

Zeitschrift: Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie = Collection criminologie / Groupe suisse de travail de criminologie
Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie
Band: 21 (2003)

Artikel: La surveillance de la correspondance par poste et télécommunication : aperçu du nouveau droit
Autor: Sträuli, Bernhard
DOI: <https://doi.org/10.5169/seals-1051092>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 20.02.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

BERNHARD STRÄULI

**LA SURVEILLANCE DE LA CORRESPONDANCE
PAR POSTE ET TÉLÉCOMMUNICATION:
APERÇU DU NOUVEAU DROIT**

Résumé

Depuis le 1^{er} janvier 2002, la surveillance de la correspondance par poste et télécommunications est régie par une loi fédérale, la LSCPT, et son ordonnance d'exécution, l'OSCPT. Ces deux textes définissent de manière fort détaillée les types de mesures et les informations susceptibles d'être collectées, les conditions matérielles et formelles d'une mise sous surveillance, les modalités d'exécution de la mesure, la levée de celle-ci ainsi que les voies de droit ouvertes aux personnes touchées. L'auteur aborde ces différents aspects d'un œil critique, dans l'espoir que les dispositions considérées subiront les adaptations qui s'imposent avant leur incorporation dans le projet de code de procédure pénale suisse, actuellement en cours d'élaboration.

Die Überwachung des Post- und Fernmeldeverkehrs: Überblick über das neue Gesetz

Seit dem 1. Januar 2002 ist die Überwachung des Post- und Fernmeldeverkehrs durch ein Bundesgesetz (BÜPF) und dessen Vollzugsverordnung (VÜPF) geregelt. Diese beiden Erlasses bestimmen in sehr ausführlicher Weise die Massnahmetypen und erlangbaren Informationen, die sachlichen und formellen Voraussetzungen der Überwachung, die Art und Weise ihrer Durchführung, die Aufhebung der Massnahme sowie die den betroffenen Personen zu Verfügung stehenden Rechtsmittel. Der Verfasser greift diese verschiedenen Aspekte kritisch auf, in der Hoffnung, dass diese Bestimmungen anlässlich der aktuellen Ausarbeitung des Entwurfs einer Bundesstrafprozessordnung nochmals überarbeitet werden.

I Introduction

Depuis le 1^{er} janvier 2002, la mesure processuelle de contrainte que 1. l'on appelait autrefois la surveillance postale, téléphonique et télégraphique est régie par la Loi fédérale sur la surveillance de la correspondance par poste et télécommunication, du 6 octobre 2000 (LSCPT) et son Ordonnance d'exécution du même nom, du 31 oc-

tobre 2001 (OSCPT)¹. Ces deux textes ont non seulement remplacé les dispositions existantes de la Loi fédérale sur la procédure pénale² et de la Procédure pénale militaire^{3/4} – , mais se sont également substitués⁵ aux réglementations prévues jusqu'alors par les vingt-six codes cantonaux de procédure pénale⁶. Après l'entrée en vigueur de la Loi fédérale sur l'aide aux victimes d'infractions⁷, avant l'adoption par les Chambres fédérales de lois sur l'investigation secrète⁸ et sur les profils d'ADN⁹, dans l'attente, enfin, de l'élaboration d'un projet de Code de procédure pénale suisse¹⁰, les nouvelles dispositions en matière de surveillance de la correspondance par poste et télécommunication constituent une seconde étape, importante, sur le chemin de l'unification complète de la procédure pénale en Suisse.

-
- 1 L'OSCPT, plus précisément l'annexe mentionnée à son art. 30 al. 1, est complétée par l'Ordonnance sur les émoluments et les indemnités en matière de surveillance de la correspondance postale et des télécommunications, du 21 juin 2000 (OEIS), provisoirement conservée de l'ancien droit (sur les raisons de ce régime transitoire, voir HANSJAKOB, Art. 30 VÜPF n° 2).
 - 2 Anciens art. 66–66^{quinquies} et 72 PPF (RO 1979 p. 1170–1172, 1992 p. 312, 1992 p. 599).
Sous réserve de ses art. 247 à 279, la PPF régit la poursuite, l'instruction et le jugement des infractions soumises à la juridiction fédérale ordinaire (non militaire), telle que définie par les art. 340 et 340^{bis} CP et les dispositions apparentées du droit pénal fédéral accessoire, par exemple les art. 40 al. 1 LFMG, 36e al. 1 LEA et 98 al. 1 LA.
 - 3 Anciens art. 70–73 PPM (RO 1979 p. 1174–1175, 1992 p. 314, 1992 p. 600).
La PPM gouverne la poursuite, l'instruction et le jugement des infractions soumises à la juridiction (fédérale) militaire, telle que définie par l'art. 218 CPM.
 - 4 Le nouveau droit n'a, en revanche, pas affecté la Loi fédérale sur le droit pénal administratif, dans l'arsenal des mesures de contrainte de laquelle (art. 45–60 DPA) les mesures de surveillance ne figurent pas (cf. ATF 118 IV 70 consid. 3c).
 - 5 Sur le fondement constitutionnel (discutable) de cette intrusion de la Confédération dans la compétence des cantons en matière de procédure pénale (art. 123 al. 3 Cst. dans sa teneur du 18 avril 1999 [RO 1999 p. 2586], en vigueur jusqu'au 31 mars 2003 [RO 2002 p. 3147–3148]), voir CONSEIL FÉDÉRAL 3705, 3751–3753.
 - 6 Notablement plus étendue que les juridictions fédérales ordinaire et militaire, la juridiction cantonale est définie par l'art. 343 CP et nombre de dispositions apparentées du droit pénal fédéral accessoire, par exemple les art. 24 al. 1 phr. 1 LSEE, 103 al. 2 LCR et 28 al. 1 LStup.
 - 7 Art. 5 à 10d LAVI.
 - 8 FF 1998 p. 3689–3771 (message et projet du Conseil fédéral), 2003 p. 4009–4018 (texte adopté par le Palament).
 - 9 FF 2001 p. 19–56. (message et projet du Conseil fédéral), 2003 p. 3981–3989 (texte adopté par le Palament).
 - 10 Cf. OFFICE FÉDÉRAL DE LA JUSTICE, Avant-projet d'un Code de procédure pénale suisse (CPP), Berne 2001; IDEM, Rapport explicatif relatif à l'avant-projet d'un Code de procédure pénale suisse, Berne 2001.

II Indications générales

A Types de mesures

1 Surveillance de la correspondance par poste

a) Notion de correspondance par poste

La correspondance par poste consiste dans la transmission d'envois **2.** de la poste aux lettres et de colis. Les premiers regroupent les envois n'excédant pas le format B4 (353 x 250 mm), l'épaisseur de 5 cm et le poids de 1 kg¹¹, par exemple les lettres, les cartes postales, les journaux, les imprimés et les télégrammes. Les seconds regroupent les autres envois pesant jusqu'à 30 kg¹².

La LSCPT ne s'applique toutefois qu'aux fournisseurs de services **3.** postaux soumis à concession¹³. Si elle permet ainsi d'appréhender toutes les prestations offertes par La Poste Suisse¹⁴, celles qui émanent d'opérateurs privés (DHL, FedEx, UPS, etc., y compris le courrier de quartier) lui échappent dans la mesure où, relevant des services dits non réservés¹⁵, leur mise sur le marché n'a pas été subordonnée par le Conseil fédéral à l'obtention d'une concession¹⁶. Dans les secteurs non couverts par la LSCPT, les mesures ordinaires d'investigations (demande de renseignements, témoignage) et de contrainte (perquisition, ordre de production, saisie) sont appelées à prendre le relais¹⁷. Sur le plan des principes, cette coexistence de deux régimes procéduraux différents et les inégalités de traitement qui en résultent¹⁸ sont injustifiables.

11 Art. 1 let. a OPO.

12 Art. 1 let. b OPO.

13 Art. 1 al. 2 LSCPT.

14 Cf. art. 1 al. 2 LPO.

15 Art. 4 LPO *cum* art. 3 al. 1 phr. 1 *e contrario* et al. 2–3 LPO; art. 2–4 OPO.

16 Cf. art. 5 al. 1 LPO.

17 CONSEIL FÉDÉRAL 3703; HANSJAKOB, Art. 1 BÜPF n° 10.

18 Cf. *infra* n° 14.

b) Objet de la surveillance

4. L'objet de la surveillance est toujours une adresse postale¹⁹, identifiable idéalement par
 - un prénom et un nom, une rue et son numéro, une localité et son code postal;
 - un prénom et un nom, un numéro de case postale, une localité, son code postal et, cas échéant, le numéro de l'office postal mettant la case à disposition; ou encore
 - un prénom et un nom, la mention «Poste restante», une localité, son code postal et, cas échéant, le numéro de l'office postal conservant les envois.
5. Contrairement à ce que suggèrent plusieurs dispositions de la loi²⁰, la surveillance ne porte donc pas sur une personne déterminée. De ce point de vue, la surveillance de la correspondance par poste est une mesure «réelle» (comme la perquisition, qui vise un lieu déterminé) et non pas une mesure «personnelle» (comme la détention préventive, qui vise un individu déterminé). Dans la pratique, il découle de cette qualification que la découverte d'une résidence secondaire, un séjour hors du domicile (par exemple à l'occasion de vacances) ou un changement d'adresse nécessitent la mise en place d'une nouvelle mesure de surveillance pour que la correspondance dirigée à l'adresse considérée soit (également) interceptée.

c) Surveillance en temps réel

6. La surveillance en temps réel représente en quelque sorte la forme classique, prospective, de la mesure, comme on la conçoit intuitivement.
7. Elle consiste d'abord²¹ dans l'interception des envois postaux dirigés vers l'adresse surveillée, leur rétention temporaire, l'ouverture du contenant (enveloppe, paquet, etc.), l'examen du contenu, la dupli-

19 Cf. art. 4 al. 1 *in fine*, 4 al. 2, 10 al. 2 let. b LSCPT.

20 Voir les art. 3 al. 1 let. a, 4 al. 1 *in limine*, 4 al. 3, 4 al. 6, 5 al. 1 let. a, 10 al. 5 LSCPT.

21 Art. 3–4 LSCPT.

tion éventuelle du contenant et/ou du contenu (photocopies, photographies, scanning, etc.), la remise du contenu dans le contenant, la fermeture de ce dernier, enfin l'acheminement de l'envoi à son destinataire²², de telle manière que celui-ci ne puisse soupçonner les opérations précitées, l'efficacité de la surveillance reposant sur son secret et la possibilité de répéter les contrôles à intervalles réguliers (en principe quotidiennement). Mais la surveillance peut aussi aboutir, cas échéant au prix du secret, à la rétention durable d'un envoi²³, notamment lorsque l'intérêt public (sécurité publique *ad* substances toxiques, manifestation de la vérité *ad* empreintes, etc.) ou l'intérêt de particuliers (par exemple le destinataire, la personne lésée par l'infraction, etc.) le commandent, l'acheminement au destinataire devant alors intervenir si et lorsque l'avancement de la procédure le permet²⁴.

La surveillance en temps réel de la correspondance postale consiste **8.** ensuite dans le relevé des données – à supposer qu'elles soient disponibles – qui caractérisent l'envoi et permettent (notamment) d'identifier les correspondants, à savoir l'identité de l'expéditeur et du destinataire, la nature de l'envoi (lettre ou colis, pli simple ou recommandé, etc.), le lieu, la date et l'heure d'expédition et d'acheminement²⁵.

La surveillance en temps réel consiste enfin dans le relevé de renseignements complémentaires sollicités par l'autorité qui a ordonné la surveillance et indiquant par exemple qui vient relever une case postale, à quelle fréquence, quels ordres de réacheminement des envois ont été donnés et par qui²⁶.

Les trois formes précitées de la surveillance en temps réel peuvent **10.** être ordonnées cumulativement ou alternativement.

22 Art. 12 let. a OSCPT.

23 Art. 8 al. 2 phr. 1 LSCPT.

24 Art. 8 al. 2 phr. 2 LSCPT.

25 Art. 5 al. 1 let. a LSCPT; art. 12 let. b OSCPT.

26 Art. 12 al. 1 phr. 2 LSCPT; art. 12 let. d OSCPT; HANSJAKOB, Art. 12 VÜPF n° 7.

d) Surveillance rétroactive

11. L'expression de «surveillance rétroactive» représente en soi une contradiction dans les termes. A proprement parler, on ne peut que surveiller un événement futur.
12. Or, avec la surveillance dite rétroactive, il s'agit d'accéder à certaines données recueillies puis conservées un temps déterminé²⁷ par les fournisseurs de services postaux à l'occasion d'acheminements d'envois commencés et achevés dans le passé, c'est-à-dire avant qu'un ordre de surveillance n'ait été décerné. *De facto* et *de iure*, une telle mesure ne permet pas de prendre connaissance du contenu de l'envoi ni, partant, de le dupliquer pour les besoins de l'enquête pénale. Elle permet en revanche aux autorités de poursuite et d'instruction de recevoir toutes les données relatives au trafic et à la facturation²⁸ que les fournisseurs de services postaux ont physiquement conservées, soit en vertu d'une obligation légale ou contractuelle, par exemple en cas de délivrance d'une lettre recommandée, d'un colis inscrit, d'un pli avec accusé de réception ou d'un envoi contre remboursement²⁹, soit pour les besoins de leur fonctionnement interne³⁰.
13. Dans la mesure restreinte où les agents des services postaux en ont gardé le souvenir³¹, les renseignements complémentaires déjà mentionnés à propos de la surveillance en temps réel peuvent également faire l'objet d'une surveillance rétroactive³². Alors même que l'art. 321^{ter} al. 5 CP réserve les dispositions fédérales et cantonales statuant une obligation de témoigner en justice, ces renseignements ne peuvent pas, en l'état du droit positif, être obtenus dans le simple cadre d'une audition des agents concernés en qualité de témoins³³; un

27 *Infra* n° 62, 94.

28 Art. 5 al. 1 let. b LSCPT.

29 Art. 12 let. c ch. 1 OSCPT qui, à l'instar de l'art. 12 let. b OSCPT relatif à la surveillance en temps réel, mentionne l'expéditeur, le destinataire et la nature de l'envoi, ainsi que ses paramètres d'acheminement, ici toutefois seulement si ces derniers sont disponibles.

30 Art. 12 let. c ch. 2 OSCPT.

31 C'est ici que réside la différence d'avec l'hypothèse visée par l'art. 12 let. c ch. 2 OSCPT précité.

32 Art. 12 let. d OSCPT.

33 Voir par exemple les art. 74–88^{ter} PPF, 41 DPA, 74–84a PPM, 42–64 CPP. Pour une critique, voir HANS-JAKOB, Art. 12 BÜPF n° 4.

tel procédé reviendrait en effet à contourner les restrictions posées notamment par les art. 3 et 7 LSCPT à la levée du secret des postes³⁴.

e) *Délimitation par rapport à la perquisition, l'ordre de production et la saisie*

Tant matériellement que formellement, la surveillance de la correspondance par poste selon la LSCPT et l'OSCPT est soumise à des exigences autrement plus restrictives que la perquisition, l'ordre de production et la saisie. Selon les codes fédéraux et cantonaux de procédure pénale³⁵, en effet, le recours à ces derniers instruments n'est pas limité à la poursuite d'infractions énumérées dans un catalogue réputé exhaustif³⁶, n'est pas soumis à une exigence de subsidiarité qualifiée³⁷, obéit à des exigences de proportionnalité moindres³⁸, s'avère possible sur la base d'une prévention plus ténue³⁹ et ne requiert pas l'approbation d'une autorité judiciaire⁴⁰. Délimiter les champs d'application respectifs de ces différentes mesures de contrainte ne relève donc pas d'un exercice purement académique, mais répond à un besoin pratique certain.

D'une manière générale, on admettra qu'une mesure de contrainte opérant en amont ou en aval de l'intervention d'un fournisseur de services postaux ne constitue pas une mesure de surveillance et échappe donc à la LSCPT et à l'OSCPT.

La mise sous main de justice, l'ouverture, la consultation et le versement éventuel au dossier d'un envoi (1) avant que son expéditeur (ou un tiers agissant pour lui) ne l'ait glissé dans une boîte aux lettres, déposé au guichet postal ou remis à un service de courrier rapide ou (2) après que son destinataire (ou son fondé de procuration,

34 *Infra* n° 81-94, 134, 147-173.

35 Voir par exemple les art. 65, 67 PPF, 46-49 DPA, 63-64, 66 PPM, 178-181 CPP.

36 Cf. art. 3 al. 2 let. a-f et al. 3 let. a-f LSCPT; *infra* n° 82.

37 Cf. art. 3 al. 1 let. c LSCPT; *infra* n° 91.

38 Cf. art. 3 al. 1 let. b LSCPT; *infra* n° 89.

39 Cf. art. 3 al. 1 let. a LSCPT; *infra* n° 98.

40 Cf. art. 179^{octies} al. 1 *in fine* CP et 7 al. 1 LSCPT; *infra* n° 134, 147-173.

un membre de sa famille, etc.) l'a reçu dans sa boîte aux lettres ou se l'est fait délivrer par un agent des services postaux, constituent dès lors une perquisition (ou un ordre de production) et une saisie.

17. La règle est identique s'agissant d'envois qui parviendraient par exemple à l'adresse d'un domicile postérieurement à sa mise sous scellés. Ce cas de figure démontre au passage que la perquisition et la saisie peuvent également revêtir certaines caractéristiques d'une mesure de contrainte «tournée vers l'avenir».
18. En revanche, le retrait au guichet postal par l'autorité de poursuite ou d'instruction pénale, moyennant la présentation de l'avis *ad hoc* laissé par l'agent postal, d'un courrier recommandé ou d'un colis inscrit adressé audit domicile placé sous scellés relève encore de la surveillance postale. Dans le cas d'espèce, la délivrance de l'envoi par le fournisseur de services postaux équivaut en effet à l'adoption (par son agent) d'un comportement constituant objectivement et subjectivement une violation du secret des postes selon l'art. 321^{ter} al. 1 CP, infraction toutefois justifiée par la loi conformément à l'art. 32 CP en liaison précisément avec la LSCPT et l'OSCPT⁴¹.
19. *De lege lata*, le critère tiré de l'existence ou non d'un agissement typiquement contraire l'art. 321^{ter} al. 1 CP est à mon sens le seul qui permette de distinguer la surveillance de la correspondance postale des autres mesures de contrainte sans devoir ouvrir la porte à une série d'exceptions qui tendraient rapidement à supplanter la règle⁴².
20. Selon ces principes, l'identification du titulaire d'une case postale se fera au moyen d'une simple demande de renseignements, accompagnée au besoin d'un ordre de production (d'une copie) des documents d'ouverture remis en son temps par l'intéressé.

41 Cf. art. 321^{ter} al. 5 CP.

42 Voir *infra* n° 33–38.

f) Renseignements sur les services de paiement

Non résolue sous l'empire de l'ancien droit, la question de savoir si 21. la remise aux autorités pénales de renseignements sur les services postaux de paiement nécessitait ou non le recours à une mesure de surveillance a reçu du législateur fédéral une réponse à juste titre négative. L'obtention de renseignements sur les services de paiement soumis à la Loi fédérale sur la poste⁴³ est expressément exclu du champ d'application de la LSCPT⁴⁴. Il n'y a en effet aucune raison de soumettre aux conditions restrictives de cette dernière l'obtention de pièces et d'informations relatives au trafic des paiements opérés via un compte de chèque postal, alors que ces mêmes données sont délivrées par les banques sur la base d'une (simple) ordonnance de perquisition (ou de production) et de saisie décernée selon le code de procédure pénale applicable.

2 *Surveillance de la correspondance par télécommunication, accès à Internet compris*

a) Notion de correspondance par télécommunication, accès à Internet compris

La correspondance par télécommunication consiste dans l'émission 22. ou la réception d'informations⁴⁵ transmises au moyen de techniques de télécommunication⁴⁶ par le truchement d'installations de télécommunication⁴⁷. Ces informations peuvent prendre la forme de sons⁴⁸

⁴³ Cf. art. 1 al. 2 phr. 1, 9 al. 1 let. a LPO; voir aussi les art. 4 al. 1 let. d, 6, 8 OPO.

⁴⁴ Art. 1 al. 3 LSCPT.

⁴⁵ Art. 3 let. a LTC.

⁴⁶ Art. 3 let. c LTC.

⁴⁷ Art. 3 let. d LTC.

⁴⁸ Il s'agira principalement de la parole.

ou la forme de données⁴⁹, transmis entre des installations d'usagers fixes⁵⁰ ou mobiles⁵¹.

23. Défini plus largement qu'en matière de surveillance de la correspondance postale⁵², le champ d'application personnel de la LSCPT vise les fournisseurs de services de télécommunication⁵³ «soumis à concession ou à l'obligation d'annoncer»⁵⁴. Le régime de la concession concerne les opérateurs qui exploitent «de manière indépendante une partie importante des installations de télécommunication»⁵⁵; parmi ceux-ci, on trouvera notamment Swisscom, Orange et Sunrise. Les autres prestataires de services sont seulement soumis à l'obligation de s'annoncer auprès de l'Office fédéral de la communication⁵⁶; ceci vaut par exemple pour les fournisseurs d'accès à Internet, inutilement mentionnés à l'art. 1 al. 2 *in fine* LSCPT⁵⁷. Le Conseil fédéral peut toutefois exclure des deux mécanismes précités, donc soustraire à la LSCPT, les fournisseurs de «services de télécommunication de faible importance économique et impliquant peu de moyens techniques»⁵⁸.
24. Quant aux exploitants de réseaux de télécommunication internes ou de centraux domestiques⁵⁹, qui échappent en tant que tels à la LSCPT⁶⁰, ils sont exclusivement tenus de tolérer la mise en oeuvre

49 Ainsi en cas d'envoi et/ou de réception d'une télécopie, d'un texte court sur un pageur ou bipeur, d'instructions données du clavier téléphonique à un serveur vocal, d'un SMS, d'un MMS, d'un e-mail, etc.

50 Téléphone fixe, relié par fil au réseau fixe; téléphone sans fil (radio-téléphone), composé d'un combiné mobile communiquant par voie hertzienne dans un rayon maximal de 300m avec une station de base reliée par fil au réseau fixe; télécopieur; ordinateur personnel, moyennant sa liaison au réseau (fixe ou mobile) par un modem; etc.

51 Téléphone mobile ou portable (natel dans le jargon suisse); pageur ou bipeur; etc.

52 *Supra* n° 3.

53 Art. 3 let. b LTC.

54 Art. 1 al. 2 LSCPT.

55 Art. 4 al. 1 LTC.

56 Art. 4 al. 2 LTC.

57 Cf. HANSJAKOB, Art. 1 BÜPF n° 12.

58 Art. 4 al. 3 LTC; pour une illustration potentielle, voir l'art. 3 al. 2 OST.

59 Cf. à ce propos l'art. 2 OST, qui mentionne la transmission d'informations à l'intérieur d'un bâtiment (let. a), sur un bien-fonds, sur deux biens-fonds contigus ou sur deux biens-fonds opposés, séparés par une route, une rue, un chemin, une ligne ferroviaire ou un cours d'eau (let. b), au sein d'une entreprise, entre la société-mère et les filiales ou au sein d'un groupe (let. c).

60 Art. 2 OST *cum* art. 1 al. 2 LSCPT.

d'une mesure de surveillance sur leurs installations⁶¹. Seule une surveillance en temps réel⁶² est ici concevable dès lors que les intéressés n'ont aucune obligation légale de conserver les données qu'ils ont acheminées par le passé ou qui seraient nées à l'occasion d'un tel acheminement⁶³. Le champ délaissé par la surveillance rétroactive⁶⁴ est ici repris par la perquisition (ou l'ordre de production) et la saisie, à la différence près que ces instruments permettent aux autorités de poursuite et d'instruction pénale d'accéder également au contenu des communications échangées dans la mesure où ces dernières existent encore. A l'inverse de ce qui vaut en cas d'utilisation de réseaux de télécommunication «externes»⁶⁵, un juge d'instruction ou un procureur est notamment fondé à se faire remettre ou aller chercher puis saisir les e-mails échangés en interne par le personnel d'une administration ou d'une entreprise et stockés sur les serveurs de ces dernières⁶⁶.

b) Objet de la surveillance

L'objet de la surveillance peut être un raccordement⁶⁷ à un réseau fixe **25.** 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, tous trois indissociablement liés), un téléphone mobile (identifiable par son numéro IMEI) ou encore une boîte aux lettres électronique auprès d'un fournisseur d'accès à Internet (identifiable par son adresse e-mail).

Comme en matière de surveillance de la correspondance par poste⁶⁸, **26.** la mesure ne vise pas une personne déterminée. La surveillance de la

61 Art. 1 al. 4 LSCPT; sur le contenu de cette obligation, voir *infra* n° 65.

62 *Mutatis mutandis*, voir *infra* n° 27.

63 L'art. 15 al. 3 LSCPT leur est notamment inapplicable.

64 *Mutatis mutandis*, voir *infra* n° 28–29.

65 *Infra* n° 31–32.

66 Cf. YASMIN IQBAL, Zugriff auf elektronische Post – E-Mails sollen in Strafverfahren herausverlangt werden, *NZZ* 53/5.3.2003 p. 15. L'auteur évoque l'instruction pénale conduite par les autorités zurichoises contre d'anciens organes du SAirGroup.

