALUNARDO-WALSER, *Verdeckte kriminalpolizeiliche Ermittlungsmassnahmen*).

ZUFFEREY NATHALIE / BACHER JEAN-LUC, *Commentaire ad art. 269 CPP*, in: KUHN ANDRÉ / JEANNERET YVAN (Eds.), *Commentaire romand du Code de procédure pénale*, Bâle à paraître (cité: ZUFFEREY / BACHER, *Art. 269 CPP*).