67 Cf. art. 4 al. 1 *in fine*, 4 al. 2, 4 al. 4, 10 al. 2 let. b LSCPT; voir aussi l'art. 3 al. 4 LSCPT.

68 *Supra* n° 4–5.

correspondance par télécommunication, accès à Internet compris, est donc elle aussi une mesure «réelle» et non pas «personnelle». Ici aussi, tout changement de raccordement, de téléphone portable ou d'adresse électronique requiert l'instauration d'une nouvelle mesure de surveillance pour que les correspondances transitant par les nouvelles installations terminales soient (également) interceptées⁶⁹.

c) *Surveillance en temps réel*

27. La surveillance en temps réel⁷⁰ de la correspondance par télécommunication représente ici aussi la forme classique, c'est-à-dire prospective, de la mesure. Elle consiste, alternativement ou cumulativement, dans la transmission aux organes exécutant la surveillance des informations suivantes:

- le contenu des télécommunications⁷¹ transitant (à l'entrée ou à la sortie) par le raccordement ou le téléphone mobile surveillés⁷²;
- la position et de la direction d'émission des antennes de téléphonie mobile avec lesquelles le téléphone portable – s'il est enclenché – de la personne surveillée est relié⁷³, la personne surveillée (ou du moins son téléphone) pouvant ainsi être suivie à la trace dans ses déplacements et localisée (*location update, tracing*);
- les paramètres qui caractérisent une correspondance par télécommunication et permettent (notamment) d'identifier les correspondants, à savoir les numéros appelant et appelé, la destination d'un appel dévié ou transféré ainsi que les numéros intermédiaires utilisés, les signaux émis par le raccordement surveillé, les caractéristiques des installations terminales (notamment les numéros SIM, IMSI et IMEI pour un téléphone mobile), la position et la direction d'émission des antennes de téléphonie mobile activées, enfin la date, l'heure et la durée de la correspondance, et cela quand bien même la communication n'a pas été établie⁷⁴;

69 Cf. art. 4 al. 4 LSCPT; *infra* n° 163.

70 Art. 3, 4, 5 al. 1 let. a LSCPT.

71 Il s'agit des informations dites utiles, selon la définition qu'en donne l'art. 2 let. f OSCPT.

72 Art. 16 let. a OSCPT.

73 Art. 16 let. b OSCPT.

74 Art. 16 let. c OSCPT.

- le contenu des e-mails arrivés dans ou expédiés depuis la boîte aux lettres électronique surveillée, ainsi que les fichiers informatiques éventuellement attachés au message⁷⁵;
- les paramètres qui caractérisent une correspondance par e-mail et permettent (notamment) d'identifier les correspondants, à savoir la date et l'heure de réception ou d'envoi du message dans/ depuis la boîte aux lettres électronique surveillée, les informations de l'enveloppe (ressources d'adressage) et les informations figurant en en-tête, singulièrement les adresses IP de (l'équipement de) l'expéditeur et du destinataire⁷⁶;
- les paramètres qui caractérisent les accès à Internet opérés pour consulter les e-mails arrivés dans la boîte aux lettres électronique surveillée et permettent (notamment) d'identifier les correspondants, à savoir la date et l'heure de la consultation, l'adresse IP de la source et le protocole utilisé⁷⁷.

d) Surveillance rétroactive

A l'instar de ce qui vaut en matière de surveillance de la correspondance par poste⁷⁸, la surveillance dite rétroactive des télécommunications, accès à Internet compris, permet aux autorités de poursuite et d'instruction d'obtenir certaines données recueillies puis conservées un temps déterminé⁷⁹ par les fournisseurs de services de télécommunication à l'occasion d'interconnections établies dans le passé, c'est-à-dire avant qu'un ordre de surveillance n'ait été délivré.

De par la loi, ces données concernent à nouveau le trafic et la facturation⁸⁰. En cas de surveillance rétroactive des télécommunications, il s'agira des numéros appelant et appelé (s'ils sont connus de l'opérateur), des caractéristiques des installations terminales (notamment les numéros SIM, IMSI et IMEI pour un téléphone mobile), la posi-

75 Art. 24 let. a ch. 2 et 4, 24 let. d ch. 2 et 4 OSCPT.

76 Art. 24 let. a ch. 1 et 3, 24 let. b, 24 let. d ch. 1 et 3, 24 let. e OSCPT.

77 Art. 24 let. c OSCPT.

78 *Supra* n° 12.

79 *Infra* n° 62 cum 63, 94.

80 Art. 5 al. 1 let. b LSCPT.

tion et la direction d'émission des antennes de téléphonie mobile avec lesquelles le téléphone portable de la personne surveillée était relié au moment de la communication, enfin la date, l'heure et la durée de la correspondance⁸¹. En cas de surveillance rétroactive des accès à Internet, l'ordonnance distingue selon que les données susceptibles d'être fournies concernent l'attribution dynamique des adresses IP⁸², les accès eux-mêmes⁸³ ou l'envoi et la réception d'e-mails⁸⁴; pour le détail des nombreuses informations susceptibles d'être communiquées, on voudra bien se reporter aux dispositions précitées, trop fournies pour être ici restituées.

30. La question de savoir si les recherches par champ d'antennes (*Antennensuchläufe*), c'est-à-dire l'établissement d'une liste de toutes les communications ayant transité par des antennes de téléphonie mobile déterminées (celles qui se situent à proximité du lieu de commission de l'infraction) durant une plage de temps déterminé (celle précédent et suivant le moment de commission de l'infraction), sont ou non juridiquement admissibles est fortement controversée en l'état. D'une part, il ne fait aucun doute que les données considérées relèvent du «trafic» au sens de l'art. 5 al. 1 let. b LSCPT. D'autre part, il est tout aussi manifeste que l'art. 16 OSCPT ne mentionne pas une telle mesure et que l'objet de la surveillance, à savoir un raccordement ou un téléphone portable déterminés ou déterminables grâce aux renseignements accessibles⁸⁵, fait ici défaut⁸⁶.
31. *De iure*, l'accès au contenu de la correspondance⁸⁷ est exclu. *De facto*, c'est-à-dire du point de vue technique, cet accès serait pourtant possible s'agissant par exemple

81 Art. 16 let. d OSCPT.

82 Art. 24 let. f OSCPT.

83 Art. 24 let. g OSCPT.

84 Art. 24 let. h OSCPT.

85 Art. 14 LSCPT; art. 19–22 OSCPT.

86 Sur l'ensemble de la question, voir HANSJAKOB, Art. 16 VÜPF n° 14–19; IDEM, *Erfahrungen* 274–275.

87 *Supra* note 71.

- d'un SMS enregistré chez le fournisseur de services de télécommunication de son destinataire dans l'attente que ce dernier enclenche son téléphone mobile, provoquant de la sorte le transfert du SMS sur son appareil et son effacement chez le fournisseur de services de télécommunication;
- d'un message envoyé sur le pageur (bipeur) de son destinataire, le fournisseur de services de télécommunication de ce dernier le conservant environ deux semaines;
- d'un message laissé sur la boîte vocale (ComBox) de son destinataire dans l'attente que ce dernier la consulte et écoute le message, provoquant de la sorte son effacement chez l'opérateur de télécommunication;
- d'un e-mail enregistré chez le fournisseur d'accès à Internet de son destinataire (non titulaire d'une adresse IP permanente) dans l'attente que ce dernier se connecte à lui et consulte sa boîte aux lettres électronique, provoquant de la sorte le transfert du message sur son ordinateur et son effacement chez le fournisseur d'accès à Internet.

Cette incapacité de la loi à appréhender les états de fait précités ne **32.** résulte pas d'une volonté délibérée du législateur, mais d'une méconnaissance par celui-ci des données techniques. Le constat est d'autant plus irritant que ces mêmes informations sont accessibles aux autorités pénales lorsque la communication emprunte un réseau interne⁸⁸. Une telle différence de traitement est parfaitement injustifiable.

e) Délimitation par rapport à la perquisition, l'ordre de production et la saisie

Conformément au critère retenu à l'enseigne de la surveillance de la **33.** correspondance postale (adoption par un fonctionnaire, un employé ou un auxiliaire d'un organisme fournissant des services de télécommunication d'un comportement typiquement contraire l'art. 321^{ter} al.

88 *Supra* n° 24.

1 CP)⁸⁹, les dispositions gouvernant la perquisition (l'ordre de production) et la saisie s'avèrent seules applicables lorsque l'autorité pénale compétente actionne adéquatement⁹⁰

- un téléphone afin d'identifier le ou les derniers numéros appellants ou appelés (s'ils n'ont pas été effacés), d'accéder au carnet électronique d'adresses qu'il renferme, etc.;
- un répondeur automatique afin d'écouter et de transcrire les messages enregistrés;
- un télécopieur afin d'imprimer les documents reçus ou envoyés et qui sont (encore) stockés dans sa mémoire;
- un téléphone portable (enclenché ou dont le code PIN est connu) afin de faire apparaître et de relever les SMS précédemment reçus, envoyés ou composés en vue d'envoi et qui sont (encore) enregistrés sur la carte SIM;
- un ordinateur dont la messagerie est ouverte afin de faire apparaître et d'imprimer les e-mails reçus ou envoyés, dans la mesure où ils n'ont pas été effacés.

34. Peu importe à nouveau que l'installation terminale reçoive encore des correspondances postérieurement à sa mise sous main de justice. Pour donner un exemple tiré de la pratique, la commande d'héroïne ou de cocaïne qui arrive sur le pageur (bipeur) d'un individu prévenu d'infractions à l'art. 19 LStup pendant son interrogatoire à la police est naturellement sujette à saisie et exploitable conformément aux prescriptions régissant dans ce domaine la découverte fortuite de charges.

35. Le contexte juridique n'est pas davantage modifié si – les mots de passe requis étant connus d'eux – les enquêteurs doivent commencer

89 *Supra* n° 19.

La seule réserve concerne le cas, atypique en soi (cf. *supra* n° 24), de l'exploitant d'un réseau de télécommunication interne ou d'un central domestique qui tolère la mise en oeuvre d'une surveillance (en temps réel) à partir de son installation. Emanant d'un auteur impossible (*extraneus*), un tel comportement échappe à l'art. 321^{er} al. 1 (*in fine*) CP.

90 Cf. HANSJAKOB, *Vorbemerkungen zum BÜPF* n° 16–23, qui parvient pour l'essentiel à des résultats identiques.

par établir une liaison avec l'opérateur de téléphonie mobile ou le fournisseur d'accès à Internet, ce dernier acheminant à cet instant seulement vers l'installation terminale les messages laissés sur une ComBox, les SMS entrés et les e-mails déposés dans la boîte aux lettres électronique.

Enfin, le recours à un ordre de production suivi d'une saisie demeure encore la voie procédurale à suivre si, préalablement aux opérations sus-décrivées, il s'agit pour les organes de poursuite et d'instruction d'obtenir de l'opérateur de téléphonie mobile le code PUK permettant de déverrouiller la carte SIM d'un téléphone portable, ou encore du fournisseur d'accès à Internet le mot de passe permettant d'établir la connexion à ses installations et d'ouvrir une boîte aux lettres électronique⁹¹.

Dans toutes les hypothèses susmentionnées, le fournisseur de services de télécommunication n'intervient pas du tout ou se borne à révéler une information (un code ou un mot de passe) qui ne tombe pas sous le secret des télécommunications ancré à l'art. 43 LTC et protégé par l'art. 321^{ter} CP. Pour la même raison, l'autorité judiciaire procédera par voie d'ordre de production si elle entend obtenir d'un opérateur l'original ou la copie du contrat le liant à un abonné, les numéros SIM et IMSI liés à un raccordement qu'il exploite, le numéro IMEI du téléphone portable connecté à un tel raccordement ou encore le numéro d'appel «rechargé» au moyen d'une carte à prépaiement de la téléphonie mobile⁹².

Sous l'empire du régime précédent l'entrée en vigueur de la LSCPT 38. et de l'OSCPT, le Tribunal fédéral avait déjà jugé qu'une mesure de surveillance commençait là où il y avait intrusion dans le secret des télécommunications⁹³, bannissant ainsi d'un trait de plume la pratique pourtant suivie jusqu'alors par de nombreux cantons, notam-

91 HANSJAKOB, *Erfahrungen* 266–267, 268–269. *Contra:* BIEDERMANN 105.

92 *Ibidem.*

93 ATF 126 I 60–64 consid. 5, avec de nombreuses références à la doctrine. *Adde:* OBERHOLZER 4.

ment romands⁹⁴, et selon laquelle la remise de données rétroactives relatives au trafic et à la facturation pouvait être obtenue au moyen d'un simple ordre de production. D'autres critères de délimitation ne sont pas ou plus compatibles avec le droit positif. Autrefois préconisée, une distinction fondée sur la nature prospective ou rétrospective de la mesure de contrainte se heurte aujourd'hui à l'art. 5 LSCPT; on a d'ailleurs pu observer que la perquisition et la saisie pouvaient déployer certains effets *pro futuro*⁹⁵. De même, il ne me paraît pas possible de caractériser la mesure de surveillance par le secret qui l'entourerait⁹⁶; d'une part, il existe des situations dans lesquelles l'enregistrement des conversations passant par un raccordement téléphonique se fera au su (fût-ce par «dol éventuel») de tous les interlocuteurs, par exemple lorsqu'un preneur d'otage appelle la famille de la victime pour lui faire part de ses exigences financières; d'autre part, un ordre de production suivi d'une saisie peuvent également être frappés de confidentialité, ainsi lorsque ces mesures sont signifiées à une banque et assorties de l'injonction – sous menace des peines prévues à l'art. 292 CP – de ne pas dévoiler leur existence au client de l'établissement.

39. *De lege ferenda*, singulièrement dans le contexte de l'élaboration d'une procédure pénale suisse unifiée, on doit toutefois se demander si les très restrictives conditions de fond (singulièrement l'existence d'une infraction cataloguée⁹⁷) et de forme (soit l'approbation judiciaire⁹⁸) posées par la LSCPT à la mise en oeuvre d'une mesure de surveillance sont nécessaires lorsque la justice pénale ne s'intéresse pas au contenu de la correspondance par poste ou télécommunication, mais exclusivement aux autres paramètres existants, désormais appréhendés par l'art. 5 LSCPT⁹⁹. De mon point de vue, la protection juridique offerte en la matière par les dispositions gouvernant la

94 Cf. toutefois RJB 132 (1996) 624–625.

95 *Supra* n° 17.

96 HANSJAKOB, *Vorbemerkungen zum BÜPF* n° 14.

97 *Infra* n° 82.

98 *Infra* n° 134, 147–173.

99 A ce propos, voir la remarquable opinion dissidente publiée en annexe à ZR 98 (1999) n° 1, p. 2–6.

perquisition, l'ordre de production et la saisie, d'une part, le témoignage, d'autre part, est amplement suffisante.

f) Renseignements sur les raccordements de télécommunication et les usagers d'Internet

Bien que la demande de renseignements sur les raccordements de télécommunication ou les usagers d'Internet soit réglementée par la LSCPT et l'OSCPT¹⁰⁰, elle ne constitue pas pour autant une mesure de surveillance.

Sur le fond, une telle demande doit donc être exécutée alors même que l'infraction faisant l'objet de la poursuite pénale ne figurerait pas au catalogue légal, ne présenterait pas le degré de gravité requis ou commanderait le recours préalable à d'autres mesures d'investigation¹⁰¹. En la forme, elle ne doit pas nécessairement émaner d'un juge d'instruction ou d'un procureur, mais peut notamment provenir de divers organes de police¹⁰², et n'est pas soumise à l'approbation d'une autorité judiciaire¹⁰³.

Une demande de renseignements sur les raccordements sera généralement connexe à une mesure de surveillance de la correspondance par télécommunication¹⁰⁴, la précédent afin d'identifier les raccordements dont la personne visée est le titulaire¹⁰⁵, la suivant afin d'identifier les titulaires d'un raccordement dont le numéro apparaît au cours de la surveillance¹⁰⁶. Toutefois, une demande de renseignements sur les raccordements de télécommunication se conçoit aussi isolément, par exemple s'il s'agit uniquement de connaître le nom et l'adresse, voire la profession, du titulaire d'un raccordement qui a été utilisé pour proférer des menaces¹⁰⁷ téléphoniques et dont le nu-

100 Art. 14 LSCPT; art. 19–22, 27 OSCPT.

101 Cf. successivement les art. 3 al. 2–3, 3 al. 1 let. b, 3 al. 1 let. c LSCPT; *infra* n° 82, 89–90, 91–92.

102 Art. 14 al. 2 let. b LSCPT; art. 22 al. 1 OSCPT.

103 Cf. art. 179^{octies} al. 1 *in fine* CP et 7 al. 1 LSCPT; *infra* n° 134, 147–173.

104 Cf. art. 14 al. 2 let. a *in fine* LSCPT.

105 Art. 19 al. 1 let. a OSCPT.

106 Art. 19 al. 1 let. b OSCPT.

107 Art. 180 CP.

méro d'appel s'est affiché sur l'écran de l'appareil de destination¹⁰⁸. D'une manière générale, la délivrance de renseignements sur les raccordements de télécommunication permet de combler les lacunes qui, au gré de la volonté de chaque abonné d'y figurer ou non¹⁰⁹, émaillent les registres publics, annuaires téléphoniques en tête, lesquels n'indiquent pas non plus avec quel opérateur le contrat a été passé.

43. Les mêmes considérations motiveront une demande de renseignements sur les usagers d'Internet¹¹⁰ si la correspondance intéressant l'autorité judiciaire s'effectue par courrier électronique. Pour autant que les fournisseurs d'accès disposent de ces informations, l'adresse e-mail d'un usager déterminé ou, inversement, le nom, l'adresse et la profession du titulaire d'une adresse e-mail donnée pourront ainsi être obtenus.
44. Lorsqu'une infraction a été commise au moyen d'Internet¹¹¹, par exemple si des propos diffamatoires¹¹² ont été adressés à un tiers par e-mail, le fournisseur d'accès est tenu de révéler à qui a été attribuée l'adresse IP utilisée pour l'envoi (cette donnée figure dans l'en-tête du message reçu) et quel est le numéro d'appel du raccordement employé pour établir la connexion à ses installations. Idéalement, ces indications permettront de remonter à l'auteur du délit.

3 *Addendum: utilisation d'appareils techniques de surveillance*

a) *Remarque préalable*

45. Lorsque l'on évoque la surveillance de la correspondance par poste et télécommunication, il n'est pas possible de passer sous silence le

108 Téléphone portable ou téléphone fixe dûment équipé et connecté à une ligne ISDN, si l'appelant n'a pas fait occulter l'identification de sa ligne (cf. art. 61 OST).

109 Art. 21 al. 3 LTC; cf. aussi l'art. 65 OST.

110 Art. 27 OSCPT.

111 Art. 14 al. 4 LSCPT.

112 Art. 173 CP.

troisième type de mesure de surveillance que connaît le droit suisse, celui que la loi appelle l'utilisation d'appareils techniques de surveillance¹¹³. Ce domaine revêt dans la pratique une importance bien moindre que la surveillance de la correspondance par poste et télécommunication. S'il convient néanmoins de le mentionner ici, c'est en raison de la technique législative communément choisie pour le réglementer.

Avant l'entrée en vigueur de la LSCPT, les codes fédéraux et cantonaux de procédure pénale soumettaient la mise en oeuvre des trois types de mesures de surveillance à des conditions identiques. En reprenant aux cantons la compétence législative en matière de surveillance de la correspondance par poste et télécommunication, la Confédération leur a laissé celle relative à l'utilisation d'appareils techniques de surveillance¹¹⁴. D'un point de vue strictement juridique, rien n'interdirait aux cantons de conserver en la matière leurs anciennes règles de procédure ou de créer un système original. En réalité, l'économie législative leur commande de renvoyer à la LSCPT, singulièrement à ses art. 3–4 et 6–10, afin de rétablir l'uniformité du régime des mesures de surveillance. Le législateur fédéral a lui-même tracé la voie en prévoyant aux art. 66 al. 2 PPF et 70 phr. 2 PPM que la LSCPT s'applique par analogie à l'utilisation d'appareils techniques de surveillance¹¹⁵. Le canton de Genève a suivi l'exemple¹¹⁶.

b) Notion d'utilisation d'appareils techniques de surveillance

L'art. 179^{octies} al. 1 CP définit l'utilisation d'appareils techniques de surveillance par un simple renvoi aux art. 179^{bis} et suivants CP. Ce renvoi signifie que le champ des mesures de surveillance effectuées au moyen d'appareils techniques correspond à celui des comporte-

¹¹³ Sur l'ensemble de la question, voir PETER GOLDSCHMID, *Der Einsatz technischer Überwachungsgeräte im Strafprozess, Unter besonderer Berücksichtigung der Regelung im Strafverfahren des Kantons Bern*, Bern 2001.

¹¹⁴ Cf. CONSEIL FÉDÉRAL 3703, 3705.

¹¹⁵ Cf. HANSJAKOB, *Erfahrungen* 272, qui signale une réglementation similaire dans le canton de St. Gall. Pour un contre-exemple, celui du canton de Thurgovie, voir BIEDERMANN 93–94.

¹¹⁶ Art. 48B LACP, 184B et 190C al. 2 CPP, dans leur teneur selon la loi n° 8732 du 16 mai 2003 (FAO 57/23.5.2003 p. 23–24).

ments incriminés par les dispositions précitées. L'art. 179^{octies} al. 1 CP intervient donc si la mesure ordonnée est en soi prohibée par les art. 179^{bis}–179^{quater} CP¹¹⁷. Si tel n'est pas le cas, il n'y a pas de surveillance au moyen d'appareils techniques; en conséquence, la mesure d'investigation échappe non seulement à la nécessité d'une approbation judiciaire immédiate, mais aussi aux règles fédérales ou cantonales de procédure pénale édictées en exécution de l'art. 179^{octies} al. 1 CP.

48. Autre est la question de savoir si de telles «mesures de surveillance pénallement atypiques» ne requièrent pas néanmoins une base légale, soit parce qu'elles portent atteinte à une liberté publique¹¹⁸, soit parce que l'activité étatique considérée mérite d'être canalisée. Dans le contexte de l'unification de la procédure pénale en Suisse, le débat est lancé s'agissant par exemple de la filature, de l'observation à la jumelle ou de la prise de vues sur le domaine public.
49. La limitation de la protection pénale offerte par les art. 179^{bis}–179^{quater} CP, donc du champ d'application de la surveillance au moyen d'appareils techniques, résulte de la définition de l'événement considéré et de l'outil utilisé¹¹⁹.
50. A l'enseigne des art. 179^{bis} et 179^{ter} CP, la loi requiert une conversation non publique, d'une part, un appareil d'écoute ou un porteur de son, d'autre part. Le comportement réprimé consiste dans l'écoute ou l'enregistrement de la conversation considérée. La notion d'appareil d'écoute regroupe tous les instruments permettant de capter des sons, singulièrement ceux imperceptibles à l'«oreille nue», du stéthoscope appliqué sur le mur mitoyen au micro directionnel à laser, en passant par le micro-espion (*Wanze*). La notion de porteur de

117 NIKLAUS OBERHOLZER, *Grundzüge des Strafprozessrechts, Dargestellt am Beispiel des Kantons St. Gallen*, Bern 1994, p. 391; NIKLAUS SCHMID, *Strafprozessrecht, Eine Einführung auf der Grundlage des Strafprozessrechtes des Kantons Zürich und des Bundes*, 3. Auflage, Zürich 1997, n° 762.

118 Art. 36 Cst.

119 L'absence de consentement (*recte d'accord*) des personnes touchées par la surveillance est ici irrelevante car les bases légales régissant les mesures de contrainte existent notamment pour pallier le défaut d'assentiment du lésé.

sons recouvre tous les supports d'enregistrement de sons, par exemple les bandes magnétiques, les puces électroniques, les disquettes informatiques ou les CD-ROM.

Sous l'angle de l'art. 179^{quater} CP, la loi requiert un fait relevant du 51. domaine secret ou un fait relevant du domaine privé ne pouvant pas être perçu «sans autre» par chacun, d'une part¹²⁰, un appareil de prise de vues et un porteur d'images, d'autre part. L'agissement incriminé consiste dans l'observation ou la fixation du fait précité. Parmi les appareils de prises de vues, on trouvera, même s'ils ne servent *in concreto* qu'à l'observation, les appareils photographiques et les caméras, numériques (enregistrement sur support électronique) ou analogiques (enregistrement sur pellicule), notamment (mais pas nécessairement) équipés d'un téléobjectif. Les jumelles, longues-vues, périscopes, lunettes et autres miroirs sans tain ne sont en revanche pas appréhendés¹²¹.

A la lumière des exigences précitées, ne constituent pas une utilisation d'appareils techniques de surveillance la simple filature d'un individu sur le domaine public¹²², la confection d'un film vidéo restituant une scène se déroulant sur la voie publique devant un restaurant¹²³, l'écoute à l'«oreille nue» d'une conversation de bistrot depuis une table voisine avec transcription des propos perçus dans un carnet de notes, ou encore la surveillance par caméras vidéo opérant le long des autoroutes (notamment dans les tunnels), aux carrefours routiers et en zones piétonnes. Par identité de motifs, la surveillance vidéo effectuée dans les magasins, dans le hall des banques et des bureaux de poste ou devant les distributeurs automatiques de billets échappent à l'art. 179^{quater} CP.

120 Cf. ATF 118 IV 44–51 consid. 3–5.

121 ATF 117 IV 33–34 consid. 2b–c.

122 Cf. OCA 45/7.2.1997 Fernandez Estrada consid. 4.

123 ZR 95 (1996) n° 70 consid. V.3.

c) Objet de la surveillance

53. En fonction des besoins de son instruction, le magistrat compétent devrait pouvoir façonner la mise en oeuvre d'appareils techniques de surveillance de manière «personnelle» ou «réelle»¹²⁴, selon qu'il s'agit par exemple de surveiller les propos et comportements que tient un individu déterminé ou ceux qu'abrite un lieu déterminé.

d) Nature de la surveillance

54. De par sa nature même, l'utilisation d'appareils techniques de surveillance est une mesure prospective, tournée vers l'avenir. Elle ne se conçoit donc qu'«en temps réel».

e) Délimitation par rapport à d'autres mesures de contrainte

55. Relevant de dispositions telles que les art. 73^{quater} PPF ou 18 al. 1–2 LPol, la prise de photographies d'un prévenu ou d'un tiers, pour les besoins de leur identification, se distingue nettement et sans peine de l'utilisation d'appareils techniques de surveillance par son objet.
56. La délimitation par rapport à la perquisition, l'ordre de production et la saisie ne devrait en principe pas poser non plus de problèmes, compte notamment tenu de la nature prospective de l'utilisation d'appareils techniques de surveillance. Ressortissent ainsi clairement à la première catégorie la mainmise judiciaire sur
- l'enregistrement télévisuel d'un match de football au cours duquel un joueur inflige une lésion corporelle à l'un de ses adversaires¹²⁵;
 - l'enregistrement vidéo d'un accident de la circulation par des caméras de surveillance du trafic routier¹²⁶;
 - l'enregistrement vidéo des faits et gestes de personnes pénétrant dans le champ des caméras placées dans les magasins, les halls de

124 Cf. *supra* n° 5, 22.

125 SJ 1987 p. 123 consid. 4.

126 Dans la mesure où l'enregistrement est effectué par un service de l'Etat, singulièrement la police routière, l'apport à la procédure pénale du film vidéo s'effectuera conformément aux règles sur l'entraide judiciaire dès lors que l'Etat ne saurait exercer des mesures de contrainte sur lui-même (cf. à ce propos l'ATF 129 IV 144 consid. 2.2).

banque ou de bureaux de poste, aux abords de bancomats ou de postomats, etc.;

- des photographies ou des films privés se trouvant en possession de l'auteur d'une infraction, du lésé ou d'un tiers;
- etc.

Il en ira de même avec la confection par l'autorité de poursuite ou **57.** d'instruction pénale de photographies destinées à documenter les traces d'une infraction retrouvées par exemple dans un domicile ou sur un corps humain, vivant ou décédé.

On peut hésiter quant à la qualification de la mesure de contrainte **58.** lorsque l'utilisation d'un appareil technique vient se greffer sur une installation terminale de télécommunication, par exemple en cas

- de fixation sur un téléphone (fixe ou mobile) d'un micro-ventouse relié à un enregistreur audio et captant les conversations passant par le raccordement;
- d'installation dans un téléphone (fixe ou mobile) d'un micro-espion transmettant les conversations passant par le raccordement;
- de programmation du téléphone portable de la personne surveillée de sorte que son micro fonctionne en permanence et transmette tous les sons qu'il capte;
- de pose d'une caméra au domicile ou sur le lieu de travail de la personne surveillée de telle manière que l'écran de son ordinateur se trouve dans le champ de vision.

Parce que ces procédés ne requièrent pas l'intervention d'un opérateur de télécommunication ni l'adoption par celui-ci d'un comportement typiquement contraire à l'art. 321^{ter} al. 1 CP¹²⁷, mais se bornent à exploiter ses prestations, ils relèvent exclusivement de l'utilisation d'appareils techniques de surveillance¹²⁸.

127 *Supra* n° 19, 33, 37.

128 JEAN-RICHARD-DIT-BRESSEL 44 note 27. *Contra: HANSJAKOB, Vorbemerkungen zum BÜPF* n° 48.

B Obligations corrélatives

60. Pour que les diverses mesures de surveillance détaillées ci-dessus puissent porter leurs fruits, les autorités judiciaires et administrative¹²⁹ compétentes doivent pouvoir compter sur la collaboration des différents prestataires de services postaux et de télécommunication. La loi s'attache donc à définir leurs devoirs procéduraux.

1 Obligations des fournisseurs de services postaux

61. Dans le cadre d'une surveillance en temps réel, les fournisseurs de services postaux ont l'obligation juridique de retenir les envois dirigés vers l'adresse surveillée, d'informer l'autorité qui a ordonné la mesure (ou ses services de police) de l'interception, de tenir les plis, les colis, etc. à sa disposition et, cas échéant, de lui remettre les données qui caractérisent l'envoi ainsi que les renseignements complémentaires sur la correspondance¹³⁰. Il incombe aux entreprises concernées de prendre les dispositions organisationnelles que l'exécution rapide de ces opérations nécessite, y compris la mise en place d'un service de piquet¹³¹.
62. Afin de pouvoir répondre à une surveillance rétroactive, les fournisseurs de services postaux sont tenus de conserver pendant 6 mois au moins les données relatives au trafic et à la facturation¹³². Nantis d'un ordre correspondant, ils doivent communiquer les informations sollicitées à l'autorité judiciaire requérante.

129 *Infra* n° 67, 126–128, 147–150.

130 Art. 12 al. 1 LSCPT; cf. *supra* n° 7–9; pour les détails, voir HANSJAKOB, Art. 12 BÜPF n° 2–5.

131 Art. 14 OSCPT; pour les détails, voir HANSJAKOB, Art. 14 VÜPF n° 1–3.

132 Art. 12 al. 2 LSCPT; cf. *supra* n° 12–13; pour les détails, voir HANSJAKOB, Art. 12 BÜPF n° 6–8.

2 *Obligations des fournisseurs de services de télécommunication et des fournisseurs d'accès à Internet*

Toutes choses égales d'ailleurs, les obligations précitées lient également les fournisseurs de services de télécommunication et les fournisseurs d'accès à Internet, à cette différence près que les opérateurs concernés en réfèrent ici au Service de surveillance¹³³ et non pas directement à l'autorité judiciaire qui a ordonné la mesure. **63.**

Pas moins de vingt-neuf alinéas sont consacrés à la définition de ces différents devoirs, pour le détail desquels on voudra bien se reporter à la loi¹³⁴ et à l'ordonnance¹³⁵. **64.**

3 *Obligations des exploitants de réseaux de télécommunication internes et de centraux domestiques*

Parce qu'ils ne sont pas réputés fournir un service de télécommunication, les exploitants de réseaux de télécommunication internes et de centraux domestiques sont uniquement tenus de tolérer la surveillance¹³⁶. Concrètement, ils doivent garantir aux agents mandatés par le Service de surveillance l'accès à leurs installations et fournir à ces personnes les renseignements nécessaires à la mise en place de la mesure¹³⁷. **65.**

133 *Infra* n° 67.

134 Art. 15 al. 1–7 LSCPT; voir HANSJAKOB, Art. 15 BÜPF n° 2–21.

135 Art. 17 al. 3–6, 18, 19 al. 3–5, 25 al. 3–5, 26 OSCPT; voir HANSJAKOB, Art. 17 VÜPF n° 5–10, Art. 18 VÜPF n° 2–9, Art. 19 VÜPF n° 5–8, Art. 25 VÜPF n° 5, Art. 26 VÜPF n° 2–5.

136 *Supra* n° 24.

137 Art 15 al. 8 LSCPT.

C Infrastructure opérationnelle mise en place par la Confédération

1 *Service de surveillance de la correspondance par poste et télécommunication*

66. A l'époque du monopole de l'Etat sur le marché de la poste et des télécommunications, les relations entre les organes (fédéraux ou cantonaux) susceptibles d'ordonner une mesure de surveillance et le seul prestataire de services existant, l'entreprise des PTT, s'établissaient directement d'autorité à autorité. Relatives à l'entraide judiciaire nationale, les contestations en la matière étaient tranchées par la Chambre d'accusation du Tribunal fédéral, conformément à l'art. 357 CP en relation avec les art. 27 al. 5 phr. 2 et 252 al. 3 PPF¹³⁸.
67. Avec la libéralisation des marchés considérés, les organes de poursuite et d'instruction pénales se sont subitement retrouvés face à plusieurs opérateurs, fournissant autant de services susceptibles d'être surveillés. Pour d'évidentes raisons de praticabilité¹³⁹, la Confédération se devait d'offrir aux uns et aux autres un interlocuteur unique, chargé de fonctionner comme interface entre les différents protagonistes. Elle l'a fait en créant le Service de surveillance de la correspondance par poste et télécommunication¹⁴⁰. Aussi appelée le Service des tâches spéciales (STS), cette entité est rattachée administrativement au Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC).

138 ATF 79 IV 182–183 consid. 1–2, 115 IV 69–70 consid. 1.

139 Voir pourtant WEBER, *passim*, qui dénonce quelques-unes des grandes difficultés pratiques auxquelles se heurtent les autorités de poursuite et d'instruction pénales dans leurs relations avec le Service de surveillance.

140 Art. 2 LSCPT; art. 3 OSCPT.

Précédemment, voir les art. 1–3 de l'Ordonnance sur le service de surveillance de la correspondance postale et des télécommunications, du 1er décembre 1997 (RO 1997 p. 3022), abrogée par l'art. 34 OSCPT.

2 *Centre de traitement des données*

Pour pouvoir exécuter les ordres de surveillance de la correspondance par télécommunication, accès à Internet compris, le Service de surveillance exploite un Centre de traitement des données recueillies à l'occasion d'une telle mesure¹⁴¹. Cette unité a remplacé les sept centrales régionales créées en son temps par la Direction générale des PTT.

3 *Système de commutation*

Afin de pouvoir répondre aux demandes de renseignements sur les raccordements de télécommunication¹⁴², le Service de surveillance exploite, en collaboration avec les opérateurs de télécommunications, un système dit de commutation. De manière simplifiée, ce système consiste en une sorte d'annuaire informatisé à double sens, «à l'endroit» pour identifier le numéro d'appel d'une personne déterminée, «à l'envers» pour identifier le titulaire d'un numéro d'appel connu¹⁴³.

Pour accéder aux données enregistrées dans le système de commutation, les autorités habilitées à demander des renseignements sur les raccordements de télécommunication¹⁴⁴ peuvent toujours s'adresser au Service de surveillance¹⁴⁵. A condition d'en justifier le besoin, un droit d'utilisation *online* du système de commutation peut cependant être octroyé à une ou plusieurs personnes nominativement désignées par les autorités précitées¹⁴⁶. Les accès au système de commutation sont journalisés¹⁴⁷.

141 Art. 8 OSCPT.

142 *Supra* n° 40–44.

143 Pour les détails, voir l'art. 19 al. 1–2 OSCPT; cf. aussi les art. 3 let. f–g LTC et 2 let. h–i OSCTP.

144 Art. 14 al. 2 LSCPT.

145 Art. 22 OSCPT.

146 Art. 20 OSCPT.

147 Art. 21 OSCPT.

D Terminologie

71. L'art. 2 OSCPT définit toute une série de termes techniques qui apparaissent régulièrement au fil de la loi et de l'ordonnance. La liste reprend en partie et complète celle qui figure à l'art. 3 LTC.
72. Ni la LSCPT ni l'OSCPT ne contiennent en revanche un glossaire des abréviations techniques qui émaillent ces deux textes, singulièrement le second.

III Conditions de la surveillance

A Restriction de droits fondamentaux

73. La surveillance de la correspondance par poste et télécommunication d'une personne (physique ou morale) constitue une atteinte à sa vie et à sa sphère privées, respectivement garanties par les art. 17 par. 1 PIDCP, 8 par. 1 CEDH (droit au respect de la correspondance)¹⁴⁸ et 13 al. 1 *in fine* Cst. (droit au respect des relations établies par poste et télécommunication)¹⁴⁹.
74. Cette atteinte n'est admissible qu'à la condition de reposer sur une base légale, d'être justifiée par un intérêt public prépondérant et de s'avérer proportionnée au but visé¹⁵⁰. Dans la mesure où le Tribunal fédéral voit dans toute mesure de surveillance une atteinte grave à la sphère privée¹⁵¹, la base légale exigée doit être formelle¹⁵² et claire, c'est-à-dire avoir été édictée par le Parlement et présenter une «densité normative» suffisante.

148 Jurisprudence constante de la Cour européenne des droits de l'homme depuis Série A 28 Klass c/ D par. 41; récemment, voir RAD 2000 II 201 Amann c/ CH par. 45.

149 ATF 126 I 60–61 consid. 5a et les arrêts cités.

150 Art. 17 par. 1 PIDCP, 8 par. 2 CEDH et 36 al. 1–3 Cst.

151 ATF 109 Ia 298 consid. 12a, 122 I 190 consid. 4c et 193 consid. 5, 123 IV 243–244 consid. 3a, 125 I 49 consid. 3c, 125 I 98 consid. 2a et 103 consid. 3e; ZBl 86 (1985) 21 consid. 2.

152 Art. 36 al. 1 phr. 2 Cst.

B Surveillance de l'auteur présumé

1 Base légale

Depuis le 1^{er} janvier 2002, on l'a vu, la surveillance de la correspondance par poste et télécommunication est régie par la LSCPT, qui prévoit les bases légales constitutionnellement et conventionnellement requises¹⁵³, et par l'OSCPT, qui précise et complète ces dernières¹⁵⁴.

2 Intérêt public

Sous l'empire de l'art. 179^{octies} al. 2 CP dans ses anciennes teneurs 76. des 23 mars 1979¹⁵⁵ et 21 juin 1991¹⁵⁶, une mesure de surveillance était susceptible de servir deux intérêts publics diamétralement opposés: la répression et la prévention d'infractions déterminées. Elle pouvait ainsi être ordonnée quand bien même les «auteurs» n'avaient pas encore franchi le seuil de la punissabilité fixé par les règles générales sur la tentative¹⁵⁷ et spéciales sur les actes préparatoires délictueux¹⁵⁸.

Dans le nouveau droit, une surveillance de la correspondance par poste et télécommunication n'est plus possible qu'«aux fins de poursuivre» certains «actes punissables»¹⁵⁹.

Bien que la lettre de l'art. 179^{octies} al. 1 CP révisé ne prohibe pas formellement l'engagement préventif de tels instruments, la cohérence du système sinon les renvois opérés par les codes de procédure pénale à la LSCPT commandent de soumettre l'utilisation d'appareils techniques de surveillance à la même restriction.

153 Cf. RAD 1998 II 524 Kopp c/ CH par. 55–75.

154 S'agissant des bases légales légitimant l'utilisation d'appareils techniques de surveillance, notamment la LSCPT et l'OSCPT sur renvoi des codes fédéraux et cantonaux de procédure pénale, voir *supra* n° 46.

155 RO 1979 p. 1177–1178.

156 RO 1992 p. 599.

157 Art. 21–23 CP.

158 Art. 260^{bis} CP; art. 19 ch. 1 al. 6 LStup; etc.

159 Art. 3 al. 2 LSCPT; voir aussi l'art. 3 al. 3 LSCPT («à des fins de poursuite»).

79. Toute mesure de surveillance s'inscrit donc nécessairement dans le cadre d'une procédure pénale nationale¹⁶⁰ ou d'une procédure d'exécution d'une demande étrangère d'entraide en matière pénale¹⁶¹, diligentées «pour constater les infractions, en rechercher les auteurs et prononcer, s'il y a lieu, les sanctions [...] prévues par la loi»¹⁶².
80. Concrètement, l'intérêt public à la répression de comportements typiquement contraires à la loi pénale résidera dans
- la manifestation de la vérité lorsque la surveillance (suivie au besoin d'une saisie probatoire) tend à recueillir des éléments de preuve, à charge comme à décharge; ou
 - la garantie de l'exécution (d'une saisie conservatoire puis) d'une confiscation lorsque la surveillance tend à intercepter des objets dangereux ou des valeurs patrimoniales¹⁶³ connexes aux infractions poursuivies.

3 *Proportionnalité*

81. Afin de garantir que l'atteinte à la vie et à la sphère privées découlant d'une mesure de surveillance s'avère réellement nécessaire, la loi instaure une série de garde-fous représentant autant de concrétisation du principe constitutionnel de la proportionnalité.

a) *Infractions susceptibles de motiver une mesure de surveillance*

82. La principale innovation apportée par la LSCPT réside dans l'établissement d'un catalogue limitatif des infractions au code pénal et au droit pénal fédéral accessoire susceptibles de motiver une mesure de surveillance¹⁶⁴. Pour un coup d'essai, l'exercice ne ressemble guère à un coup de maître¹⁶⁵!

160 Art. 1 al. 1 let. a LSCPT.

161 Art. 1 al. 1 let. b LSCPT.

162 Art. 1 CPP.

163 Art. 58–59 CP; art. 38–39 LFMG; art. 36b–36d LEA; etc.

164 Art. 3 al. 2 let a–f et 3 let. a–f LSCPT.

165 Pour une critique complète et détaillée, voir HANSJAKOB, Art 3 BÜPF n° 35–68; JEAN-RICHARD-DIT-BRESSEL 60–67.

Un examen rapide des dispositions énumérées révèle tout d'abord **83.** que la liste n'est pas à jour puisqu'elle se réfère encore aux anciens droits de l'avortement et de la corruption¹⁶⁶.

Elle présente ensuite des lacunes flagrantes dans la mesure où elle **84.** omet par exemple de viser

- l'inondation et l'écoulement, d'une part, les dommages aux installations électriques, travaux hydrauliques et ouvrages de protections, d'autre part¹⁶⁷, pourtant passibles de 20 ans de réclusion à l'instar de l'incendie intentionnel et de l'explosion intentionnelle¹⁶⁸, lesquels figurent au catalogue;
- le génocide¹⁶⁹, prévoyant même la réclusion à perpétuité;
- la dénonciation calomnieuse portant sur un crime ou un délit¹⁷⁰, passible de 20 ans de réclusion.

Le catalogue renferme enfin des incohérences manifestes en tant **85.** qu'il mentionne par exemple

- la séquestration et l'enlèvement simples¹⁷¹, mais non pas leurs formes aggravées¹⁷²;
- la contrainte sexuelle et le viol perpétrés par un auteur unique¹⁷³, mais non pas leur commission en commun par plusieurs personnes¹⁷⁴;
- le faux dans les titres commun¹⁷⁵, mais non pas le faux dans les titres commis dans l'exercice de fonctions publiques¹⁷⁶.

166 Ancien art. 119 ch. 2 CP, devenu l'art. 118 al. 2 CP; anciens art. 288 et 315 CP, remplacés par les art. 322^{er}, 322^{quater} et 322^{septies} CP.

La loi fédérale du 21 mars 2003 concernant la modification du code pénal et de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (Financement du terrorisme) ne corrige qu'imparfaitement le tir puisqu'elle laisse subsister l'ancien art. 119 ch. 2 CP précité (FF 2003 p. 2532–2536).

167 Art. 227–228 CP.

168 Art. 221 al. 1–2 et 223 ch. 1 CP.

169 Art. 264 CP.

170 Art. 303 ch. 1 CP.

171 Art. 183 CP.

172 Art. 184 CP.

173 Art. 189 al. 1 et 3, 190 al. 1 et 3 CP.

174 Art. 200 CP.

175 Art. 251 ch. 1 CP.

176 Art. 317 ch. 1 CP.

86. Au-delà de ces incongruités, qui seront vraisemblablement corrigées par voie prétorienne¹⁷⁷, le législateur s'est également laissé aller, de manière cette fois à lier le juge chargé d'appliquer la loi, à divers choix politico-juridiques contestables, voire franchement incompréhensibles. Ainsi, pourquoi avoir laissé en marge du catalogue

- la fausse alerte¹⁷⁸, presque toujours commise au moyen du téléphone;
- la mise en danger de la vie d'autrui¹⁷⁹, alors que l'infraction jumelle d'exposition¹⁸⁰ s'y trouve;
- la représentation de la violence¹⁸¹, mais non pas la pornographie¹⁸², deux délits pourtant largement apparentés;
- le vol simple¹⁸³, la gestion déloyale (avec dessein d'enrichissement illégitime)¹⁸⁴, la banqueroute frauduleuse et la fraude dans la saisie¹⁸⁵ ou encore la diminution effective de l'actif au préjudice des créanciers¹⁸⁶, alors que l'abus de confiance¹⁸⁷ et l'escroquerie¹⁸⁸, pourtant assortis d'une clause punitive identique dans leur forme de base, y figurent;
- l'usure¹⁸⁹, possible ordinairement de 5, en cas de métier, de 10 ans de réclusion;
- la contrainte sexuelle ou le viol sur le conjoint¹⁹⁰, alors que ces infractions se caractérisent seulement par l'exigence d'une plainte du lésé, une distinction à laquelle échappent d'ailleurs les infractions contre le patrimoine¹⁹¹;

177 Cf. toutefois *supra* n° 74.

178 Art. 128^{bis} CP.

179 Art. 129 CP.

180 Art. 127 CP.

181 Art. 135 CP.

182 Art. 197 CP.

183 Art. 139 ch. 1 CP.

184 Art. 158 ch. 1 al. 3 et ch. 2 CP.

185 Art. 163 CP.

186 Art. 164 CP.

187 Art. 138 ch. 1 CP.

188 Art. 146 al. 1 CP.

189 Art. 157 CP.

190 Art. 189 al. 2, 190 al. 2 CP.

191 Cf. art. 138 ch. 1 al. 4, 139 ch. 4, 143 al. 2, 146 al. 3, 147 al. 3 et 160 ch. 1 al. 3 CP.

- l'enlèvement de mineur¹⁹², une surveillance des télécommunications étant souvent le seul moyen de localiser l'auteur (et les enfants enlevés!);
- l'entrave à l'action pénale¹⁹³;
- le blanchiment d'argent simple, en rupture avec la jurisprudence antérieurement établie¹⁹⁴;
- le faux témoignage alors que le Tribunal fédéral, après avoir laissé la question ouverte, avait jugé admissible le recours à une mesure de surveillance¹⁹⁵.

En l'état, la liste des infractions mentionnées à l'art. 3 al. 2 et 3 LSCPT **87.** suscite avant tout la perplexité. Elle pousse au crime dans la mesure où ses imperfections invitent quasiment tout procureur ou juge d'instruction normalement constitué au bricolage juridique, par exemple en qualifiant la fausse alerte mentionnée plus haut de (tentative de) menaces¹⁹⁶. Son utilité pratique est d'ailleurs fort douteuse au regard des autres conditions posées par la loi à une mise sous surveillance, à commencer par l'exigence de gravité de l'acte poursuivi¹⁹⁷.

De lege ferenda, le législateur serait bien inspiré de revenir à des **88.** techniques simples et éprouvées en prévoyant que tout crime ou délit (au sens de l'art. 9 CP) peut a priori motiver une mesure de surveillance. Ce faisant, il rétablirait une certaine échelle des valeurs, qui s'accorde mal de ce qu'il est aujourd'hui plus aisément d'incarcérer préventivement un individu que d'intercepter son courrier ou d'écouter son téléphone.

192 Art. 220 CP.

193 Art. 305 CP.

194 Art. 305^{bis} ch. 1 CP; ATF 125 I 51–53 consid. 7a.

195 Art. 307 CP; ATF 117 Ia 13 n° 3, 125 I 51–53 consid. 7a.

196 Art. (22 cum) 180 CP.

197 *Infra* n° 89–90.

b) Gravité de l'acte

89. Selon l'art 3 al. 1 let. b LSCPT, la gravité de l'acte doit ensuite justifier la surveillance. Alternativement avec «la particularité de l'acte», cette exigence résultait déjà de l'ancien art. 179^{octies} al. 2 CP.
90. La loi constraint ici les autorités compétentes pour ordonner puis approuver la surveillance, après avoir contrôlé abstraitemment que l'infraction considérée figurait au catalogue¹⁹⁸, de procéder à un examen concret du cas d'espèce. Sous cet angle, même la contravention d'utilisation abusive d'une installation de télécommunication¹⁹⁹ peut, toutes proportions gardées, s'avérer suffisamment grave pour motiver le recours à une mesure de surveillance. Sur la base des éléments disponibles²⁰⁰, l'appréciation s'effectuera en fonction de toutes les circonstances objectives et subjectives caractérisant l'infraction, singulièrement
- la nature du bien juridique attaqué;
 - l'importance de sa lésion ou de sa mise en danger;
 - le *modus operandi* retenu, notamment l'existence d'une action ou d'une omission improprement dite;
 - l'intensité de la volonté délictueuse, de «l'énergie criminelle» déployée par l'auteur (considérant que le catalogue renferme seulement des infractions intentionnelles);
 - les mobiles du délinquant et la finalité de l'acte.

c) Subsidiarité de la mesure de surveillance

91. Dans la mesure où elles «ratissent» de manière particulièrement large²⁰¹, la surveillance de la correspondance par poste ou télécommunication et l'utilisation d'appareils techniques de surveillance ne peuvent être ordonnés qu'à titre d'*ultima ratio* procédurale. L'art. 3 al. 1 let. c LSCPT concrétise cette exigence en disposant que «les mesures prises jusqu'alors dans le cadre de l'instruction sont restées

198 *Supra* n° 82.

199 Art. 179^{septies} CP, visé par l'art. 3 al. 2 let. f LSCPT.

200 *Infra* n° 98–99.

201 *Infra* n° 195.

sans succès ou les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles en l'absence de surveillance».

Aux termes mêmes de la loi, la subsidiarité de la mesure ne doit pas **92.** nécessairement être positivement établie par l'épuisement préalable de l'arsenal des autres moyens d'investigation prévus (ou du moins non prohibés) par les codes de procédure pénale. Au gré de la spécificité de l'infraction poursuivie ou des modalités de sa perpétration, une subsidiarité «présumable» sera suffisante si les enseignements de la criminalistique ou l'expérience des enquêteurs démontrent la vanité ou la disproportion de méthodes moins liberticides.

d) Durée de la surveillance

La surveillance en temps réel dure 3 mois au plus²⁰². La période **93.** commence avec la transmission de l'ordre de surveillance au Service de surveillance²⁰³. Le décompte s'effectue à la minute près; si l'ordre de surveillance a été décerné le 15 juin à 16 h 30, la mesure expire donc le 15 septembre à 16 h 29 au plus tard. La surveillance peut cependant être prolongée par tranches successives de 3 mois au plus chacune²⁰⁴.

Quant à la surveillance rétroactive de la correspondance postale et **94.** des télécommunications, elle s'étend sur une période maximale de 6 mois²⁰⁵, celle durant laquelle les fournisseurs de services ont l'obligation de conserver les données relatives au trafic et à la facturation²⁰⁶. Les informations plus anciennes qu'ils posséderaient ne sont pas accessibles aux autorités de poursuite et d'instruction pénale, fût-ce par le détournement d'une perquisition ou d'un ordre de production²⁰⁷.

202 Art. 7 al. 3 phr. 4 LSCPT.

203 *Infra* n° 131.

204 Art. 7 al. 5 phr. 1 LSCPT; *infra* n° 174–177.

205 Art. 5 al. 2 LSCPT.

206 *Supra* n° 62–63.

207 *Supra* n° 14–20, 33–39; voir HANSJAKOB, Art. 5 BÜPF n° 13.

e) *Limites posées aux branchements directs*

95. Un raccordement de télécommunication fait l'objet d'un branchement direct lorsque la correspondance transitant par lui est transmise directement (par déviation) à l'autorité qui a ordonné la surveillance, en pratique à ses services de police, lesquels se substitueront au Service de surveillance pour enregistrer les informations brutes ainsi obtenues²⁰⁸.
96. Le branchement direct, qui permet donc à l'autorité chargée de l'enquête de prendre connaissance en temps réel (*live*) des communications interceptées, est admissible s'il «est probable qu'il ne portera pas atteinte à des intérêts privés prépondérants» et si «la protection des données est garantie»²⁰⁹. Cas échéant, la première condition fera obstacle au branchement direct du raccordement de l'auteur présumé s'il apparaît d'emblée ou en cours de surveillance que la ligne est essentiellement utilisée par des tiers étrangers aux infractions poursuivies. Quant à la seconde exigence, elle commandera notamment de restreindre au strict minimum le cercle des agents chargés de prendre connaissance des communications acheminées.
97. En toute hypothèse, le branchement direct du raccordement de l'auteur présumé est interdit lorsque ce dernier est une personne soumise au secret professionnel²¹⁰. Cette interdiction absolue est le corollaire de la règle selon laquelle le tri des informations recueillies lors de la surveillance d'un tel raccordement incombe à une autorité judiciaire différente de celle qui mène l'instruction (et qui avait en principe ordonné la mesure)²¹¹. S'il apparaît en cours de surveillance que la personne visée est tenue au secret professionnel, le branchement direct doit immédiatement être supprimé, les éléments recueillis dans l'intervalle demeurant toutefois exploitables²¹².

208 Cf. art. 2 let. e OSCPT.

209 Art. 3 al. 4 phr. 1 LSCPT; voir HANSJAKOB, Art. 3 BÜPF n° 75–77.

210 Art. 3 al. 4 phr. 2 LSCPT; sur le cercle des personnes soumises au secret professionnel, voir *infra* n° 117–118.

211 Art. 4 al. 6 phr. 1 LSCPT; *infra* n° 202–205.

212 HANSJAKOB, Art. 3 BÜPF n° 80.

4 **Prévention suffisante**

Constituant un rempart contre les *“fishing expeditions”*, l’existence de 98. charges suffisantes objectivement fondées gouverne la mise en oeuvre de toutes les mesures processuelles de contrainte. En l’espèce, l’art. 3 al. 1 let. a et – même si sa formulation est plus succincte – l’art. 4 al. 3 let. a LSCPT exigent que la personne dont l’adresse postale, le raccordement de télécommunication, le téléphone mobile ou la boîte aux lettres électronique seront surveillés voie peser sur elle de graves soupçons, reposant sur des faits déterminés, d’avoir commis l’une des infractions énumérées dans le catalogue.

Peu importe que le prévenu apparaisse comme étant un participant 99. principal (auteur direct, coauteur, auteur médiat) ou seulement accessoire (instigateur ou complice)²¹³ du délit considéré, lequel peut avoir été consommé ou simplement tenté²¹⁴.

5 **Attribution de l’objet de la surveillance**

Lorsque les conditions posées par l’art. 3 al. 1–3 LSCPT²¹⁵ sont remplies, l’autorité compétente est habilitée à ordonner la mise sous surveillance de l’adresse postale, du raccordement de télécommunication, du téléphone mobile ou de la boîte aux lettres électronique «de» l’auteur présumé. Il reste ainsi à définir les critères en fonction desquels les différents objets d’une surveillance de la correspondance par poste et télécommunication²¹⁶ sont réputés «appartenir» au prévenu.

L’attribution d’une adresse postale à l’auteur présumé est purement 101. «factuelle». Elle résulte non seulement de l’existence d’un domicile

213 Art. 24–25 CP.

214 Art. 21–23 CP.

215 *Supra* n° 75–99.

216 *Supra* n° 4, 25.

(individuel ou partagé) ou d'un lieu de travail réels à l'adresse considérée, mais peut aussi découler d'une domiciliation purement fictive, caractérisée – cas échéant à l'insu du véritable résidant – par l'adjonction des mentions «c/o» ou «p.a.» sur un envoi²¹⁷ ou par l'apposition (momentanée) sur une boîte aux lettres d'une étiquette comportant le nom du destinataire d'un envoi. Un auteur présumé peut ainsi avoir plusieurs adresses sujettes à surveillance. Son nom, qu'il s'agisse de son véritable patronyme ou d'un alias connu, doit toutefois figurer sur les envois à intercepter; la surveillance d'un tiers selon l'art. 4 al. 1 LSCPT commence là où l'auteur présumé se dissimule derrière le nom d'autrui²¹⁸.

102. Inversement, l'attribution d'un raccordement à l'auteur présumé résulte d'un acte juridique, soit d'un contrat passé entre l'intéressé et un fournisseur de services de télécommunication, aux termes duquel le premier s'abonne au raccordement mis à sa disposition par le second²¹⁹. La même approche préside à l'attribution d'une boîte aux lettres électronique à l'auteur présumé. Dans les deux cas, il suffit que le prévenu apparaisse comme étant l'un des titulaires du raccordement ou de la boîte aux lettres électronique à surveiller lorsque l'opérateur de télécommunication ou le fournisseur d'accès à Internet a contracté avec plusieurs personnes conjointement, par exemple avec les époux occupant un même logement; nonobstant la certitude d'intercepter également les appels passés par la femme (et les enfants) du prévenu, la mise sur écoute de la ligne téléphonique desservant leur domicile commun ne relève pas encore de la surveillance d'un tiers au sens de l'art. 4 al. 1 LSCPT²²⁰.
103. Nécessaire, cette exigence de (co)titularité de l'objet de la surveillance est aussi suffisante. Il s'ensuit que l'adresse postale, le raccordement de télécommunication et la boîte aux lettres électronique de

217 Cf. HANSJAKOB, Art. 4 BÜPF n° 5.

218 *Infra* n° 112.

219 Cf. art. 1 let. a OST; CONSEIL FÉDÉRAL 3712.

220 *Infra* n° 112; cf. ATF 125 I 98–101 consid. 2.

l'auteur présumé peuvent être surveillés même si celui-ci, du fait notamment de son incarcération, se trouve (temporairement) dans l'impossibilité de les utiliser²²¹.

S'agissant enfin de la surveillance d'un téléphone portable au moyen **104.** de son numéro IMEI, le critère de la possession de l'appareil par le prévenu devrait être déterminant.

C Surveillance d'un tiers

L'auteur présumé d'une infraction figurant au catalogue de l'art. 3 **105.** al. 2-3 LSCPT n'est pas seul à pouvoir faire l'objet d'une mesure de surveillance. A certaines conditions complémentaires²²², d'autres personnes sont également susceptibles de voir leur adresse postale, leur raccordement de télécommunication, leur téléphone mobile ou leur boîte aux lettres électronique être surveillés.

La loi regroupe ces personnes sous l'appellation de «tiers».

106.

1 Surveillance d'un tiers en général

Aux termes de l'art. 4 al. 1 LSCPT, «la surveillance d'un tiers peut être **107.** ordonnée si des faits déterminés font présumer que le suspect utilise ou fait utiliser l'adresse postale ou le raccordement de télécommunication du tiers pour recevoir ou transmettre des envois ou des communications». La portée de cette disposition se laisse relativement bien illustrer à l'exemple du raccordement téléphonique dont l'abonné – une personne physique ou morale – est un tiers non prévenu. L'auteur présumé

221 ATF 125 I 98–101 consid. 2 précité; RJB 122 (1986) 31 et 34–35.

222 Cf. BIEDERMANN 85.

- a) utilise le raccordement téléphonique de ce tiers pour recevoir ou transmettre des communications s'il
 - appelle (une autre personne, voire le tiers lui-même) depuis ce raccordement;
 - est appelé (par une autre personne, voire par le tiers lui-même) à ce raccordement;
- b) fait utiliser le raccordement téléphonique de ce tiers pour recevoir ou transmettre des communications
 - s'il appelle ce raccordement pour communiquer avec le tiers ou avec une autre personne²²³;
 - si, pour son compte, il amène
 - le tiers ou une autre personne à l'appeler lui ou à appeler un individu différent encore depuis ce raccordement;
 - le tiers ou une autre personne à être appelés par un tel individu à ce raccordement;
 - un tel individu à appeler ce raccordement pour communiquer avec le tiers ou avec une autre personne.

108. La suspicion que l'auteur présumé utilise ou fait utiliser le raccordement du tiers doit reposer sur des faits déterminés, c'est-à-dire des indices objectifs permettant raisonnablement de tirer une telle conclusion.

109. Peu importe que le tiers soit de bonne ou de mauvaise foi. Dans cette dernière hypothèse, il pourrait toutefois se voir reprocher une infraction propre et, si celle-ci remplit les conditions de l'art. 3 al. 1–3 LSCPT, faire l'objet d'une mise sous surveillance en qualité d'auteur présumé.

223 Sous l'empire des anciens textes (art. 66 al. 1^{bis} phr. 3 PPF dans sa teneur des 23 mars 1979 [RO 1979 p. 1170] et 21 juin 1991 [RO 1992 p. 599]; art. 70 al. 2 phr. 3 PPM dans sa teneur des 23 mars 1979 [RO 1979 p. 1174] et 21 juin 1991 [RO 1992 p. 600]; art. 184A al. 2 phr. 2 CPP dans sa teneur du 7 mai 1981 [RAG 1981 p. 216]), qui ne prévoyaient généralement pas l'alternative utiliser / faire utiliser, ce cas de figure était assimilé par la pratique à l'utilisation du raccordement du tiers (RJB 122 [1986] 31 et 35, 125 [1989] 555). Cette construction n'est plus nécessaire aujourd'hui (*contra*: CONSEIL FÉDÉRAL 3712; HANSJAKOB, Art. 4 BÜPF n° 6). Au nom de la cohérence terminologique, il convient même de la bannir et de conserver à l'expression «utiliser» le sens étroit qui, selon la volonté clairement manifestée du législateur, lui revient à l'art. 4 al. 3 let. b LSCPT (*infra* n° 122).

Une utilisation directe (personnelle) ou indirecte (par personne interposée) du raccordement du tiers est en revanche toujours nécessaire. Alors qu'une perquisition est généralement possible «en tous lieux où la recherche de la vérité l'exige»²²⁴, par exemple donc au domicile d'un témoin qui détiendrait une pièce à conviction, la surveillance du raccordement d'un tel témoin est juridiquement exclue alors même que des indices concrets donneraient à penser que l'intéressé dispose d'informations concernant l'infraction poursuivie et qu'il les partage téléphoniquement avec d'autres personnes. En pareille situation, seule l'utilisation d'appareils techniques de surveillance est susceptible d'apporter aux autorités pénales les renseignements recherchés. De même, la mise sur écoute du raccordement du lésé ou de la victime de l'infraction poursuivie n'est admissible que si des éléments objectifs indiquent que l'auteur présumé l'utilisera directement ou indirectement, par exemple en appelant ou en faisant appeler au domicile des parents d'un enfant qu'il a enlevé pour leur dicter ses exigences²²⁵.

Les règles susmentionnées s'appliquent *mutatis mutandis* à l'utilisation personnelle ou par personne interposée de la boîte aux lettres électronique d'un tiers, dont le *username* et le mot de passe nécessaires à la connexion aux installations du fournisseur d'accès devront simplement être connus de l'auteur présumé ou de son instrument.

Lorsqu'il utilise ou fait utiliser le raccordement de télécommunication d'un tiers, l'auteur présumé se dissimule en quelque sorte derrière l'abonné et exploite le fait que la trace laissée ne conduit pas, dans un premier temps du moins, à lui. Ces spécificités doivent également caractériser l'utilisation directe ou indirecte de l'adresse postale d'un tiers. Ici, l'auteur présumé aura fait en sorte de ne pas apparaître, sous son vrai nom ou sous un pseudonyme connu, sur les envois qui lui sont destinés²²⁶.

224 Ainsi l'art. 178 al. 1 CPP; cf. aussi les art. 67 al. 1 PPF, 48 al. 1 DPA, 66 al. 1 PPM.

225 Art. 185 CP.

226 Cf. *supra* n° 101.

2 *Surveillance d'un raccordement public et d'un raccordement anonyme*

113. Les règles développées ci-dessus à l'enseigne de l'utilisation du raccordement (téléphonique) d'un tiers conservent toute leur validité lorsque la mesure de surveillance vise un poste public de télécommunication ou un raccordement qui ne peut être attribué à une personne connue²²⁷.
114. La notion de «poste public de télécommunication»²²⁸ recouvre principalement les cabines téléphoniques payantes placées sur le domaine public ou à l'intérieur de certains établissements publics (cafés, restaurants, théâtres, cinémas, etc.), ainsi que les télécopieurs payants mis à la disposition du public dans les offices postaux. En revanche exclus les raccordements desservant les établissements publics précités eux-mêmes et susceptibles, à la discréption du propriétaire ou du gérant, d'être utilisés par la clientèle pour passer ou recevoir des appels.
115. Les raccordements qui ne peuvent être attribués à une personne connue sont essentiellement ceux que les opérateurs de téléphonie mobile offrent contre prépaiement à des usagers dont ils ne relèvent ou ne conservent pas l'identité²²⁹. Parce qu'elle revient à substituer au critère juridique régissant l'attribution d'un raccordement à un individu²³⁰ le critère factuel de l'utilisation effective de la ligne considérée, on peut douter de l'exactitude de l'opinion²³¹ selon laquelle un raccordement à prépaiement sort du champ d'application de l'art. 4 al. 2 LSCPT pour tomber dans celui des art. 3 al. 1–3 ou 4 al. 1

227 Art. 4 al. 2 LSCPT.

228 Cf. art. 19 al. 1 let. e OST.

229 La loi fédérale du 21 mars 2003 concernant la modification du code pénal et de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (Financement du terrorisme) introduit à l'art. 15 LSCPT un nouvel al. 5^{bis} qui fera dorénavant obligation aux opérateurs de la téléphonie mobile de (faire) relever et de conserver deux ans au moins les renseignements prévus à l'art. 14 al. 1 let. a–c LSCPT (FF 2003 p. 2532–2536).

230 *Supra* n° 102.

231 HANSJAKOB, *Erfahrungen* 277.

LSCPT dès l'instant – mais pour combien de temps? – où son usager est identifié; la question revêt une certaine importance pratique lorsque l'usager identifié s'avère être l'auteur présumé, les mesures de protection fondées sur l'art. 4 al. 5 LSCPT²³² pouvant alors être levées.

3 *Surveillance d'un tiers tenu au secret professionnel*

La mise sous surveillance de tiers tenus au secret professionnel fait **116**. l'objet d'une réglementation spécifique, plus restrictive que celle prévue par l'art. 4 al. 1–2 pour les tiers «ordinaires».

Pour délimiter le cercle des personnes ainsi privilégiées, l'art. 4 al. 3 **117**. LSCPT s'en remet au droit (fédéral ou cantonal) de procédure pénale gouvernant l'action publique et à ses règles interdisant ou dispensant les membres de certains corps professionnels d'apporter leur témoignage à la justice. A Genève, l'art. 47 CPP vise tout d'abord les ecclésiastiques, avocats, défenseurs en justice, notaires, médecins, dentistes, pharmaciens, sages-femmes et leurs auxiliaires. Une énumération实质上 identique figure aux art. 77 PPF²³³ et 75 let. b PPM. Ensuite, l'art. 47 CPP renvoie lui-même à toutes les dispositions fédérales de procédure²³⁴ prévoyant une dispense de témoigner, par exemple l'art. 139 al. 3 CC pour les conseillers conjugaux ou familiaux et les médiateurs en matière familiale, l'art. 4 al. 1–3 LAVI pour les collaborateurs des centres de consultation ouverts aux victimes d'infraction ou encore l'art. 15 al. 2 phr. 2 LStup pour le personnel des institutions de traitement ou d'assistance des toxicomanes.

232 *Infra* n° 197–201.

233 Cette disposition est applicable par analogie dans les procédures soumises au droit pénal administratif (art. 41 al. 2 phr. 1 DPA).

234 A l'exclusion donc des dispositions de droit matériel (cf. Pr 85 [1996] n° 198 consid. 3).

118. Soumis à diverses restrictions intéressant l'objet de la publication et la nature des infractions poursuivies²³⁵, le secret professionnel (réactionnel) du journaliste (indirectement) consacré par l'art. 27^{bis} CP²³⁶ tombe également dans le champ d'application de l'art. 4 al. 3 LSCPT²³⁷.
119. La loi ne prévoit en revanche aucun privilège pour les tiers astreints au secret de fonction²³⁸ et les proches de l'auteur présumé²³⁹, à moins bien sûr qu'ils ne soient simultanément soumis au secret professionnel²⁴⁰, par exemple en qualité de médecin d'un service pénitentiaire.
120. Dans sa formulation, l'al. 3 let. b de l'art. 4 LSCPT diffère en trois points des deux alinéas qui le précèdent.
121. D'abord, l'interdiction de la surveillance d'un tiers soumis au secret professionnel est érigée en principe, tandis que le recours à une telle mesure n'est autorisé qu'exceptionnellement. Le sens de cette opposition demeure obscur, la loi ne livrant aucun critère propre à distinguer la règle et les dérogations qu'elle tolère. En pratique, elle n'aura pas d'autre finalité que d'inviter l'autorité à effectuer ici une pesée particulièrement scrupuleuse des intérêts en présence²⁴¹.

235 Le catalogue dressé par l'art. 27^{bis} al. 2 let. b CP diffère toutefois sensiblement de celui figurant à l'art. 3 al. 2–3 LSCPT.

236 Dans sa teneur selon la loi n° 8655 du 16 mai 2003 (FAO 57/23.5.2003 p. 23), le nouvel art. 47A CPP prévoit, aux conditions fixées par l'art. 27^{bis} CP, une dispense explicite du journaliste de témoigner.

237 Cf. RAD 1996 II 483 Goodwin c/ UK par. 39–46; ATF 123 IV 247–249 consid. 8a; RSJ 93 (1997) 138 consid. VI. *Contra*: HANSJAKOB, Art. 4 BÜPF n° 27, qui retient ici l'application exclusive de l'art. 27^{bis} CP.

La seule conséquence pratique du détour par l'art. 4 al. 3 LSCPT, ici préconisé, réside dans la mise des journalistes au bénéfice des protections particulières en matière de branchements directs (*supra* n° 97) et de tri des informations recueillies (*infra* n° 202–205).

238 Voir par exemple les art. 78 PPF, 77 al. 2 PPM, 46 al. 1 CPP. L'art. 78 PPF est applicable par analogie dans les procédures soumises au droit pénal administratif (art. 41 al. 2 phr. 1 DPA).

239 Cf. ATF 122 I 197–200 consid. 6.

Sur la dispense de témoigner généralement accordée aux proches du prévenu, voir par exemple les art. 75 let. a PPF et 75 let. a PPM. L'art. 75 let. a PPF est applicable par analogie dans les procédures soumises au droit pénal administratif (art. 41 al. 2 phr. 1 DPA).

240 Cf. art. 46 al. 2 *in fine* CPP.

241 Cf. HANSJAKOB, Art. 4 BÜPF n° 13 note 266 et la référence citée.

Ensuite, la mise sous surveillance de l'adresse postale, du raccordement de télécommunication ou de la boîte aux lettres électronique d'un confident nécessaire n'est possible que si l'auteur présumé les utilise, mais non pas s'il les fait utiliser. Il s'ensuit, pour reprendre l'exemple précédemment proposé²⁴², que la ligne téléphonique d'un avocat ou d'un médecin ne peut être surveillée que si le prévenu appelle depuis ou est appelé sur le raccordement du professionnel, mais non pas s'il appelle ce raccordement²⁴³ ou amène un intermédiaire à actionner le combiné qui s'y trouve connecté.

Enfin, l'art. 4 al. 3 let. b LSCPT ne contient pas les mots «pour recevoir ou transmettre des envois ou des communications». A en croire les travaux préparatoires²⁴⁴, cette omission volontaire signifierait que seuls les envois et communications sortants pourraient être interceptés. Une telle interprétation est évidemment absurde. D'une part et de manière tout à fait générale, on ne voit pas à quoi pourrait bien servir l'utilisation d'un raccordement sinon à la réception et la transmission de communications; n'apportant rien aux dispositions qui la renferment, la formule ne peut rien enlever à celle qui l'écarte. D'autre part, il suffirait à l'auteur présumé souhaitant passer un appel depuis le téléphone d'un tiers tenu par le secret professionnel d'inviter son correspondant à le rappeler immédiatement²⁴⁵; bien trop simple à contourner, l'«obstacle» ne mérite aucune reconnaissance légale.

Déjà évoquée en relation avec la surveillance de l'auteur présumé, l'interdiction de brancher directement le raccordement d'un confident nécessaire²⁴⁶ vaut a fortiori en l'absence de prévention (suffisante) contre ce dernier.

242 *Supra* n° 107.

243 CONSEIL FÉDÉRAL 3713.

244 Voir HANSJAKOB, Art. 4 BÜPF n° 31 et la référence citée.

245 *Ibidem*.

246 Art. 3 al. 4 phr. 2 LSCPT; *supra* n° 97.

IV Procédure de mise sous surveillance

A Mesure préalable éventuelle

125. Afin d'identifier le numéro d'appel ou l'adresse e-mail de la personne à surveiller, la mise sous surveillance proprement dite sera, cas échéant, précédée d'une demande de renseignements sur les raccordements de télécommunication et les usagers d'Internet²⁴⁷.

B Ordre de surveillance

I Compétence

126. En procédure pénale fédérale, les autorités habilitées à ordonner une mesure de surveillance sont le juge d'instruction fédéral et, avant l'ouverture de l'instruction préparatoire, le procureur général de la Confédération²⁴⁸.
127. En procédure pénale militaire, le juge d'instruction militaire est seul compétent²⁴⁹.
128. A Genève, enfin, la surveillance est ordonnée
- par le procureur général au cours de l'enquête préliminaire de police judiciaire, mais seulement à titre rétroactif²⁵⁰ et pour autant qu'il ne requiert pas l'ouverture d'une instruction préparatoire²⁵¹;
 - par le juge d'instruction dans le cadre de l'instruction préparatoire ou de l'exécution d'une demande d'entraide judiciaire²⁵²;

²⁴⁷ *Supra* n° 40–44.

²⁴⁸ Art. 6 let. a ch. 1–2 LSCPT; art. 66 al. 2 phr. 1 PPF.

²⁴⁹ Art. 6 let. a ch. 3 LSCPT; art. 70 phr. 2 PPM.

²⁵⁰ *Supra* n° 11–13, 28–32.

²⁵¹ Art. 48A al. 1 let. a LACP et 115C CPP *cum* art. 6 let. a ch. 4 LSCPT, dans leur teneur selon la loi n° 8732 du 16 mai 2003 (FAO 57/23.5.2003 p. 23).

²⁵² Art. 48A al. 1 let. b LACP et 184A CPP *cum* art. 6 let. a ch. 4 et let. c LSCPT, dans leur teneur selon la loi n° 8732 du 16 mai 2003 (FAO 57/23.5.2003 p. 23).

- par le président du Tribunal de la jeunesse lorsque l'action publique est dirigée contre un mineur²⁵³.

2 *Contenu*

Selon qu'il concerne une adresse postale, un raccordement de télé-**129.** communication, un téléphone mobile ou une boîte aux lettres électronique, d'une part, selon qu'il est destiné à déployer des effets pro- ou rétrospectifs, d'autre part, l'ordre de surveillance doit contenir toute une série de données indispensables à la mise en oeuvre de la mesure. L'ordonnance en dresse la liste²⁵⁴.

Afin de simplifier la tâche des autorités compétentes pour ordonner **130.** la surveillance, le Service de surveillance a établi des formules à leur attention²⁵⁵.

3 *Destinataire et mode de transmission*

L'ordre de surveillance doit obligatoirement être adressé au Service **131.** de surveillance²⁵⁶. Un ordre envoyé directement au fournisseur de services concerné par la mesure sera, d'office et sans délai, réacheminé par ce dernier au Service de surveillance.

L'ordre de surveillance peut être transmis au Service de surveillance **132.** par poste, par télécopieur ou par tout autre moyen sécurisé autorisé par le DETEC²⁵⁷. Dans la pratique, l'usage du télécopieur devrait se généraliser; un envoi parallèle des originaux par courrier n'est pas requis. En cas d'urgence, une communication orale (téléphonique)

²⁵³ Art. 48A al. 1 let. c LACP *cum* art. 6 let. a ch. 4 LSCPT, dans sa teneur selon la loi n° 8732 du 16 mai 2003 (FAO 57/23.5.2003 p. 23).

²⁵⁴ Voir les art. 11, 15 et 23 OSCPT.

²⁵⁵ Cf. art. 33 al. 2 let. a OSCPT.

²⁵⁶ Cf. art. 5 al. 1 OSCPT.

²⁵⁷ Art. 5 al. 1 let. a OSCPT.

est également possible, mais l'ordre doit être confirmé par écrit et acheminé au Service de surveillance selon l'un des modes précités²⁵⁸.

4 *Effets*

133. Même affecté d'un vice²⁵⁹, l'ordre de surveillance est immédiatement exécutoire²⁶⁰. En conséquence, il déploie ses effets déjà durant les 24 heures à disposition du magistrat pour demander l'autorisation de la surveillance²⁶¹, respectivement les 5 jours laissés à la juridiction compétente pour approuver la mesure²⁶².

C **Demande d'autorisation de la surveillance**

1 *Fondement*

134. Très généralement secrètes, les mesures de surveillance échappent par nature au contrôle judiciaire immédiat habituellement offert aux parties à la procédure et aux tiers atteints dans leurs droits, sous la forme d'un recours contre les décisions et opérations du juge d'instruction ou du procureur. Pour ainsi dire en contrepartie, l'art. 179^{octies} al. 1 *in fine* CP soumet la mise en oeuvre des mesures de surveillance à l'approbation originaire d'un juge²⁶³.

2 *Compétence*

135. La demande d'autorisation de la surveillance doit émaner du magistrat même qui a ordonné la mesure²⁶⁴. Tenu de procéder d'office,

258 Art. 5 al. 1 let. b et al. 2 OSCPT.

259 *Infra* n° 178, 185.

260 Cf. art. 7 al. 4 LSCPT.

261 *Infra* n° 136.

262 *Infra* n° 153.

263 OBERHOLZER 4.

264 Art. 179^{octies} al. 1 *in fine* CP; art. 7 al. 2 LSCPT.

l'intéressé ne peut pas déléguer l'accomplissement de cette démarche à un tiers.

3 *Délai*

La demande d'autorisation doit être transmise dans les 24 heures à 136. l'autorité judiciaire chargée d'approuver la surveillance²⁶⁵.

Le délai commence à courir avec la transmission de l'ordre de surveillance au Service de surveillance²⁶⁶, c'est-à-dire avec sa remise à la poste, son envoi par télécopie ou sa communication orale²⁶⁷.

A rigueur de texte, le délai est observé si la demande d'autorisation 138. est transmise à temps à l'autorité compétente. Il n'est donc pas nécessaire que la requête lui parvienne aussi dans les 24 heures²⁶⁸.

Les 24 heures prévues se comptent à la minute près. La computation 139. n'est possible que si les dates et heures exactes de transmission de l'ordre de surveillance et de transmission de la demande d'autorisation sont inscrites au dossier.

En l'absence de dispositions expresses en la matière, le délai imparti 140. n'est susceptible d'aucune suspension ou prolongation. Son expiration n'est pas davantage reportée au premier jour ouvrable si sa fin tombe sur un samedi, un dimanche ou un autre jour férié.

Toutefois, il est généralement admis que les 24 heures de l'art. 7 al. 2 141. LSCPT ne constituent qu'un simple délai d'ordre, dont l'inobservance n'est assortie d'aucune sanction procédurale²⁶⁹.

265 Art. 7 al. 2 LSCPT.

266 HANSJAKOB, Art. 7 BÜPF n° 7; JEAN-RICHARD-DIT-BRESSEL 51.

267 *Supra* n° 132.

268 *Contra*: HANSJAKOB, Art. 7 BÜPF n° 7.

269 HANSJAKOB, Art. 7 BÜPF n° 9 et les références citées.

4 *Forme*

142. La demande d'autorisation prend la forme d'un «exposé des motifs» auquel seront joints l'ordre de surveillance²⁷⁰ et les pièces du dossier nécessaires à l'autorité compétente pour statuer²⁷¹.
143. En pratique, le magistrat chargé de l'enquête rédigera une ordonnance, dont les considérants détailleront en fait et en droit la réalisation des conditions de la mise sous surveillance²⁷² et dont le dispositif spécifiera le type de mesure ordonnée, sa durée et ses modalités d'exécution²⁷³. Il y annexera les principaux éléments de preuve dont il dispose déjà, par exemple des déclarations de témoins ou des documents saisis, mais aussi les informations recueillies durant les premières heures de la surveillance.

5 *Destinataire et mode de transmission*

144. La demande d'autorisation est adressée directement à l'autorité judiciaire désignée par le droit fédéral ou cantonal²⁷⁴.
145. La loi ne contient aucune prescription quant aux canaux à utiliser pour acheminer la demande d'autorisation à son destinataire. Afin de laisser 5 jours pleins au juge appelé à statuer²⁷⁵, l'usage du télécopieur ou le recours aux services d'un coursier – singulièrement lorsque les pièces jointes à l'ordre de surveillance sont volumineuses – devraient l'emporter sur la voie postale.

270 *Supra* n° 129–130.

271 Art. 7 al. 2 let. a–b LSCPT.

272 *Supra* n° 75–124; cf. OBERHOLZER 7–8.

273 Cf. *infra* n° 180, 185.

274 Art. 7 al. 2 LSCPT; *infra* n° 148–150.

275 *Infra* n° 153.

6 *Conséquences de l'absence de demande*

En l'absence de toute demande d'autorisation de la surveillance, et 146. non pas simplement en cas de (léger) retard de celle-ci²⁷⁶, l'art. 7 al. 4 LSCPT prévoit les mêmes conséquences procédurales qu'en cas de refus de l'autorité compétente d'approuver la mesure. La question sera abordée dans ce dernier contexte²⁷⁷.

D **Décision sur la demande d'autorisation de la surveillance**

1 *Compétence*

Aux termes de l'art. 179^{octies} al. 1 *in fine* CP, seul un juge est habilité à 147. statuer sur une demande d'autorisation de surveillance.

En procédure pénale fédérale, il s'agit aujourd'hui du président de la 148. Chambre d'accusation du Tribunal fédéral²⁷⁸. Dès l'entrée en vigueur de la LTPF, la compétence passera au président de la Cour des plaintes du Tribunal pénal fédéral²⁷⁹.

En procédure pénale militaire, la décision incombe au président du 149. Tribunal militaire de cassation²⁸⁰.

A Genève, enfin, la loi désigne le président de la Chambre d'accusation²⁸¹. 150.

276 *Supra* n° 141.

277 *Infra* n° 169–172.

278 Art. 7 al. 1 let. a LSCPT.

279 Voir FF 2002 p. 6058.

280 Art. 7 al. 1 let. b LSCPT.

281 Art. 48A al. 2 let. a LACP *cum* art. 7 al. 1 let. c LSCPT, dans sa teneur selon la loi n° 8732 du 16 mai 2003 (FAO 57/23.5.2003 p. 23).

2 Examen

151. Particulièrement mal formulé, l'art. 7 al. 3 phr. 1 LSCPT donne à penser que l'autorité judiciaire saisie d'une demande d'autorisation de la surveillance ne peut sanctionner qu'un manquement à l'exigence de proportionnalité. En réalité, le juge compétent doit, comme sous l'empire de l'ancien droit, vérifier que l'ensemble des conditions découlant des art. 3 à 5 LSCPT sont remplies²⁸². A cet effet, il dispose d'un plein pouvoir de cognition sur toutes les questions de fait et de droit pertinentes²⁸³; les considérations d'opportunité, notamment celles qui touchent à la stratégie de l'enquête, devraient en revanche demeurer du seul ressort de l'autorité ayant ordonné la mesure.
152. Concrètement, le juge examinera successivement si l'infraction retenue figure au catalogue, si la prévention s'avère suffisante, si la gravité de l'acte justifie la surveillance et si cette dernière constitue bien l'*ultima ratio*. Il contrôlera en outre que la durée de la mesure est adéquate, que les limites posées aux branchements directs sont observées et que la surveillance de tiers obéit aux conditions supplémentaires de la loi. Il veillera enfin à ce que l'exécution de la mesure soit assortie des précautions nécessaires, notamment celles qui tendent à limiter l'accès aux informations étrangères à l'affaire²⁸⁴.

3 Délai

153. L'autorité judiciaire chargée d'approuver la surveillance dispose de 5 jours pour se déterminer et rendre sa décision²⁸⁵, fût-elle seulement provisoire²⁸⁶.

282 *Supra* n° 75–124; BIEDERMANN 96; HANSJAKOB, Art. 7 BÜPF n° 15.

283 OBERHOLZER 8.

284 *Infra* n° 197–201.

285 Art. 7 al. 3 phr. 2 LSCPT.

286 *Infra* n° 159.

Le délai court dès la transmission de l'ordre de surveillance au **154.** Service de surveillance²⁸⁷.

Conformément aux principes généraux régissant la supputation des **155.** délais non fixées en heures²⁸⁸, le premier jour n'est cependant pas compté. Si le juge d'instruction décerne un ordre de surveillance le 6 mars à 10 h 45, son autorité de tutelle doit donc se prononcer le 11 mars à minuit au plus tard.

Le délai est observé si l'autorité judiciaire compétente transmet à **156.** temps sa décision à ses destinataires. Peu importe donc que ces derniers ne reçoivent l'acte qu'après l'échéance²⁸⁹.

A l'instar des 24 heures de l'art. 7 al. 2 LSCPT²⁹⁰, les 5 jours de l'art. **157.** 7 al. 3 phr. 2 LSCPT représentent un délai d'ordre, dont le dépassement n'invalider pas la décision rendue²⁹¹.

4 Forme

La décision sur la demande d'autorisation de la surveillance doit re- **158.** vêtir la forme d'une ordonnance écrite, brièvement motivée en fait et en droit²⁹². Tantôt pratiquée sous l'empire de l'ancien droit, l'apposition d'un timbre ou d'une mention sur l'ordre de surveillance ou sur l'exposé des motifs qui l'accompagne ne suffit plus aujourd'hui²⁹³.

²⁸⁷ *Supra* n° 137.

²⁸⁸ Cf. art. 32 al. 1 OJ.

²⁸⁹ HANSJAKOB, Art. 7 BÜPF n° 16.

²⁹⁰ *Supra* n° 141.

²⁹¹ HANSJAKOB, Art. 7 BÜPF n° 16.

²⁹² Art. 7 al. 3 phr. 2 LSCPT; art. 6 OSCPT.

5 *Autorisation provisoire et demande d'informations complémentaires*

159. Si elle s'estime insuffisamment renseignée pour donner son approbation et qu'un refus pur et simple de sa part, avec ses conséquences drastiques²⁹⁴, s'avérerait disproportionné au regard de la gravité de l'infraction poursuivie, l'autorité judiciaire compétente peut autoriser la surveillance à titre provisoire et demander au magistrat en charge de l'enquête de compléter le dossier ou de lui apporter d'autres éclaircissements²⁹⁵. A cet effet, elle lui fixera un délai raisonnable pour s'exécuter, lequel ne devrait cependant pas dépasser 5 jours²⁹⁶.
160. Sitôt en possession des informations complémentaires sollicitées, l'autorité judiciaire devra statuer «définitivement» en accueillant ou en rejetant la demande d'autorisation de la surveillance. Il n'y aura pas de seconde navette.

6 *Mesures supplémentaires de protection de la personnalité et charges*

161. Conformément à l'art. 7 al. 3 phr. 3 et 4 LSCPT, le juge appelé à approuver la surveillance peut «exiger des mesures supplémentaires de protection de la personnalité» et rendre une décision positive «assortie de charges». Derrière ces formules peu explicites se cache simplement la faculté pour l'autorité compétente de délivrer l'autorisation tout en réformant l'ordre de surveillance dans le sens d'une limitation de l'atteinte à la sphère privée. Ainsi le juge pourra-t-il par exemple réduire la durée de la mesure, exclure un branchement direct ou renforcer les dispositions prises pour limiter l'accès aux informations étrangères à l'affaire²⁹⁷.

293 CONSEIL FÉDÉRAL 3718.

294 *Infra* n° 169–172.

295 Art. 7 al. 3 phr. 3 LSCPT.

296 Cf. art. 7 al. 3 phr. 2 LSCPT.

297 *Supra* n° 93–97; *infra* n° 197–201.

Toutes ces modifications devront figurer dans le dispositif de l'ordonnance d'approbation de la surveillance. **162.**

7 *Autorisation-cadre en cas de changements fréquents de raccordement*

Techniquement, la mise sous surveillance d'un second raccordement, **163.** d'un troisième, etc. constitue à chaque fois une nouvelle mesure soumise à l'approbation de l'autorité judiciaire compétente²⁹⁸. Pour alléger quelque peu – à vrai dire très modestement – la charge administrative qui pèse sur lui, le magistrat conduisant l'enquête peut solliciter une autorisation-cadre lorsque «l'enquête établit que le suspect change de raccordements à intervalles rapprochés»²⁹⁹.

En tant que telle, l'utilisation (directe ou indirecte) d'une pluralité **164.** de raccordements, par exemple celui du domicile, de la résidence secondaire, du bureau, de la voiture et du téléphone mobile, ne suffit pas³⁰⁰; le passage d'un raccordement à l'autre doit quasiment reposer sur une volonté de l'auteur présumé de brouiller les pistes ou de cloisonner son activité délictueuse. L'exemple classique est celui du revendeur de stupéfiants possédant un téléphone mobile dans lequel il insert successivement plusieurs cartes SIM, auxquelles correspondent donc autant de numéros d'appel différents susceptibles d'être surveillés. Dans ce cas toutefois, la parade des autorités de poursuite pénale résidera dans la mise sous surveillance de l'installation mobile elle-même, identifiable par son numéro IMEI.

Sans doute moins fréquente en pratique, l'hypothèse inverse du **165.** prévenu qui posséderait plusieurs téléphones portables alternativement connectés au réseau au moyen d'une carte SIM unique, devrait également tomber sous le coup de l'art. 4 al. 4 phr. 1 LSCPT. En

298 OBERHOLZER 5.

299 Art. 4 al. 4 phr. 1 LSCPT.

300 HANSJAKOB, Art. 4 BÜPF n° 34.

d'autres termes, la notion de «raccordement» ici employée revêt une acception large, non technique³⁰¹.

166. S'il bénéficie d'une autorisation-cadre, le juge d'instruction ou le procureur est dispensé de demander l'autorisation de la surveillance pour chaque nouveau raccordement ou téléphone mobile identifiés. La nécessité de décerner un nouvel ordre de surveillance subsiste en revanche³⁰². En lieu et place de la demande ponctuelle d'autorisation, le magistrat soumettra, une fois par mois et au moment de lever la mesure, à l'approbation de son autorité de tutelle un rapport mentionnant les surveillances ordonnées et les circonstances dans les- quelles elles l'ont été³⁰³.

8 *Destinataire et mode de transmission*

167. Après avoir statué, l'autorité compétente pour autoriser la surveillance communique immédiatement sa décision au Service de surveillance, ce que la loi prévoit expressément³⁰⁴, et au magistrat qui a ordonné la mesure, ce que la loi ne dit pas, mais qui va de soi.
168. D'un point de vue strictement juridique, une communication du seul dispositif suffit³⁰⁵. Pratiquement, une transmission intégrale de l'ordonnance est sans doute préférable. Pour ce faire, le télécopieur ou le coursier constituent assurément les moyens les plus appropriés³⁰⁶, mais le recours aux services de la Poste n'est pas prohibé.

301 HANSJAKOB, Art. 4 BÜPF n° 35.

302 Art. 4 al. 4 phr. 2 LSCPT.

303 Art. 4 al. 4 phr. 3 LSCPT.

304 Art. 7 al. 3 phr. 5 LSCPT; art. 6 OSCPT.

305 HANSJAKOB, Art. 7 BÜPF n° 16; cf. *supra* n° 162.

306 Cf. *supra* n° 145.

9 Conséquences du refus d'autoriser la surveillance

Lorsque l'autorité compétente refuse d'approver la surveillance, 169. d'emblée ou après avoir délivré une autorisation provisoire, la mesure doit immédiatement cesser de déployer ses effets. Il incombe au Service de surveillance de prendre les dispositions nécessaires dès l'instant où il reçoit la décision correspondante de l'autorité qui avait ordonné la mesure³⁰⁷.

Les envois postaux interceptés et retenus sont à acheminer à leurs 170. destinataires³⁰⁸; les éventuelles copies de leur contenu doivent être retirées du dossier et détruites³⁰⁹. En cas de surveillance des télécommunications, les supports de données (bandes magnétiques, disquettes, CD-ROM, etc.) contenant l'enregistrement des correspondances surveillées doivent être écartés de la procédure puis effacés, leurs transcriptions sur papier, détruites³¹⁰.

De la procédure de mise sous surveillance ne seront conservés que 171. l'ordre de surveillance, la demande d'autorisation et ses annexes, une éventuelle autorisation provisoire, enfin la décision refusant de ratifier la mesure.

Pour parachever la réglementation, l'art. 7 al. 4 phr. 3 LSCPT instaure 172. une interdiction absolue d'exploiter les informations recueillies avant que ne tombe le *veto* judiciaire, non seulement comme moyens de preuve, mais aussi comme moyens d'investigation. Si le lien de causalité requis est établi, l'impossibilité procédurale d'utiliser un élément issu de la surveillance peut donc déteindre sur un élément obtenu subséquemment d'une manière parfaitement légale en soi. Cette problématique, dite des «fruits de l'arbre empoisonné», est l'une des plus complexes et controversées du droit de procédure pénale³¹¹.

307 Art. 10 al. 1 LSCPT; *infra* n° 235, 238, 242.

308 Art. 7 al. 4 phr. 2 LSCPT.

309 Art. 7 al. 4 phr. 1 LSCPT.

310 *Ibidem*.

311 Cf. SCHMID 309–314 et les nombreuses références citées.

173. La question de savoir si le juge d'instruction ou le procureur ayant essuyé un refus de l'autorité compétente est en droit de revenir à la charge et d'ordonner une nouvelle surveillance appelle une réponse différenciée. Si la non-ratification repose sur des considérations de fond (prévention insuffisante, défaut de subsidiarité, disproportion, etc.)³¹², le magistrat doit apporter des faits nouveaux (*echte Nova*) ou nouvellement connus (*unechte Nova*) qui justifient une modification de l'appréciation originelle³¹³. Inversement, si le refus est uniquement motivé par l'inobservation de prescriptions de forme, par exemple la présentation d'une demande d'autorisation amplement tardive ou grossièrement lacunaire³¹⁴, rien ne s'oppose au renouvellement de la mesure moyennant le respect des formalités requises³¹⁵.

E Prolongation de la surveillance

I Demande

174. Confronté à la nécessité de faire durer la surveillance au-delà du temps pour lequel elle avait initialement été autorisée, le juge d'instruction ou le procureur peut en solliciter la prolongation pour une nouvelle période de 3 mois au plus³¹⁶. A cet effet, il est tenu d'adresser une demande motivée à l'autorité compétente pour approuver la mesure, en indiquant notamment les progrès effectués par son enquête³¹⁷. Sa requête devra en outre être communiquée au Service de surveillance³¹⁸ afin d'éviter que celui-ci ne mette fin à la surveillance à son échéance³¹⁹.

312 *Supra* n° 81–99.

313 Cf. HANSJAKOB, Art. 7 BÜPF n° 38 et la référence citée.

314 *Supra* n° 136–143.

315 Cf. ATF 109 Ia 324 consid. 3e, 120 IV 299–300 consid. 3e; Pr 89 (2000) n° 145 consid. 2b.

316 Art. 7 al. 5 phr. 1 LSCPT.

317 Art. 7 al. 5 phr. 2 LSCPT.

318 Art. 7 al. 5 phr. 3 LSCPT.

319 Art. 11 al. 1 let. d et 13 al. 1 let. g LSCPT; *infra* n° 235, 239.

La loi impose au magistrat d'effectuer les démarches précitées avant **175.** l'expiration de la mesure³²⁰, mais pas nécessairement plus de 5 jours auparavant, de manière à permettre au juge de statuer avant l'échéance³²¹. Fort curieusement, la «prolongation» de la surveillance peut ainsi intervenir postérieurement au terme fixé à l'origine.

2 *Décision*

Saisie d'une demande de prolongation de la surveillance, l'autorité **176.** mentionnée à l'art. 7 al. 1 LSCPT³²² procédera exactement selon les règles qui l'avaient amenée à autoriser la mesure³²³. Une décision négative de sa part, répercutee au Service de surveillance par le magistrat qui avait ordonné la mesure³²⁴, entraînera le retrait du dossier et l'inexploitabilité de toutes les informations recueillies postérieurement au terme initial de la surveillance, ainsi que l'effacement des supports de données et la destruction des documents correspondants³²⁵.

3 *Nouvelles demandes et nouvelles décisions*

Les opérations susmentionnées pourront être renouvelées autant de **177.** fois que l'autorise le respect du principe de la proportionnalité.

320 Art. 7 al. 5 phr. 1 LSCPT.

321 HANSJAKOB, Art. 7 BÜPF n° 41.

322 *Supra* n° 147–150.

323 *Supra* n° 151–168.

324 Art. 10 al. 1 LSCPT; *infra* n° 235, 238.

325 *Supra* n° 169–172.

V Exécution de la surveillance

A Surveillance de la correspondance par poste

1 Tâches du Service de surveillance

178. A réception d'un ordre de surveillance de la correspondance par poste, le Service de surveillance vérifie que celui-ci concerne une infraction figurant au catalogue de l'art. 3 al. 2–3 LSCPT et émane d'une autorité compétente selon l'art. 6 LSCPT³²⁶. En outre, il relèvera les erreurs manifestes et l'omission d'indications indispensables³²⁷, par exemple le dépassement des durées maximales prévues par les art. 5 al. 2 et 7 al. 3 phr. 4 LSCPT³²⁸ ou l'absence de mesures de protection des personnes tenues au secret professionnel³²⁹. Purement formel, le contrôle ne saurait en revanche porter – à supposer même qu'il s'avère possible – sur les conditions normatives de la mise sous surveillance que sont la gravité de l'acte, la subsidiarité de la mesure et l'existence d'une prévention suffisante³³⁰.
179. La détection d'un vice n'autorise pas le Service de surveillance à ne pas donner suite à un ordre par ailleurs exécutable, mais lui fait obligation d'attirer l'attention du juge d'instruction ou du procureur sur l'informalité et d'interdire au prestataire de services de mettre les envois interceptés à la disposition du magistrat ou de lui délivrer les informations requises³³¹.

326 Art. 11 al. 1 let. a phr. 1 LSCPT; *supra* n° 82, 126–128.

Afin de permettre au Service de surveillance d'effectuer ces deux vérifications, l'ordonnance prévoit que l'ordre de surveillance mentionnera l'infraction poursuivie (art. 11 let. e OSCPT) et que les cantons communiqueront le nom des autorités compétentes pour ordonner la mesure (art. 4 let. a OSCPT).

327 Art. 11 al. 1 let. a phr. 2 *in limine* LSCPT.

Le défaut de motivation de l'ordre de surveillance s'examinera à la lumière de l'art. 11 OSCPT, qui détaille le contenu nécessaire de cette décision (*supra* n° 129–130).

328 *Supra* n° 93–94.

329 CONSEIL FÉDÉRAL 3724.

330 HANSJAKOB, Art. 11 BÜPF n° 2 et 4; *supra* n° 89–92, 98–99.

331 HANSJAKOB, Art. 11 BÜPF n° 8.

Après avoir au besoin conseillé le magistrat en charge de l'instruction³³² et convenu avec lui d'un *modus operandi*³³³, le Service de surveillance détermine dans chaque cas particulier les mesures techniques et organisationnelles nécessaires à la mise en oeuvre de la surveillance³³⁴ puis communique les directives correspondantes aux fournisseurs de services postaux concernés³³⁵. S'agissant de l'obtention de données relatives au trafic et à la facturation³³⁶, d'une part, de renseignements complémentaires sur la correspondance par poste³³⁷, d'autre part, il aura préalablement examiné avec les entreprises considérées si les informations sollicitées sont disponibles, respectivement, si les demandes formulées peuvent être exécutées³³⁸.

Parallèlement aux tâches précitées, le Service de surveillance tient un registre des fournisseurs de services postaux³³⁹, établit une statistique des surveillances³⁴⁰ et suit l'évolution de la technique³⁴¹.

2 *Tâches des fournisseurs de services postaux*

Dans les limites de leurs obligations procédurales précédemment détaillées³⁴², les fournisseurs de services postaux exécutent les directives du Service de surveillance³⁴³ et l'informent de l'accomplissement de leur mission³⁴⁴. Dans le cas d'une surveillance en temps réel³⁴⁵, l'ouverture du contenant, l'examen du contenu, la duplication éventuelle de ces derniers, la remise du contenu dans le contenant et

332 Art. 11 al. 2 phr. 1 LSCPT.

333 Art. 13 al. 1 *in fine* OSCPT.

334 Art. 13 al. 1 *in limine* OSCPT.

335 Art. 11 al. 1 let. b LSCPT.

336 *Supra* n° 12.

337 *Supra* n° 9, 13.

338 Art. 13 al. 4 OSCPT.

339 Art. 11 al. 2 phr. 2 LSCPT.

340 Art. 11 al. 1 let. f LSCPT.

341 Art. 11 al. 1 let. g LSCPT.

342 *Supra* n° 61–62.

343 *Supra* n° 180.

344 Art. 13 al. 2 OSCPT.

345 *Supra* n° 7.

la fermeture de celui-ci incombent aux organes de justice et de police; conformément à l'art. 12 al. 1 phr. 1 LSCPT, l'entreprise postale intervient uniquement en amont et en aval de ces opérations, en mettant les plis et colis interceptés à disposition de l'autorité pénale, puis en les acheminant à leur destinataire.

183. Originaire ou subséquent, tout empêchement technique d'un fournisseur de services postaux de remplir ses obligations doit faire l'objet d'un avis immédiat auprès du Service de surveillance³⁴⁶.

3 *Emoluments et indemnités*

184. Sur la base d'un décompte que lui adressent les fournisseurs de services postaux requis³⁴⁷, le Service de surveillance facture à l'autorité qui a ordonné la mesure toutes les prestations fournies à celle-ci³⁴⁸ et rétrocède une partie de cet émolumennt à l'entreprise considérée à titre d'indemnité pour ses frais³⁴⁹.

B **Surveillance de la correspondance par télécommunication, accès à Internet compris**

1 *Tâches du Service de surveillance*

185. L'essentiel des tâches qui incombent au Service de surveillance dans le cadre de l'exécution d'une mesure de surveillance de la correspondance postale³⁵⁰ s'imposent également à lui lorsqu'il est saisi

346 Art. 13 al. 3 OSCPT.

347 Art. 31 al. 2 OSCPT.

348 Art. 31 al. 1 OSCPT.

349 Art. 16 al. 1 LSCPT; art. 30 al. 1 OSCPT.

Pour les détails relatifs à la composition et au montant de l'émolumennt, voir les art. 16 al. 2 LSCPT, 30 al. 2–3 OSCPT et 3 ch. 6 OEIS.

350 *Supra* n° 178–181.

d'un ordre de surveillance de la correspondance par télécommunication, accès à Internet compris³⁵¹.

En outre, le Service de surveillance reçoit par déviation vers son **186.** Centre de traitement³⁵² les communications qui transitent par le raccordement, le téléphone mobile ou l'adresse électronique surveillés, les enregistre puis remet les supports de données et les documents³⁵³ à l'autorité qui a ordonné la surveillance³⁵⁴; les paramètres qui caractérisent ces correspondances³⁵⁵ et les données relatives au trafic et à la facturation³⁵⁶ suivent le même cheminement³⁵⁷. Sur demande, le Service de surveillance peut également être chargé de trier les communications interceptées³⁵⁸, de transcrire (ou d'imprimer) sur papier leur enregistrement et de traduire ces transcriptions si elles apparaissent dans une langue étrangère³⁵⁹. Lorsque l'autorité judiciaire compétente a ordonné un branchement direct³⁶⁰, il veille à l'installation de celui-ci mais n'enregistre pas les communications, à moins d'en avoir été spécialement requis³⁶¹. En dernier lieu, le Service de surveillance peut se voir imposer par le juge qui a autorisé la surveillance de mettre en oeuvre les mesures supplémentaires de protection de la personnalité qu'il a ordonnées³⁶².

351 Voir successivement les art. 13 al. 1 let. a (examen de l'ordre de surveillance), 13 al. 1 let. b (directives aux fournisseurs de services de télécommunication), 13 al. 1 let. j (statistique des surveillances), 13 al. 1 let. k (suivi de l'évolution technique) et 13 al. 2 let. e LSCPT (conseils techniques), ainsi que les art. 17 al. 1 et 25 al. 1 let. a OSCPT (détermination des mesures techniques et organisationnelles).

352 *Supra* n° 68.

353 Sur ces deux dernières notions, voir *infra* n° 207–209.

354 Art. 13 al. 1 let. c LSCPT.

Dans le cas visé par les art. 17 al. 2 et 25 al. 2 OSCPT, le Service de surveillance se voit toutefois interdit de remettre les supports de données et les documents au magistrat en charge de l'enquête (*infra* n° 202).

355 *Supra* n° 27.

356 *Supra* n° 29.

357 Art. 13 al. 1 let. e LSCPT.

358 Cf. *infra* n° 202–205, 206, 211–213.

359 Art. 13 al. 2 let. b–d LSCPT.

360 *Supra* n° 95.

361 Art. 13 al. 1 let. d et al. 2 let. a LSCPT.

362 Art. 13 al. 1 let. f LSCPT; cf. *supra* n° 161 et *infra* n° 197–201.

187. Dans le cas particulier de la surveillance de télécommunications à l'intérieur d'un réseau interne ou d'un central domestique, le Service de surveillance devra procéder lui-même à l'ensemble des opérations d'exécution de la mesure si l'exploitant refuse de s'en charger ou ne dispose pas des équipements adéquats³⁶³.

2 *Tâches des fournisseurs de services de télécommunication et des fournisseurs d'accès à Internet*

188. Dans les limites de leurs obligations procédurales³⁶⁴, les fournisseurs de services de télécommunication et d'accès à Internet sont principalement tenus de dévier vers le Centre de traitement les communications concernées par la mesure, de rassembler les autres informations requises et de les remettre au Service de surveillance. Ils doivent faire en sorte que la surveillance demeure imperceptible pour les personnes en correspondance et que les informations recueillies échappent à toute utilisation non autorisée ou abusive³⁶⁵.
189. Pour le surplus, les tâches des entreprises considérées correspondent à celles qui incombent également aux fournisseurs de services postaux³⁶⁶.

3 *Renseignements sur les raccordements de télécommunication et les usagers d'Internet*

190. Afin d'identifier les titulaires de numéros d'appel ou d'adresses e-mail apparus lors de la surveillance, cette dernière sera, le cas échéant, suivie d'une demande de renseignements sur les raccordements de télécommunication et les usagers d'Internet³⁶⁷.

363 Pour les détails, voir les art. 28–29 OSCPT.

364 *Supra* n° 63–64.

365 Art. 17 al. 6 et 25 al. 5 OSCPT.

366 *Supra* n° 182–183.

Voir notamment les art. 17 al. 3 et 25 al. 3 (annonce de l'exécution de la mesure), 17 al. 5 et 25 al. 4 OSCPT (avis en cas d'empêchement technique d'exécuter la surveillance).

367 *Supra* n° 40–44.

4 ***Emoluments et indemnités***

La perception des émoluments et l'allocation des indemnités obéissent aux règles précédemment établies en relation avec la surveillance de la correspondance postale³⁶⁸.

Une remarque complémentaire s'impose toutefois. En matière de surveillance des télécommunications, les tarifs imposés sont tout simplement prohibitifs. Sur le modèle de ce qui se pratique dans les relations entre les banques et les autorités pénales leur intimant l'ordre de produire des documents, la coopération des fournisseurs de services de télécommunication devrait être gratuite!

C *Addendum: utilisation d'appareils techniques de surveillance*

1 Tâches de la police

L'exécution d'une surveillance au moyen d'appareils techniques ne pose pas de problèmes particuliers. En règle générale, le magistrat conduisant l'instruction confiera cette mission à ses services de police, dont les fonctionnaires desserviront les instruments d'écoute, d'enregistrement, d'observation ou de prise de vues.

2 Collaboration de particuliers

S'ils y consentent, des particuliers peuvent être associés à l'exécution de la surveillance, leur collaboration pouvant aller de la simple mise à disposition du matériel nécessaire jusqu'à son installation et son exploitation. Dans ce dernier cas, une étroite supervision policière ou judiciaire des opérations s'impose.

³⁶⁸ *Supra* n° 184.

Pour les détails relatifs à la composition et au montant des émoluments, voir les art. 16 al. 2 LSCPT, l'art. 30 al. 2-3 OSCPT, les art. 2, 3 ch. 1-5, 4-6 OEIS et l'annexe à l'OSCPT.

D Prescriptions communes

195. La mise en oeuvre d'une mesure de surveillance s'apparente au déploiement d'un filet de pêche formé de mailles suffisamment étroites pour retenir et ramener à la surface des bicyclettes rouillées et de vieilles chaussures, d'une part, des poissons appartenant à une espèce protégée, d'autre part. En termes juridiques: des informations ne présentant aucun rapport avec les faits à élucider, d'une part, des informations dont la loi interdit l'exploitation, d'autre part.
196. Conscient de ce double écueil, le législateur s'est donné la peine – et en a eu – d'entourer l'exécution des mesures de surveillance de différents garde-fous.

I Accès aux informations étrangères à l'objet de l'enquête

197. En cas de surveillance d'un tiers³⁶⁹, d'un raccordement public ou anonyme³⁷⁰ et d'une personne tenue au secret professionnel (auteur présumé ou tiers)³⁷¹, ainsi qu'en cas de changements fréquents de raccordement³⁷², l'art. 4 al. 5 LSCPT fait obligation à l'autorité ayant ordonné la mesure de veiller à ce que «les personnes qui mènent l'enquête ne puissent pas prendre connaissance d'informations étrangères à l'objet de l'enquête».
198. Raisnable de prime abord, cette disposition n'en soulève pas moins un sérieux problème d'interprétation. D'aucuns considèrent même que la norme est d'application impossible dans la mesure où la séparation des informations pertinentes à l'action publique de celles sans rapport avec elle passe nécessairement par la remise aux agents chargés du tri d'un minimum d'indications quant aux infrac-

369 *Supra* n° 107–112.

370 *Supra* n° 113–115.

371 *Supra* n° 75–104 et 116–124.

372 *Supra* n° 163–166.

tions poursuivies, à leurs auteurs présumés et au complexe de faits qui les sous-tend; or cette circonstance suffirait déjà à faire desdits agents des «personnes qui mènent l'enquête»³⁷³.

Quitte à sacrifier la lettre de la loi au profit de son esprit, une première manière d'échapper au cercle vicieux consisterait à imposer au magistrat en charge de l'instruction d'effectuer lui-même le tri. Au regard de la masse des informations à traiter, une telle solution s'avère toutefois largement impraticable lorsqu'une surveillance des télécommunications, accès à Internet compris, est en jeu.

La seconde échappatoire³⁷⁴ résiderait dans le recours systématique au Service de surveillance pour trier les données interceptées³⁷⁵. S'engouffrer dans cette voie reviendrait cependant à priver *de facto* les autorités de poursuite et d'instruction de l'instrument du branchement direct, par ailleurs seulement prohibé en relation avec la surveillance de personnes tenues au secret professionnel³⁷⁶.

A ce jour, la porte de sortie n'a pas encore été trouvée et on peut douter qu'elle existe³⁷⁷. Une fois de plus, il appartiendra au Tribunal fédéral de donner un sens à une règle de droit insuffisamment pensée.

2 *Tri des informations en cas de surveillance d'une personne tenue au secret professionnel*

Les incertitudes susmentionnées affectent également l'art. 4 al. 6 phr. 1 LSCPT. Ajoutant un degré supplémentaire à la protection des personnes astreintes au secret professionnel (auteur présumé ou

373 JEAN-RICHARD-DIT-BRESSEL 48; voir aussi HANSJAKOB, *Erfahrungen* 276.

374 Cf. HANSJAKOB, *Erfahrungen* 277.

375 Art. 13 al. 2 let. d LSCPT; *supra* n° 186.

376 *Supra* n° 97.

377 Cf. HANSJAKOB, Art. 4 BÜPF n° 44–46, dont les propositions opèrent toutes en aval d'une prise de connaissance des correspondances surveillées par les personnes chargées d'en faire le tri.

tiers), cette disposition prévoit que le tri des informations recueillies sera «exécuté sous la surveillance d'une autorité judiciaire qui n'est pas saisie du dossier d'enquête». Les art. 17 al. 2 et 25 al. 2 OSCPT complètent la réglementation en remplaçant l'obligation faite au Service de surveillance, s'il devait constater qu'aucune mesure adéquate n'a été ordonnée, de transmettre les supports de données et les documents à l'autorité qui a ordonné la mesure³⁷⁸ par celle d'aviser le juge qui l'a autorisée.

- 203.** Concrètement, la loi fait ici interdiction au magistrat ayant ordonné la surveillance de l'adresse postale, du raccordement de télécommunication ou de la boîte aux lettres électronique d'un confident nécessaire de trier personnellement le bon grain de l'ivraie ou simplement de piloter l'opération. Cette tâche doit impérativement revenir à un juge ou un tribunal qui n'est pas en charge de l'enquête préliminaire ou de l'instruction préparatoire. D'une certaine manière, la séparation des fonctions d'investigation et de triage ici instaurée correspond à celle qui caractérise la procédure de levée des scellés (*Entsiegelungsverfahren*) susceptible d'émailler une perquisition visant des papiers³⁷⁹. L'objectif poursuivi est de soustraire à la sagacité du juge d'instruction ou du procureur les éléments dont la connaissance est inutile à l'accomplissement de sa mission ou dont l'exploitation comme moyen de preuve est prohibée par la loi³⁸⁰.
- 204.** En procédure genevoise, la supervision du tri incombe *ex lege* au président de la Chambre d'accusation³⁸¹, celui-là même qui avait précédemment autorisé la surveillance³⁸². Ce cumul des attributions est rationnel au vu des art. 9 al. 2 et 8 al. 4 LSCPT³⁸³, qui confient à l'autorité d'approbation de la surveillance la tâche de statuer au be-

378 *Supra* n° 186.

379 En droit fédéral, voir les art. 69 al. 3 PPF, 50 al. 3 DPA, 67 al. 3 PPM.

380 Cf. art. 4 al. 6 phr. 2 LSCPT; *infra* n° 206–214.

381 Art. 48A al. 2 let. b LACP, dans sa teneur selon la loi n° 8732 du 16 mai 2003 (FAO 57/23.5.2003 p. 23).

382 *Supra* n° 150.

383 Cf. HANSJAKOB, Art. 4 BÜPF n° 53.

soin sur l'utilisation contre le confident nécessaire³⁸⁴ d'informations couvertes par le secret professionnel³⁸⁵.

Théoriquement, le juge désigné pourrait procéder au tri en personne; pratiquement, il donnera les injonctions nécessaires au Service de surveillance³⁸⁶. En toute hypothèse, c'est lui seul qui décidera quelles informations (jugées pertinentes et exploitables) seront finalement remises au magistrat conduisant les investigations afin d'être versées au dossier.

3 Traitement des informations inutiles à la procédure

Toute mesure de surveillance, on l'a dit, confronte les autorités de poursuite et d'instruction pénale à un volume important d'informations sans intérêt pour la manifestation de la vérité. L'art. 8 al. 1 LSCPT s'attache à régler leur sort en prévoyant que «les documents qui ne sont pas nécessaires à la procédure doivent être conservés séparément du dossier et détruits immédiatement après la clôture de la procédure pénale, d'entraide judiciaire ou d'extradition».

D'après les travaux préparatoires³⁸⁷, l'évocation des seuls documents, à l'exclusion donc des supports de données mentionnés par ailleurs aux art. 7 al. 4 phr. 1³⁸⁸ et 9 al. 3 phr. 2 LSCPT³⁸⁹, serait délibérée. Sous l'angle de la *ratio legis*, le résultat ne manque pas de surprendre. Selon le type de mesure ordonnée, en effet, l'objectif de protection de la sphère privée est tantôt atteint, tantôt manqué.

S'agissant d'une surveillance qui engendre exclusivement des pairs, par exemple l'interception du courrier ensuite acheminé à son

384 *Infra* n° 222–224.

385 *Infra* n° 214.

386 Cf. art. 13 al. 2 let. d LSCPT; HANSJAKOB, Art. 4 BÜPF n° 51; *supra* n° 186.

387 HANSJAKOB, Art. 8 BÜPF n° 5–6 et les références citées.

388 *Supra* n° 170.

389 *Infra* n° 227.

destinataire³⁹⁰, l'art. 8 al. 1 LSCPT constraint l'autorité en charge de l'enquête de verser le produit direct de la mesure (photocopies des écrits retenus) – et ses éventuels duplicata – dans un dossier fantôme, inaccessible aux parties même après la levée de la mesure. Ce dossier sera ultérieurement détruit sur ordre de la dernière autorité saisie de la cause; à Genève, il s'agira du procureur général s'il abandonne les poursuites³⁹¹, de la Chambre d'accusation en cas de non-lieu³⁹² et du juge du fond après des débats³⁹³. La loi dresse ici un rempart assurément adéquat contre toute utilisation abusive des renseignements recueillis.

- 209.** Tel n'est en revanche nullement le cas lorsque la surveillance vise des conversations téléphoniques, l'échange de SMS ou encore la correspondance par e-mail. Dans toutes ces situations, l'enregistrement sur un support de données³⁹⁴ aura précédé l'éventuelle transcription des informations sur le papier. En imposant la destruction du second tout en tolérant la conservation du premier, les Chambres fédérales ont, en violation des art. 13 al. 2 Cst., 8 par. 1 CEDH et 17 par. 1 PIDCP, failli à leur devoir de sauvegarder la vie privée du citoyen.
- 210.** Le report de la destruction des documents (et des supports de données!) à la fin de la procédure, c'est-à-dire au moment où la décision mettant un terme à l'action publique entre en force et devient exécutoire, se justifie par la nécessité pour les autorités de jugement et/ou de recours de revoir au besoin le tri effectué à l'origine par le magistrat qui avait ordonné la surveillance et de verser au dossier des pièces dont l'utilité aurait été méconnue ou ne serait apparue qu'après coup.

390 Demeure réservée l'utilisation de moyens informatiques, notamment un scanner, pour copier les correspondances interceptées.

391 Art. 116 al. 1, 198 al. 1 CPP.

392 Art. 204 al. 1 CPP.

393 Art. 229, 245 al. 1, 327 CPP. En cas d'ordonnance de condamnation (art. 218–218 F CPP), l'ordre de destruction émanera du procureur général (art. 115 al. 4, 198 al. 3 CPP) ou du juge d'instruction (art. 185 al. 2 CPP), qui s'érigent ici en juge du fond.

394 Bandes magnétiques, disquettes, CD-ROM, etc.

4 **Traitement des informations couvertes par le secret professionnel**

A l'instar de l'art. 8 al. 1 précité, l'art. 8 al. 3 LSCPT, censé déterminer le sort des informations couvertes par le secret professionnel, se borne à prévoir le retrait du dossier et la destruction – immédiate ici – des «documents y relatifs». Le passage sous silence des supports de données est d'autant moins compatible avec les art. 13 al. 2 Cst., 8 par. 1 CEDH et 17 par. 1 PIDCP que les informations dont la préservation est de la sorte assurée sont hautement sensibles et appellent une protection accrue.

Moyennant l'extension de son champ d'application aux supports de données, l'art. 8 al. 3 LSCPT s'adresse tout d'abord à l'autorité qui a ordonné la surveillance d'un auteur présumé ou d'un tiers non tenus au secret professionnel et qui recueille fortuitement des renseignements couverts par celui-ci. L'illustration classique est celle du délinquant dont la ligne téléphonique est placée sur écoute et qui parle avec son défenseur, son psychiatre ou son pasteur des infractions qui lui sont imputées. En pareille situation, le juge d'instruction ou le procureur ne peut pas ne pas prendre connaissance de la correspondance dès lors que c'est à lui de décider s'il doit l'écartier du dossier, *recte ne pas* même l'y verser, et procéder à son élimination physique.

L'art. 8 al. 3 LSCPT s'adresse ensuite à l'autorité chargée en vertu de l'art. 4 al. 6 LSCPT³⁹⁵ de contrôler le tri lorsque la surveillance vise, comme auteur présumé ou comme tiers, un confident nécessaire³⁹⁶. A Genève, il appartiendra par exemple au président de la Chambre d'accusation³⁹⁷ de remettre dans le circuit de distribution postale le pli par lequel un avocat soupçonné de blanchiment aggravé d'argent et surveillé pour ce motif reçoit de l'un de ses clients des aveux de meurtre; de même, il devra retenir puis (faire) détruire toute trace

³⁹⁵ *Supra* n° 202–203 et 205.

³⁹⁶ Cf. SCHMID 301. *Contra: HANSJAKOB*, Art. 8 BÜPF n° 19.

³⁹⁷ *Supra* n° 204.

de l'appel téléphonique au cours duquel un patient dévoile ses comportements pédophiles à son médecin traitant, dont la ligne est surveillée parce que son assistante est suspectée de se livrer au trafic aggravé de stupéfiants depuis le cabinet.

- 214.** L'impossibilité juridique d'exploiter au titre de la preuve des informations relevant du secret professionnel trouve ses limites lorsque le confident nécessaire s'avère être lui-même l'auteur d'une infraction figurant au catalogue de l'art. 3 al. 2–3 LSCPT. Faisant écho à l'art. 4 al. 3 let. a, l'art. 8 al. 4 LSCPT rappelle expressément ce principe³⁹⁸, mais subordonne l'utilisation du résultat de la surveillance à l'autorisation du juge des art. 179^{octies} al. 1 CP et 7 al. 1 LSCPT³⁹⁹. Cette probation coïncidera généralement avec celle prévue par l'art. 9 al. 2 LSCPT⁴⁰⁰; elle prendra nécessairement la forme d'une démarche spontanée lorsque le magistrat compétent est également chargé de trier les renseignements rassemblés dans le cadre de la surveillance d'une personne astreinte au secret professionnel⁴⁰¹.

5 *Traitements des découvertes fortuites*

- 215.** Le traitement juridique de ce que la terminologie allemande appelle les *Zufallsfunde* représente sans doute l'une des principales pierres d'achoppement du nouveau droit. Trois situations doivent être distinguées.
- a) Découverte d'autres infractions imputables à l'auteur présumé*
- 216.** Lorsque la surveillance de l'adresse postale, du raccordement de télécommunication ou de l'adresse électronique d'un auteur présumé ou d'un tiers, ordonnée en raison d'une infraction déterminée, révèle la participation (principale ou accessoire) du premier nommé

398 Cf. ATF 125 I 50 et les références citées.

399 *Supra* n° 147.

400 *Infra* n° 222–224; SCHMID 302.

401 Cf. OBERHOLZER 13.

à une autre infraction, les éléments ainsi obtenus peuvent être utilisés comme moyens de preuve contre lui dans deux hypothèses distinctes, quoique complémentaires:

- si l'infraction nouvellement apparue a été commise en sus de celle initialement suspectée⁴⁰²;
- si l'infraction nouvellement apparue remplit les conditions posées par la loi à une mise sous surveillance⁴⁰³.

L'art. 9 al. 1 let. a LSCPT ouvre la voie à une condamnation pour un **217.** crime, un délit ou une contravention⁴⁰⁴ qui, isolément considérés, n'auraient pas pu faire l'objet d'une mesure de surveillance faute de satisfaire aux exigences de l'art. 3 LSCPT, par exemple une injure⁴⁰⁵, des menaces sans gravité⁴⁰⁶ ou une escroquerie susceptible d'être établie grâce à la saisie de pièces⁴⁰⁷. Cette infraction doit cependant avoir été perpétrée «en plus», condition assurément remplie si son auteur est reconnu coupable au moins de l'un des «actes punissables» à l'origine de la surveillance⁴⁰⁸. Au regard de la lettre de l'art. 9 al. 1 let. a LSCPT, une telle déclaration de culpabilité n'est toutefois pas nécessaire dès lors que l'accusé acquitté ou mis au bénéfice d'un non-lieu ensuite de l'intervention d'un fait justificatif⁴⁰⁹ ou d'une clause d'excution⁴¹⁰ aura, lui aussi, typiquement «commis» l'infraction considérée⁴¹¹. Selon la même logique, un classement en pure opportunité⁴¹² des charges qui avaient motivé la surveillance ne saurait faire obstacle à l'utilisation d'un *Zufallsfund* dans le cadre de poursuites limitées aux agissements répréhensibles que ce dernier a mis en lumière. Cas échéant, il appartiendra donc au juge du fond

402 Art. 9 al. 1 let. a LSCPT.

403 Art. 9 al. 1 let. b LSCPT.

404 HANSJAKOB, Art. 9 BÜPF n° 11; SCHMID 290.

405 Art. 177 al. 1 CP; cf. art. 3 al. 1 let. a LSCPT; *supra* n° 82–88.

406 Art. 180 CP; cf. art. 3 al. 1 let. b LSCPT; *supra* n° 89–90.

407 Art. 146 CP; cf. art. 3 al. 1 let. c LSCPT; *supra* n° 91–92.

408 SCHMID 291; cf. aussi HANSJAKOB, Art. 9 BÜPF n° 13.

409 Art. 32–34 CP.

410 Irresponsabilité (art. 10 CP), erreur de droit inévitable (art. 20 CP; cf. ATF 120 IV 316–317), état de nécessité absolutoire (art. 34 CP), etc.

411 SCHMID 291 note 30.

412 Art. 116 al. 1 hypo. 2, 198 al. 1 CPP; cf. ATF 119 IV 100–102 consid. 2h–3, 120 IV 42–43 consid. 3, 120 IV 109–112 consid. 2c.

saisi d'une action publique tronquée de déterminer à titre préjudiciel si les infractions abandonnées par l'accusation étaient ou non réalisées.

218. Au-delà des problèmes d'interprétation que suscite l'art. 9 al. 1 let. a LSCPT, le concept qui sous-tend cette disposition est largement critiquable⁴¹³. En faisant dépendre la possibilité d'utiliser une preuve intéressant une infraction déterminée (donc une question formelle surgissant tout au long de la procédure) de la réalisation d'une infraction sans autre rapport avec la première que l'identité de leur auteur (donc d'une question de fond qui ne sera tranchée qu'à l'issue des débats, voire plus tard encore dans le cadre d'une procédure séparée), le législateur entretient une incertitude dont la conséquence ultime résidera dans la nécessité de déposer une demande en révision s'il s'agit d'obtenir l'annulation d'une condamnation définitive (c'est-à-dire entrée en force de chose jugée) pour un délit découvert fortuitement lorsque son auteur est ultérieurement acquitté *in dubio pro reo* de l'infraction qui avait conduit à sa mise sous surveillance.
219. Alternativement aux conditions précitées, l'art. 9 al. 1 let. b LSCPT autorise les différentes juridictions pénales, du procureur au juge du fond en passant par le juge d'instruction, d'utiliser les informations relatives à une infraction dont la poursuite aurait justifié une mesure de surveillance. La formulation légale donne à penser que toutes les conditions découlant de l'art. 3 LSCPT doivent effectivement être remplies. En réalité, la nature même des découvertes fortuites impose certaines dérogations. Sous l'empire de l'ancien droit déjà, le Tribunal fédéral avait considéré qu'une prévention suffisante préexistante⁴¹⁴ ne pouvait pas être requise⁴¹⁵. Il doit en aller de même avec

413 Cf. HANSJAKOB, Art. 9 BÜPF n° 13; OBERHOLZER 14; SCHMID 290–291.

414 *Supra* n° 98–99.

415 ATF 122 I 195–196 consid. 5b/aa; voir aussi CONSEIL FÉDÉRAL 3721; HANSJAKOB, Art. 9 BÜPF n° 14; JEAN-RICHARD-DIT-BRESSEL 55–56; OBERHOLZER 14; SCHMID 293.

l'exigence de subsidiarité⁴¹⁶ et les conditions propres à la surveillance d'un tiers⁴¹⁷. Il est en revanche impératif que les éléments mis en lumière pointent en direction d'une infraction qui figure au catalogue⁴¹⁸ et présente la gravité voulue⁴¹⁹.

Les deux hypothèses envisagées par l'art. 9 al. 1 LSCPT se laissent **220**. également combiner, en ce sens qu'une infraction nouvelle ne remplaissant pas les conditions de l'art. 3 LSCPT peut aussi avoir été commise en plus (let. a) d'une autre infraction nouvelle qui satisfait à cette exigence (let. b)⁴²⁰. Si la surveillance d'un faux monnayeur présumé ne permet pas d'établir une violation de l'art. 240 al. 1 CP, mais révèle que l'intéressé falsifie des titres⁴²¹ et contrevient en outre à ses obligations d'entretien⁴²², tous les éléments de preuve recueillis sont exploitables. En d'autres termes, il suffit aux fins de l'art. 9 al. 1 LSCPT que l'existence d'une infraction sujette à surveillance soit démontrée pour que l'ensemble des informations rassemblées grâce à la mesure puissent être utilisées contre l'auteur.

A l'inverse de ce que prévoit l'art. 9 al. 2 LSCPT⁴²³, l'exploitation **221**. d'une découverte fortuite n'est pas subordonnée, ici, à l'approbation de l'autorité compétente pour autoriser la surveillance⁴²⁴.

b) Découverte de participants à l'infraction poursuivie et d'infractions imputables à d'autres personnes

Lorsque la mise en oeuvre d'une surveillance révèle des charges à **222**. l'encontre d'un individu qui ne figure pas comme auteur présumé

⁴¹⁶ *Supra* n° 91–92; voir CONSEIL FÉDÉRAL 3721; HANSJAKOB, Art. 9 BÜPF n° 14; JEAN-RICHARD-DIT-BRESSEL 56; SCHMID 294.

⁴¹⁷ *Supra* n° 105–124; voir SCHMID 300–301.

⁴¹⁸ *Supra* n° 82–88; voir CONSEIL FÉDÉRAL 3721; HANSJAKOB, Art. 9 BÜPF n° 14; JEAN-RICHARD-DIT-BRESSEL 57; SCHMID 292.

⁴¹⁹ *Supra* n° 89–90; voir CONSEIL FÉDÉRAL 3721; HANSJAKOB, Art. 9 BÜPF n° 14; JEAN-RICHARD-DIT-BRESSEL 57; Schmid 294.

⁴²⁰ HANSJAKOB, Art. 9 BÜPF n° 15; SCHMID 291–292.

⁴²¹ Art. 251 ch. 1 CP.

⁴²² Art. 217 al. 1 CP.

⁴²³ *Infra* n° 222–224.

⁴²⁴ HANSJAKOB, Art. 9 BÜPF n° 17; JEAN-RICHARD-DIT-BRESSEL 57; SCHMID 297–298.

dans l'ordre *ad hoc*⁴²⁵ (personne initialement ni suspectée ni surveillée, suspectée mais non surveillée, surveillée [comme tiers] mais non suspectée), l'ouverture d'une action publique contre celui-ci et l'utilisation à son endroit des preuves obtenues nécessite l'approbation de l'autorité compétente pour autoriser la mesure⁴²⁶.

223. L'accomplissement de cette formalité s'impose dès l'instant où⁴²⁷ la surveillance de l'adresse postale, du téléphone mobile, du raccordement de télécommunication ou de l'adresse électronique

- d'un auteur présumé, lui-même participant principal ou accessoire, dévoile la participation principale (activité directe, coactivité, activité médiate) ou accessoire (instigation, complicité) d'une autre personne à l'infraction poursuivie;
- d'un auteur présumé fait apparaître à la charge d'une autre personne, comme participant principal ou accessoire, la commission d'une infraction distincte de celle qui a motivé la mesure;
- d'un tiers dévoile la participation principale ou accessoire d'une autre personne à l'infraction de l'auteur présumé;
- d'un tiers fait apparaître à la charge d'une autre personne, comme participant principal ou accessoire, la commission d'une infraction distincte de celle qui a motivé la mesure;
- d'un tiers dévoile sa propre participation, principale ou accessoire, à l'infraction de l'auteur présumé;
- d'un tiers fait apparaître à sa propre charge, comme participant principal ou accessoire, la commission d'une infraction distincte de celle qui a motivé la mesure.

224. Avisé par le procureur ou le juge d'instruction d'un tel état de fait, ou s'y trouvant directement confronté lors du tri des informations recueillies⁴²⁸, le juge des art. 179^{octies} al. 1 CP et 7 al. 1 LSCPT⁴²⁹ examinera si «les conditions pour une surveillance au sens de la [...] loi

⁴²⁵ *Supra* n° 216–221.

⁴²⁶ Art. 9 al. 2 phr. 1 LSCPT dans sa version allemande, trahie en plusieurs endroits par le texte français.

⁴²⁷ HANSJAKOB, Art. 9 BÜPF n° 18–20; SCHMID 296, 300–301.

⁴²⁸ *Supra* n° 202–205.

⁴²⁹ *Supra* n° 147.

sont remplies»⁴³⁰. En réalité, il se bornera à vérifier que l'infraction considérée est mentionnée au catalogue de l'art. 3 al. 2-3 LSCPT et présente la gravité requise par l'art. 3 al. 1 let. b LSCPT⁴³¹. Contrairement à ce qu'indique le texte légal, la réalisation de ces deux conditions ne confère pas au magistrat la simple faculté de délivrer son autorisation; elle lui en fait l'obligation⁴³².

En l'absence de cette approbation, les autorités de poursuite et d'instruction pénale ont l'interdiction de procéder contre l'individu considéré, notamment de le soumettre à un interrogatoire, de l'inculper ou de le placer en détention préventive, à moins naturellement que son activité délictueuse démontrée par le *Zufallsfund* avait antérieurement déjà motivé l'ouverture d'une action publique contre lui⁴³³. En toute hypothèse, l'approbation est nécessaire pour exploiter les découvertes fortuites. Une fois donnée, elle couvrira également l'utilisation d'informations que la surveillance en cours pourrait ultérieurement amener⁴³⁴ et permettra, cas échéant, la prise en considération d'éléments de preuve intéressant d'autres infractions commises par l'auteur nouvellement identifié, conformément à l'art. 9 al. 1 let. a-b LSCPT⁴³⁵.

La finalité de la réglementation instaurée par l'art. 9 al. 2 LSCPT demeure pour le moins obscure. On a singulièrement peine à comprendre pourquoi une autorisation judiciaire est indispensable ici et non dans le cadre de l'art. 9 al. 1 LSCPT. Sur un plan théorique d'abord, l'art. 9 al. 2 LSCPT déroge sans justification aucune au principe de la saisine *in rem* des juridictions d'instruction⁴³⁶ lorsque surgissent de nouveaux participants à l'infraction poursuivie. Sur un plan pratique ensuite, les démarches qu'impose l'obtention de l'autorisation sont

430 Art. 9 al. 2 phr. 2 LSCPT.

431 HANSJAKOB, Art. 9 BÜPF n° 21; SCHMID 297, 300–301; cf. *supra* n° 219.

432 HANSJAKOB, Art. 9 BÜPF n° 26; SCHMID 298.

433 SCHMID 299.

434 SCHMID 300.

435 *Supra* n° 216–221; SCHMID 298–299. *Contra*: HANSJAKOB, Art. 9 BÜPF n° 31.

436 Cf. art. 111 PPF, 111 PPM, 119–120 CPP; voir aussi ATF 128 IV 83 consid. 2a.

susceptibles d'offrir aux délinquants pourtant démasqués le temps de se soustraire à l'intervention des organes de l'Etat⁴³⁷. D'une manière plus générale enfin, on ne voit pas à quoi peuvent bien servir les contrôles «préventifs» prévus par les art. 8 al. 4 et 9 al. 2 LSCPT dès lors que les juridictions de jugement et de recours appelées à connaître de la cause en fin de parcours auront, quoi qu'il arrive, le droit et le devoir d'écartier du dossier les preuves ne répondant pas aux exigences de la loi; la multiplication des contraintes administratives est assurément le plus mauvais moyen de garantir l'observation de la loi.

c) *Inexploitabilité d'autres découvertes fortuites*

227. En marge des situations précitées⁴³⁸, il n'y a plus aucune place pour l'exploitation procédurale de découvertes fortuites. L'art. 9 al. 3 LSCPT prévoit en effet que de telles «informations ne peuvent pas être utilisées» et que «les supports de données et les documents en question doivent être détruits immédiatement».
228. Cette réglementation conduit probablement à des résultats encore acceptables lorsque la surveillance dirigée contre un meurtrier présumé ne permet pas de lui imputer d'infraction à l'art. 111 CP, mais révèle que l'intéressé s'adonne à la soustraction d'impôt⁴³⁹, organise l'entrée illégale d'étrangers en Suisse⁴⁴⁰ ou conduit en état d'ébriété⁴⁴¹.
229. Un certain malaise surgit lorsque la mise sur écoute téléphonique d'un voleur agissant par métier⁴⁴² confirme les soupçons, mais dévoile en outre la participation isolée (absence de bande⁴⁴³) et non professionnelle d'un tiers. Utilisables à l'encontre du premier, les con-

437 SCHMID 299.

438 *Supra* n° 216–226.

439 Art. 175 LIFD; art. 56 al. 1 LHID.

440 Art. 23 al. 2 LSEE.

441 Art. 91 al. 1 LCR.

442 Art. 139 ch. 2 CP.

443 Aart. 139 ch. 3 al. 2 CP.

versations interceptées ne le sont pas à l'endroit du second dès lors qu'elles démontrent seulement la commission par le «nouveau venu» d'un vol simple⁴⁴⁴.

On verse enfin dans l'absurde lorsque la surveillance de l'auteur 230. présumé d'un abus de confiance, d'une escroquerie ou d'un blanchiment aggravé d'argent⁴⁴⁵ établit que les faits considérés sont en réalité constitutifs de gestion déloyale, de vol simple ou de blanchiment simple d'argent⁴⁴⁶, soit autant d'infractions qui n'apparaissent pas au catalogue de l'art. 3 al. 2–3 LSCPT et aux fins de la poursuite des- quelles les résultats de la mesure sont donc inexploitables⁴⁴⁷.

Ces aberrations ne découlent pas exclusivement des graves défauts 231. qui affectent le catalogue précité⁴⁴⁸. Elles trouvent concurremment leur origine dans le concept, vicié et vicieux, qui sous-tend l'ensem- ble de l'art. 9 LSCPT⁴⁴⁹. De l'ouverture de l'action publique au pro- noncé du dernier jugement au fond, l'objet d'une procédure pénale n'est pas de vérifier si un événement déterminé relève bien de la qualification juridique qui lui a été initialement donnée. Le procès pénal tend au contraire à établir la réalité de cet événement, consi- déré dans sa globalité, pour examiner ensuite s'il tombe *überhaupt* sous le coup de la loi pénale. Telle est l'origine du principe d'accusa- tion et de la maxime *Iura novit curia*, qui imposent au tribunal ap- pelé à juger un accusé de s'en tenir au complexe de faits reproché à ce dernier, mais de lui appliquer le droit d'office⁴⁵⁰. En opérant à l'art. 9 LSCPT avec la notion d'«acte punissable», le législateur fédé- ral greffe sans la moindre justification théorique ou pratique une composante juridique sur une base qui devait rester strictement fac- tuelle. Il colle arbitrairement l'étiquette de «découverte fortuite» à

⁴⁴⁴ Art. 139 ch. 1 CP; SCHMID 307.

⁴⁴⁵ Voir successivement les art. 138, 146 et 305^{bis} ch. 2 CP.

⁴⁴⁶ Voir successivement les art. 158, 139 ch. 1 et 305^{bis} ch. 1 CP.

⁴⁴⁷ HANSJAKOB, Art. 9 BÜPF n° 10; JEAN-RICHARD-DIT-BRESSEL 57; SCHMID 306–307.

⁴⁴⁸ *Supra* n° 84–86.

⁴⁴⁹ JEAN-RICHARD-DIT-BRESSEL 52–53 et 68–70; SCHMID 307 note 96.

⁴⁵⁰ Cf. art. 165–166 PPF (plus précis dans leur version allemande), 147–148 PPM, 283 CPP.

la mise en évidence d'éléments qui, loin d'entamer l'intégrité du complexe de faits à l'origine de la surveillance, commandent simplement d'en modifier la qualification juridique. La nécessité de pareilles corrections de tir n'est en rien le fruit du hasard; elle est inhérente à la nature même d'une procédure pénale orientée vers la recherche de la vérité matérielle.

232. A l'occasion des travaux d'élaboration d'un Code de procédure pénale suisse, toute la philosophie des découvertes fortuites devra impérativement être repensée. Un premier pas dans la bonne direction consistera à substituer au critère matériel d'«infraction» (*Strafstat*) le critère processuel du «complexe de faits» (*Tat*). Le second résidera dans la suppression de toute entrave à l'exploitation des éléments de preuve apportés par une mesure de contrainte dès lors qu'ils intéressent ledit complexe de faits.
233. L'obligation de détruire toute trace d'un *Zufallsfund* aussitôt que celui-ci s'avère inutilisable est également problématique dans la mesure où elle exclut tout retour en arrière. L'exemple suivant illustrera le propos⁴⁵¹. Une surveillance ordonnée sur la base de soupçons d'infraction à l'art. 322^{quater} CP ne fournit pas assez d'éléments à charge pour renvoyer de ce chef le fonctionnaire visé en jugement, mais révèle que l'intéressé enfreint de manière répétée l'art. 320 CP. L'élimination immédiate – ici lors du classement de la procédure – des preuves des violations du secret de fonction empêche *de facto* la répression de ces délits alors même que leur auteur, au gré de faits nouveaux motivant la reprise des poursuites, est finalement jugé pour corruption passive.
234. Les différentes propositions faites en doctrine⁴⁵² pour donner un sens raisonnable à l'art. 9 al. 3 phr. 2 LSCPT se heurtent très rapidement à la lettre de la loi. Une pesée des intérêts en présence devrait

⁴⁵¹ Pour d'autres illustrations des difficultés pratiques soulevées par l'art. 9 al. 3 phr. 2 LSCPT, voir HANSJAKOB, Art. 9 BÜPF n° 41; SCHMID 308–309.

⁴⁵² *Ibidem*.

conduire le législateur à privilégier celui de l'Etat (conservation des preuves susceptibles de retrouver leur fonction) sur celui du particulier incriminé (protection de sa sphère privée) et biffer une disposition qui constitue un corps étranger dans notre ordre juridique. Toutes choses égales d'ailleurs, nul ne soutient qu'un accusé acquitté aurait le droit d'obtenir la destruction de son dossier et des pièces à conviction qui l'accompagnent afin de se prémunir contre une demande en révision en sa défaveur.

VI Fin de la surveillance

A Levée de la surveillance

1 Cas

La surveillance de la correspondance par poste et télécommunication, accès à Internet compris, doit être levée lorsque

- aucune demande d'autorisation de la mesure n'a été déposée⁴⁵³;
- l'autorisation de la mesure a été refusée⁴⁵⁴;
- la mesure arrive à échéance sans que sa prolongation n'ait été demandée⁴⁵⁵;
- la prolongation de la mesure a été refusée⁴⁵⁶;
- la mesure n'est plus utile à l'enquête⁴⁵⁷.

La surveillance aura notamment perdu son utilité si l'adresse postale, le raccordement de télécommunication, le téléphone mobile ou la boîte aux lettres électronique surveillés ne sont plus utilisés ou si la mesure a livré tous les éléments de preuve (à charge comme à décharge) escomptés. En revanche, l'arrestation de l'auteur présumé

453 En l'absence de base légale expresse, on se référera ici à l'art. 7 al. 4 LSCPT (*supra* n° 146), qui prévoit en filigrane l'obligation de lever la surveillance.

454 Art. 10 al. 1 LSCPT; cf. *supra* n° 169.

455 Art. 11 al. 1 let. d, 13 al. 1 let. g LSCPT; cf. *supra* n° 174.

456 Art. 10 al. 1 LSCPT; cf. *supra* n° 176.

457 Art. 10 al. 1 LSCPT.

ne conduira pas nécessairement à mettre un terme à la surveillance⁴⁵⁸.

237. En bonne logique, la surveillance (en temps réel) doit également prendre fin dès l'instant où les conditions posées par la loi à sa mise en oeuvre ne sont plus remplies, par exemple s'il apparaît en cours de route que la prévention s'évanouit, qu'elle se déplace vers une infraction ne figurant pas au catalogue de l'art. 3 al. 2-3 LSCPT, que la gravité de l'acte a été initialement surestimée ou que d'autres mesures d'investigations sont désormais susceptibles de conduire à la manifestation de la vérité⁴⁵⁹.

2 *Compétence*

238. Dans les trois hypothèses visées par l'art. 10 al. 1 LSCPT, une décision formelle du magistrat qui avait ordonné la surveillance⁴⁶⁰ est nécessaire pour y mettre fin. Cette exigence s'impose naturellement lorsque la mesure doit cesser avant que n'arrive son échéance. Inversement, rien ne la justifie en cas de refus du juge des art. 179^{octies} al. 1 CP et 7 al. 1 LSCPT⁴⁶¹ d'autoriser ou de prolonger la surveillance dès lors que le procureur ou le juge d'instruction doivent immédiatement et inconditionnellement se plier à la volonté de leur autorité de tutelle; il aurait été à la fois suffisant et opportun de permettre ici au Service de surveillance, qui reçoit communication des refus précités⁴⁶², de lever la mesure de son propre chef⁴⁶³.

458 *Supra* n° 103 et les références citées. *Contra*: HANSJAKOB, Art. 10 BÜPF n° 5, qui semble confondre l'utilisation du raccordement du prévenu par un tiers et l'utilisation du raccordement d'un tiers par le prévenu.

459 Cf. *supra* n° 82, 89–92, 98–99.

460 *Supra* n° 126–128.

461 *Supra* n° 147.

462 *Supra* n° 167, 176.

463 HANSJAKOB, Art. 10 BÜPF n° 7, Art. 11 BÜPF n° 17.

De lege lata, une telle compétence n'est reconnue au Service de surveillance que dans l'hypothèse d'une mesure qui parvient à son terme sans avoir fait l'objet d'une demande tendant à la prolonger⁴⁶⁴. **239.**

En application analogique des art. 11 al. 1 let. d et 13 al. 1 let. g **240.** LSCPT, le Service de surveillance devrait également être investi du pouvoir de lever *motu proprio* une mesure qui n'a pas été soumise à l'approbation du juge compétent⁴⁶⁵, ce dont il se rendra compte à l'expiration des 5 jours prévus par l'art. 7 al. 3 phr. 2 LSCPT ou fort peu de temps après⁴⁶⁶.

La levée d'une mesure de surveillance qui ne satisfait plus aux conditions légales incombe logiquement au magistrat qui l'avait ordonnée⁴⁶⁷. **241.**

3 Destinataire de la décision

L'ordonnance par laquelle l'autorité en charge de l'enquête met un **242.** terme à la surveillance de la correspondance par poste et télécommunication, accès à Internet compris, doit être communiquée au Service de surveillance, qui répercuttera la décision auprès des différents fournisseurs de services concernés.

4 Formalités

En faisant obligation au Service de surveillance d'informer l'autorité **243.** compétente pour autoriser la mesure de la levée de cette dernière⁴⁶⁸, la loi poursuit deux objectifs: «d'une part pour confirmer à l'autorité que l'interruption a bien eu lieu, d'autre part pour mettre en éviden-

464 Art. 11 al. 1 let. d, 13 al. 1 let. g LSCPT.

465 *Contra*: HANSJAKOB, Art. 11 BÜPF n° 17.

466 *Supra* n° 153, 157.

467 Art. 10 al. 1 hypo. 1 LSCPT, appliqué par analogie.

468 Art. 11 al. 1 let. c, 13 al. 1 let. h LSCPT.

ce les éventuels ordres de surveillance n'ayant pas fait l'objet d'une demande d'autorisation»⁴⁶⁹.

- 244.** Le Service de surveillance conserve chaque ordre de surveillance pendant une année à compter de la levée de la mesure⁴⁷⁰.

B Information

1 *Obligation et moment*

- 245.** Généralement décidée et exécutée en secret⁴⁷¹, une mesure de surveillance sera normalement dévoilée au moment où le magistrat qui l'avait ordonnée versera les résultats de celle-ci au dossier et y confrontera l'auteur présumé. Pour garantir la transparence de principe qu'impose le droit constitutionnel et conventionnel⁴⁷², même (et surtout) lorsque l'opération n'a livré que des informations inutiles ou inexploitables⁴⁷³, la loi prescrit une communication «au plus tard lors de la clôture de la procédure pénale ou de la suspension de la procédure».
- 246.** Ainsi reproduit, l'art. 10 al. 2 LSCPT diverge grossièrement de sa version allemande, qui doit ici prévaloir⁴⁷⁴. On retiendra que l'information doit être donnée au plus tard avant (*vor*) la clôture de l'instruction préparatoire (*Abschluss der Strafuntersuchung*) ou le prononcé d'un classement, respectivement d'un non-lieu (*Einstellung des Verfahrens*).

⁴⁶⁹ CONSEIL FÉDÉRAL 3724.

⁴⁷⁰ Art. 11 al. 1 let. e, 13 al. 1 let. i LSCPT.

⁴⁷¹ Cf. *supra* n° 7, 134.

⁴⁷² Art. 17 par. 1 PIDCP, 8 par. 1 CEDH, 13 al. 1 *in fine* Cst.; cf. ATF 109 Ia 298–303 consid. 12, 123 IV 241 consid. 2b/cc et 244 consid. 3a; ZBl 86 (1985) 30–34 consid. 12.

⁴⁷³ *Supra* n° 206, 211–213, 227.

⁴⁷⁴ Cf. HANSJAKOB, Art. 10 BÜPF n° 15–17.

L'alternative «clôture de l'instruction préparatoire / classement ou **247.** non-lieu» s'avère absurde dans tous les systèmes qui – à l'instar des procédures pénales fédérale⁴⁷⁵, militaire⁴⁷⁶ et genevoise⁴⁷⁷ – connaissent l'institution du juge d'instruction et confient la décision d'abandonner les poursuites à une autorité différente, par exemple au Ministère public ou à une juridiction de renvoi. Si cette dernière porte la cause devant un tribunal, il incombe au juge d'instruction d'effectuer la communication avant de se dessaisir du dossier; à cet instant, ce magistrat ne peut cependant pas encore savoir ce que décideront le procureur ou une Chambre d'accusation.

L'obligation d'informer concerne indistinctement la surveillance en **248.** temps réel et la surveillance rétroactive⁴⁷⁸. Elle naît alors même que l'ordonnance de classement ou de non-lieu revêtirait un caractère provisoire, l'auteur de l'infraction étant inconnu, introuvable ou temporairement inapte à passer en jugement⁴⁷⁹; en effet, la possibilité de revenir sur une telle décision réside dans sa nature intrinsèque et les faits nouveaux, circonstances, preuves ou charges nouvelles⁴⁸⁰ susceptibles de motiver la reprise de l'action publique constituent de conditions (résolutoires) trop aléatoires pour perpétuer le secret sans l'approbation judiciaire prévue à l'art. 10 al. 3 LSCPT⁴⁸¹.

La «procédure» que vise l'art. 10 al. 2 LSCPT est celle dans le cadre **249.** de laquelle la surveillance avait été ordonnée⁴⁸². Afin de ne pas compromettre une enquête séparée portant sur un complexe de faits distinct et/ou dirigée contre un autre prévenu, ouverte notamment à la suite d'un *Zufallsfund*⁴⁸³, l'autorité compétente⁴⁸⁴ devra au besoin

⁴⁷⁵ Voir les art. 119 al. 3, 120 al. 1 et 131 al. 1 phr. 1 PPF.

⁴⁷⁶ Voir les art. 112 et 116 al. 1 PPM.

⁴⁷⁷ Voir les art. 185, 198 al. 1 et 204 al. 1 CPP.

⁴⁷⁸ HANSJAKOB, Art. 10 BÜPF n° 10.

⁴⁷⁹ *Contra*: HANSJAKOB, Art. 10 BÜPF n° 17.

⁴⁸⁰ Cf. art. 134 PPF; art. 116 al. 1 *in fine*, 198 al. 1 *in fine*, 206 al. 2 CPP.

⁴⁸¹ *Infra* n° 262.

⁴⁸² HANSJAKOB, Art. 10 BÜPF n° 14 et la référence citée.

⁴⁸³ *Supra* n° 215–226.

⁴⁸⁴ *Infra* n° n° 250–251.

solliciter et obtenir l'autorisation de différer ou de restreindre la communication, voire de s'y soustraire intégralement⁴⁸⁵.

2 *Compétence*

250. L'existence d'une mesure de surveillance sera en principe révélée par le magistrat qui l'avait ordonnée⁴⁸⁶.
251. Lorsque ce magistrat n'est plus saisi du dossier au moment où la communication doit être effectuée, cette dernière incombe à l'autorité qui se trouve alors en charge de la procédure⁴⁸⁷. En droit fédéral ordinaire comme à Genève, le juge d'instruction peut ainsi être amené à dévoiler une surveillance ordonnée par le procureur général durant l'enquête préliminaire de police judiciaire. En procédure pénale militaire et genevoise, le Ministère public prononçant un non-lieu ou un classement devra délivrer l'information si le juge d'instruction à l'origine de la mesure ne l'a pas fait.
252. L'art. 10 al. 4 LSCPT revêt une importance toute particulière dans le contexte de l'entraide internationale en matière pénale. Au dispositif de son ordonnance de clôture⁴⁸⁸, l'autorité helvétique d'exécution mentionnera l'obligation de l'Etat requérant d'informer les ayants droit de la surveillance opérée en Suisse⁴⁸⁹.

485 *Infra* n° 259–262; pour les détails, voir HANSJAKOB, Art. 10 BÜPF n° 14.

486 Art. 10 al. 2 LSCPT; voir *supra* n° 126–128.

487 Art. 10 al. 4 LSCPT; cf. *supra* n° 247.

488 Art. 80d EIMP.

489 Cf. HANSJAKOB, Art. 10 BÜPF n° 13 et 39.

L'opinion selon laquelle il incomberait à l'autorité helvétique requise d'informer les tiers se trouvant en Suisse me paraît contraire au texte clair de la loi.

3 Destinataires

Le recours à une mesure de surveillance sera tout d'abord signalé à 253. l'auteur présumé de l'infraction poursuivie⁴⁹⁰. Peu importe que l'adresse postale, le raccordement de télécommunication, le téléphone mobile ou la boîte aux lettres électronique visés étaient (aussi) les siens⁴⁹¹ ou ceux d'un tiers⁴⁹². L'individu qui vient à être suspecté au gré d'un *Zufallsfund*⁴⁹³ fait également partie des destinataires de l'information considérée.

En second lieu, l'existence de la mesure doit être dévoilée «aux personnes dont l'adresse postale ou le raccordement ont fait l'objet d'une surveillance»⁴⁹⁴. La loi appréhende ici non seulement les tiers susmentionnés, mais aussi les personnes qui partagent avec l'auteur présumé la titularité de l'objet surveillé⁴⁹⁵, boîte aux lettres électronique et téléphone portable compris⁴⁹⁶. Les exploitants de postes publics de télécommunication⁴⁹⁷, qui n'ignorent rien de la mesure puisqu'ils ont contribué à sa mise en oeuvre⁴⁹⁸, sont logiquement exclus⁴⁹⁹.

En définissant de la manière indiquée ci-dessus le cercle des destinataires de l'information, le législateur a rompu avec la jurisprudence fédérale rendue à l'enseigne de l'ancien art. 66^{quinquies} al. 1 PPF⁵⁰⁰, laquelle imposait aux autorités de poursuite et d'instruction pénale d'informer également les co-utilisateurs de fait d'un raccordement surveillé (*tatsächliche Mitbenützer eines überwachten Anchlusses*)⁵⁰¹,

490 Art. 10 al. 2 let. a LSCPT («aux suspects»).

491 *Supra* n° 75–104.

492 *Supra* n° 105–124.

493 *Supra* n° 215–226.

494 Art. 10 al. 2 let. b *in limine* LSCPT.

495 *Supra* n° 102.

496 *Supra* n° 25.

497 Sur la notion de postes publics de télécommunication, voir *supra* n° 114.

498 *Supra* n° 188–189.

499 Art. 10 al. 2 let. b *in fine* LSCPT.

500 RO 1992 p. 312.

501 ATF 123 IV 244 consid. 3a. Pour une pratique cantonale divergente, proche de la réglementation actuelle, voir RFJ 1995 n° 19 p. 91 consid. 5.

par exemple les familiers du prévenu ou les employés d'une personne morale. Si l'économie administrative découlant de la dispense d'identifier et de mettre au courant des personnes susceptibles de se compter par centaines est assurément appréciable, on éprouve néanmoins quelque peine à concilier le régime instauré avec le droit de recours expressément reconnu aux intéressés⁵⁰².

256. Le problème se pose en des termes similaires pour les correspondants des personnes surveillées⁵⁰³, lesquels ne bénéficient pas davantage d'une information⁵⁰⁴.

4 *Contenu et forme*

257. Selon l'art. 10 al. 2 *in fine* LSCPT, l'autorité compétente doit communiquer «les motifs, le mode et la durée de la surveillance». Concrètement, elle indiquera brièvement quel état de fait se trouvait à l'origine de la mesure, en quoi les conditions posées par la loi étaient remplies⁵⁰⁵, quels objets ont été surveillés⁵⁰⁶, quelles informations ont été sollicitées⁵⁰⁷, enfin quelle période a été couverte par la mesure.
258. Dès lors que la communication est appelée à faire partir un délai de recours⁵⁰⁸, les mentions qui précèdent seront formalisées dans une ordonnance, dûment notifiée à ses destinataires⁵⁰⁹.

502 *Infra* n° 269–270.

503 Voir *infra* n° 270–271.

504 Cf. HANSJAKOB, Art. 10 BÜPF n° 26 et les références citées.

505 *Supra* n° 75–124.

506 *Supra* n° 4, 25, 53.

507 *Supra* n° 6–13, 27–30, 54.

508 *Infra* n° 275.

509 P. 92 (2003) n° 119 consid. 2; BIEDERMANN 100; HANSJAKOB, Art. 10 BÜPF n° 22 et la référence citée.

5 *Exceptions*

En dérogation à l'obligation de principe d'informer⁵¹⁰, l'autorité **259.** compétente⁵¹¹ peut retarder sa communication ou même y renoncer complètement si, alternativement⁵¹²,

- des intérêts publics prépondérants, notamment en matière de sûreté intérieure ou extérieure ou de lutte contre le crime organisé, ne peuvent pas être protégés autrement;
- le dévoilement de la mesure de surveillance risque de mettre des tiers sérieusement en danger;
- le destinataire de l'information ne peut pas être atteint.

La nécessité de ne pas compromettre une enquête parallèle⁵¹³ ou la **260.** reprise ultérieure d'une action publique avortée en l'état relève classiquement d'un intérêt public digne de protection. Les circonstances du cas d'espèce et le respect du principe de la proportionnalité détermineront si un report de l'information suffit et quelle sera, le cas échéant, sa durée; la non-communication doit demeurer l'exception⁵¹⁴.

Nonobstant la réalisation de l'une ou l'autre des conditions pré- **261.** citées, toute occultation est exclue si les résultats de la surveillance doivent être utilisés comme moyens de preuve dans la procédure⁵¹⁵. Il en va du respect du droit des parties d'être entendues⁵¹⁶, notamment de consulter le dossier.

En la forme, l'autorité habilitée à autoriser la surveillance⁵¹⁷ doit ap- **262.** prouver la décision⁵¹⁸ de maintenir, provisoirement ou définitive-

510 *Supra* n° 245–249.

511 *Supra* n° 250–252.

512 Art. 10 al. 3 let. a–c LSCPT.

513 *Supra* n° 249.

514 HANSJAKOB, Art. 10 BÜPF n° 30 et la référence citée.

515 Art. 10 al. 3 *in fine* LSCPT.

516 Art. 29 al. 2 Cst.; art. 6 par. 1 phr. 1 et par. 3 let. b CEDH; art. 14 par. 1 phr. 2 et par. 3 let. b PIDCP.

517 *Supra* n° 147–150.

518 Cf. BIEDERMANN 100.

ment, le secret⁵¹⁹. Elle statuera à la requête du magistrat chargé de la communication, dans le cadre d'une ordonnance qui rejoindra le volet inaccessible du dossier si l'aval est donné.

VII Voies de droit

A Contre la mise sous surveillance

1 Autorité compétente

- 263. En procédure pénale fédérale, le recours contre la mise sous surveillance est examiné par la Chambre d'accusation du Tribunal fédéral⁵²⁰. Dès l'entrée en vigueur de la LTPF, cette tâche incombera sans doute à la Cour des plaintes du Tribunal pénal fédéral⁵²¹.
- 264. En procédure pénale militaire, le Tribunal militaire de cassation est compétent⁵²².
- 265. Quant au droit genevois, il désigne la Chambre d'accusation⁵²³.
- 266. S'ils avaient antérieurement approuvé ou prolongé la surveillance⁵²⁴, les présidents des trois juridictions précitées doivent se récuser⁵²⁵.

519 Art. 10 al. 3 *in limine* LSCPT.

520 Art. 10 al. 5 let. a LSCPT.

521 En arrêtant la LTPF, le législateur fédéral a manifestement omis d'adapter l'art. 10 al. 5 let. a LSCPT au nouveau droit (cf. FF 2002 p. 6058).

522 Art. 10 al. 5 let. b LSCPT.

523 Art. 48A al. 3 LACP et 190C al. 1 CPP *cum* art. 10 al. 5 let. c LSCPT, dans leur teneur selon la loi n° 8732 du 16 mai 2003 (FAO 57/23.5.2003 p. 23–24).

524 *Supra* n° 148–150, 176.

525 Cf. ATF 123 IV 240 consid. 1.

2 Décisions susceptibles de recours

La loi ne dit pas si le recours doit être dirigé contre l'ordre de surveillance⁵²⁶ ou contre la décision d'approbation de la mesure⁵²⁷. Considérant que la procédure d'autorisation de la surveillance présente les caractéristiques d'un appel (effet dévolutif complet, pouvoir de réformation du *iudex ad quem*)⁵²⁸, la seconde solution s'impose naturellement⁵²⁹.

Parce qu'une surveillance (en temps réel) initialement conforme à la loi peut perdre cette qualité au cours de son existence⁵³⁰, le plaideur avisé prendra le soin d'attaquer en outre les éventuelles ordonnances de prolongation de la mesure⁵³¹.

3 Qualité pour recourir

De lege lata, la qualité pour recourir est reconnue aux personnes qui ont fait l'objet de la surveillance et à celles qui ont utilisé le même raccordement ou la même adresse⁵³².

S'il ne fait pas de doute que cette description permet d'appréhender l'auteur présumé et le tiers dont l'adresse postale, le raccordement de télécommunication, le téléphone mobile ou la boîte aux lettres électronique ont été surveillés, ainsi que les personnes qui partagent avec l'auteur présumé la titularité des objets précités⁵³³ et les co-uti-

526 *Supra* n° 129.

527 *Supra* n° 158.

528 *Supra* n° 151–152, 161–162.

529 BIEDERMANN 101–102; cf. aussi OBERHOLZER 10. *Contra* (apparemment): HANSJAKOB, Art. 10 BÜPF n° 41.

530 Cf. *supra* n° 237.

531 *Supra* n° 176–177.

532 Art. 10 al. 5 et al. 6 phr. 1 LSCPT.

Ces dispositions paraissent plus explicites dans leur version allemande, qui vise les personnes contre lesquelles la surveillance était dirigée et celles qui ont co-utilisé l'adresse ou le raccordement surveillés.

533 *Supra* n° 254; HANSJAKOB, Art. 10 BÜPF n° 42.

lisateurs de fait du raccordement surveillé⁵³⁴, on peut lire en doctrine que le prévenu (suspect) ne serait pas recevable à agir lorsque la mesure vise un tiers⁵³⁵, pas davantage que les co-utilisateurs seulement occasionnels du raccordement considéré⁵³⁶ ou les simples correspondants des personnes surveillées⁵³⁷.

271. De telles restrictions me paraissent incompatibles avec les art. 13 al. 1 Cst., 8 par. 1 CEDH et 17 par. 1 PIDCP. Selon la jurisprudence fédérale relative à ces dispositions, toute personne ayant connu l'interception d'une communication à laquelle elle a pris part bénéficie d'une protection constitutionnelle et conventionnelle propre; elle peut exiger que la légalité de la surveillance soit contrôlée a posteriori, cas échéant au stade de l'instruction préparatoire déjà, en interjetant un recours contre la mesure⁵³⁸. Du moment que la sphère privée ici en cause constitue un droit de caractère civil⁵³⁹, la qualité pour recourir de l'intéressée découle en outre directement des art. 6 par. 1 phr. 1 CEDH et 14 par. 1 phr. 2 PIDCP, qui incorporent le droit d'accéder à un tribunal pour faire trancher la contestation soulevée⁵⁴⁰.

534 *Supra* n° 255.

La co-utilisation d'une adresse postale n'est guère concevable en pratique (HANSJAKOB, Art. 10 BÜPF n° 51).

535 BIEDERMANN 102–103; OBERHOLZER 10.

Cette opinion est insoutenable au regard du statut du prévenu dans la procédure pénale et de son intérêt évident à contester une mesure de contrainte entachée d'irrégularités. Elle priverait ensuite l'art. 10 al. 2 let. a LSCPT de sa raison d'être (*supra* n° 253), qui est de mettre l'auteur présumé en état de recourir contre la surveillance (ATF 123 IV 244 consid. 3a; cf. aussi HANSJAKOB, Art. 10 BÜPF n° 42).

536 OBERHOLZER 10 («nur der regelmässige Mitbenutzer»).

537 BIEDERMANN 102; HANSJAKOB, Art. 10 BÜPF n° 42 et 51, qui se réfère en note 498 aux travaux préparatoires; OBERHOLZER 10.

538 ATF 120 Ia 317–318 consid. 2c, 122 I 189 consid. 3b et 190–193 consid. 4b–c, 123 IV 244 consid. 3a, 125 I 49 consid. 5, 125 I 101–103 consid. 3c–e.

539 Cf. ATF 127 I 122–124 consid. 6.

540 ATF 127 I 120 consid. 5 et 124–127 consid. 7–9, avec de nombreuses références à la jurisprudence européenne.

4 Moyens

Aux termes de l'art. 10 al. 5 LSCPT, le recourant peut invoquer le caractère illicite et l'absence de proportionnalité de la surveillance. La formule est doublement trompeuse. D'une part, elle semble ériger la disproportion en moyen autonome, alors qu'un tel défaut rend nécessairement la mesure illicite⁵⁴¹. D'autre part, elle donne à penser que le contrôle est limité à la violation du droit (*revisio in iure*); la garantie de l'accès à un tribunal selon les art. 6 par. 1 phr. 1 CEDH et 14 par. 1 phr. 2 PIDCP précités⁵⁴² emporte toutefois que le contrôle judiciaire s'étende également aux questions de fait (*revisio in facto*)⁵⁴³.

Ces dernières considérations s'opposent aussi à ce que l'on déduise de l'art. 10 al. 6 phr. 2 *in fine* LSCPT⁵⁴⁴ une quelconque limitation des moyens susceptibles d'être invoqués par les personnes ayant utilisé les raccordements surveillés.

Le bien-fondé des moyens soulevés s'examinera *ex ante*, les juges devant déterminer si la mesure de surveillance était conforme à la loi au moment où celle-ci avait été approuvée ou prolongée⁵⁴⁵.

5 Délai

Le délai de recours est de 30 jours à compter de la communication de la surveillance⁵⁴⁶.

541 HANSJAKOB, Art. 10 BÜPF n° 45.

542 *Supra* n° 271.

543 ATF 126 I 152 consid. 3c et les références citées; voir aussi ATF 129 I 109.

544 Cf. OBERHOLZER 10.

545 Cf. BIEDERMANN 103.

546 Art. 10 al. 5 *in limine* LSCPT; Pr. 92 (2003) n° 119 consid. 2; cf. *supra* n° 245–258.

276. En l'absence d'une telle communication⁵⁴⁷, le délai court à partir de la prise de connaissance effective des motifs, du mode et de la durée de la mesure, au sens de l'art. 10 al. 2 *in fine* LSCPT⁵⁴⁸.

6 *Procédure*

277. La procédure de recours est celle que prévoient les codes fédéraux et cantonaux applicables⁵⁴⁹.
278. En complément sinon en dérogation aux règles précitées, l'art. 10 al. 6 phr. 2 LSCPT confère aux co-utilisateurs des raccordements surveillés⁵⁵⁰ le droit de consulter les informations qui concernent leur personne et qui ont été exploitées dans la procédure pénale, puis de solliciter l'élimination de celles qui ne s'avèrent pas nécessaires. Il est patent qu'un si maigre «accès au dossier» ne permettra pas aux intéressés de valablement faire valoir leurs droits⁵⁵¹.

7 *Décision sur recours*

279. Si l'autorité de recours parvient à la conclusion que la mesure de surveillance avait été ordonnée ou prolongée à tort, sa décision emportera les effets prévus à l'art. 7 al. 4 LSCPT, applicable par analogie⁵⁵².

547 Cf. *supra* n° 255–256.

548 *Supra* n° 257; cf. HANSJAKOB, Art. 10 BÜPF n° 43.

549 Voir *infra* n° 281–283.

550 *Supra* n° 269–270.

551 Cf. HANSJAKOB, Art. 10 BÜPF n° 54 *cum* 21 et les références citées.

552 *Supra* n° 170–172; OBERHOLZER 10.

B Contre les autres décisions de l'autorité ayant ordonné la surveillance

Les décisions du juge d'instruction ou du procureur autres que la mise sous surveillance, par exemple celles qui concernent le tri des informations recueillies et leur versement au dossier, sont soumises aux voies de recours ordinairement prévues par les codes fédéraux et cantonaux de procédure. 280.

En procédure pénale fédérale, la plainte devant la Chambre d'accusation du Tribunal fédéral est recevable⁵⁵³. Avec l'entrée en vigueur de la LTPF, la Cour des plaintes du Tribunal pénal fédéral sera compétente⁵⁵⁴. 281.

En procédure pénale militaire, les décisions, opérations et omissions du juge d'instruction peuvent faire l'objet d'une plainte auprès de l'Auditeur en chef⁵⁵⁵. 282.

A Genève, enfin, le recours devant la Chambre d'accusation sera envisagé⁵⁵⁶. 283.

C Contre les décisions du Service de surveillance

Pour les fournisseurs de services postaux et de télécommunication, les décisions du Service de surveillance sont susceptibles d'un recours administratif⁵⁵⁷ auprès de la Commission de recours du DETEC⁵⁵⁸. 284.

⁵⁵³ Art. 105^{bis} al. 2, 214–219 PPF.

⁵⁵⁴ Art. 28 al. 1 let. g LTPF; voir FF 2002 p. 6040, 6047, 6052–6053.

⁵⁵⁵ Art. 166–171 PPM.

⁵⁵⁶ Art. 190–196 CPP.

⁵⁵⁷ Art. 44–64, 71a–71d PA.

⁵⁵⁸ Art. 32 OSCPT; HANSJAKOB, Art. 10 BÜPF n° 58, Art. 32 VÜPF n° 1–3.

285. Intéressant l'entraide nationale, les contestations entre les autorités judiciaires fédérales ou cantonales et le Service de surveillance sont tranchées par la Chambre d'accusation du Tribunal fédéral⁵⁵⁹. Dès l'entrée en vigueur de la LTPF, la compétence passera à la Cour des plaintes du Tribunal pénal fédéral⁵⁶⁰.

Bibliographie choisie

- FELIX BÄNZIGER, *Telefonüberwachung in der Schweiz*, Krim 2002 p. 551–553.
- AUGUST BIEDERMANN, *Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000*, RPS 120 (2002) 77–106.
- CONSEIL FÉDÉRAL, *Message concernant les lois fédérales sur la surveillance de la correspondance postale et des télécommunications et sur l'investigation secrète*, FF 1998 p. 3689–3771.
- THOMAS HANSJAKOB, *BÜPF / VÜPF, Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*, St. Gallen 2002.
- THOMAS HANSJAKOB, *Die ersten Erfahrungen mit dem Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)*, RPS 120 (2002) 265–283.
- THOMAS HANSJAKOB, *Telefonüberwachung aus anwaltlicher Sicht*, RAV 2003 p. 43–46.
- ROBERT HAUSER / ERHARD SCHWERI, *Schweizerisches Strafprozessrecht*, 5. Auflage, Basel / Genf / München 2002, § 71 n° 1–33.
- MARC JEAN-RICHARD-DIT-BRESSEL, *Ist ein Milionendiebstahl ein Bagatelldelikt? – Fragen zum Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000*, RPS 119 (2001) 40–70.
- URS MAURER / SERGIO GANSSEN, Umfassende Überwachung leicht gemacht, *Plädoyer* 3/2002 p. 24–26.

559 Art. 357 CP; *supra* n° 66.

560 Art. 28 al. 1 let. g LTPF; voir FF 2002 p. 6040, 6047.

JUDITH NATTERER, *Die Verwertbarkeit von Zufallsfunden aus der Telefonüberwachung im Strafverfahren*, Bern 2001.

NIKLAUS OBERHOLZER, *Das neue Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)*, ZGRG 2002 p. 3–15.

GÉRARD PIQUEREZ, *Manuel de procédure pénale suisse*, Zurich 2001, n° 1693–1734.

NIKLAUS SCHMID, *Verwertung von Zufallsfunden sowie Verwertungsverbote nach dem neuen Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)*, RPS 120 (2002) 284–320.

OLIVER SIDLER, *Staatliche Internet-Überwachung*, ML 2002 p. 115–116.

MARKUS WEBER, *Vollzugsdefizite im UVEK*, RPS 120 (2002) 357–368.

Abréviations juridiques

ATF	Arrêts du Tribunal fédéral suisse, Recueil officiel
CC	Code civil suisse, du 10 décembre 1907 (RS 210)
CEDH	Convention de sauvegarde des droits de l'homme et des libertés fondamentales, du 4 novembre 1950 (RS 0.101)
CP	Code pénal suisse, du 21 décembre 1937 (RS 311.0)
CPM	Code pénal militaire, du 13 juin 1927 (RS 321.0)
CPP	Code genevois de procédure pénale, du 29 septembre 1977 (RSG E 4 20)
Cst.	Constitution fédérale de la Confédération suisse, du 18 avril 1999 (RS 101)
DPA	Loi fédérale sur le droit pénal administratif, du 22 mars 1974 (RS 313.0)
FAO	Feuille d'avis officielle de la République et canton de Genève
FF	Feuille fédérale
Krim	Kriminalistik
LA	Loi fédérale sur l'aviation, du 21 décembre 1948 (RS 748.0)
LACP	Loi genevoise d'application du code pénal et d'autres lois fédérales en matière pénale, du 14 mars 1975 (RSG E 4 10)

LAVI	Loi fédérale sur l'aide aux victimes d'infractions, du 4 octobre 1991 (RS 312.5)
LCR	Loi fédérale sur la circulation routière, du 19 décembre 1958 (RS 741.01)
LEA	Loi fédérale sur l'utilisation pacifique de l'énergie atomique, du 23 décembre 1959 (RS 732.0)
LFMG	Loi fédérale sur le matériel de guerre, du 13 décembre 1996 (RS 514.51)
LHID	Loi fédérale sur l'harmonisation des impôts directs des cantons et des communes, du 14 décembre 1990 (RS 642.14)
LIFD	Loi fédérale sur l'impôt fédéral direct, du 14 décembre 1990 (RS 642.11)
LSEE	Loi fédérale sur le séjour et l'établissement des étrangers, du 26 mars 1931 (RS 142.20)
LPO	Loi fédérale sur la poste, du 30 avril 1997 (RS 783.0)
LPol	Loi genevoise sur la police, du 26 octobre 1957 (RSG F 1 05)
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication, du 6 octobre 2000 (RS 780.1)
LStup	Loi fédérale sur les stupéfiants, du 3 octobre 1951 (RS 812.121)
LTC	Loi fédérale sur les télécommunications, du 30 avril 1997 (RS 784.10)
LTPF	Loi fédérale sur le Tribunal pénal fédéral, du 4 octobre 2002 (FF 2002 p. 6034-6059; non encore en vigueur)
ML	Medialex, Revue de droit de la communication
OCA	Ordonnance de la Chambre d'accusation du canton de Genève
OEIS	Ordonnance sur les émoluments et les indemnités en matière de surveillance de la correspondance postale et des télécommunications, du 21 juin 2000 (RS 780.115.1)
OJ	Loi fédérale d'organisation judiciaire, du 16 décembre 1943 (RS 173.110)
OJPM	Ordonnance fédérale concernant la justice pénale militaire, du 24 octobre 1979 (RS 322.2)

OPO	Ordonnance fédérale sur la poste, du 29 octobre 1997 (RS 783.01)
OSCPT	Ordonnance fédérale sur la surveillance de la correspondance par poste et télécommunication, du 31 octobre 2001 (RS 780.11)
OST	Ordonnance fédérale sur les services de télécommunication, du 31 octobre 2001 (RS 784.101.1)
PA	Loi fédérale sur la procédure administrative, du 20 décembre 1968 (RS 172.021)
PIDCP	Pacte international relatif aux droits civils et politiques, du 16 décembre 1966 (RS 0.103.2)
Pläd	Plädoyer, Das Magazin für Recht und Politik
PPF	Loi fédérale sur la procédure pénale, du 15 juin 1934 (RS 312.0)
PPM	Procédure pénale militaire, du 23 mars 1979 (RS 322.1)
Pr	Die Praxis (jusqu'en 1990, Die Praxis des Bundesgerichts)
RAD	Cour européenne des droits de l'homme, Recueil des arrêts et décisions (jusqu'en 1995, Série A)
RAG	Recueil authentique des lois et actes du gouvernement de la République et canton de Genève
RAv	Revue de l'avocat
RFJ	Revue fribourgeoise de jurisprudence
RJB	Revue de la société des juristes bernois
RO	Recueil officiel des lois fédérales
RPS	Revue pénale suisse
RS	Recueil systématique du droit fédéral
RSJ	Revue suisse de jurisprudence
RSG	Recueil systématique de la législation genevoise
Série A	Publications de la Cour européenne des droits de l'homme, Série A, Arrêts et décisions (dès 1996, RAD)
SJ	La Semaine Judiciaire
ZGRG	Zeitschrift für Gesetzgebung und Rechtsprechung in Graubünden
ZR	Blätter für zürcherische Rechtsprechung

ZBl Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht (jusqu'en 1988, Schweizerisches Zentralblatt für Staats- und Gemeindeverwaltung)

Abréviations techniques

ADSL	Asymetric Digital Subscriber Line
E-MAIL	Electronic Mail
GSM	Global System for Mobile Communication
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet(working) Protocol
ISDN	Integrated Services Digital Network
MMS	Multimedia Messaging Service
MSISDN	Mobile Station ISDN Number
PIN	Personal Identification Number
PUK	Personal Unblocking Key
SIM	Subscriber Identity Module
SMS	Short Message Switching
SMTP	Simple Mail Transfert Protocol
UMTS	Universal Mobile Telecommunication System
URL	Uniform Resource Locator
WAP	Wireless Application Protocol
WWW	World Wide Web