Philippe BONVIN

Les mesures de surveillance secrètes (art. 269 et ss CPP)

Lausanne, le 5 mai 2024

Table des matières

Table des abréviations

al.	alinéa
art.	article(s)
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
CCC	Convention du 23 novembre 2001 sur la cybercriminalité (RS 0.311.43)
CEDH	Convention du 4 novembre 1950 de sauvegarde des droits de l'homme et des libertés fondamentales (RS 0.101)
CourEDH	Cour européenne des droits de l'homme
CJUE	Cour de justice de l'Union européenne
consid.	considérant
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS 101)
CP	Code pénal suisse du 21 décembre 1937 (RS 311.0)
CPP	Code de procédure pénale suisse du 5 octobre 2007 (RS 312.0)
éd.	édition
EIMP	LF du 20 mars 1981 sur l'entraide internationale en matière pénale (RS 351.1)
édit.	éditeur(s)
etc.	et cætera
LF	Loi fédérale
LRens	LF du 25 septembre 2015 sur le renseignement (RS 121)
LTF	Loi du 17 juin 2005 sur le Tribunal fédéral (RS 173.110)
LPD	LF du 25 septembre 2020 sur la protection des données (RS 235.1)
LSCPT	LF du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (RS 780.1)
n°(s)	numéro(s)
OSCPT	Ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (RS 780.11)
p.	page(s)
pp.	pages
rés.	résumé

RS	Recueil systématique du droit fédéral
ss	suivant(e)s
TF	Tribunal fédéral suisse
Tmc	Tribunal des mesures de contrainte
trad.	traduction

Bibliographie

Doctrine

BULAK UYGUN Begüm, *La protection des données personnelles et la coopération policière en Europe*, thèse, Zürich 2018.

CAPUS Nadja / BALLY Elodie, *Intercepter avec des interprètes*, RPS 138/2020 p. 345 ss.

DELLAGANA-SABRY Yasmine, *Perquisitions en procédure pénale*, Zürich 2021.

GAUDERON Ryan, *L'investigation secrète : mesure de contrainte licite ou moyen d'instruction déloyal ?*, PJA 2020 p. 1430 ss.

JACOT-GUILLARMOD Emilie, *L'enregistrement systématique des données secondaires de communication*, in : LawInside (www.lawinside.ch), 2018, p. « www.lawinside.ch/600/ » (28 avril 2024).

Jeanneret, Yvan / Kuhn, André / Perrier Depeursinge, Camille (édit.), *Commentaire romand, Code de procédure pénale suisse*, 2e éd. Bâle 2019.

JEANNERET Yvan / KUHN André, *Précis de procédure pénale*, 2e éd. Berne 2018.

JOSITSCH, Daniel / SCHMID, Niklaus, *Schweizerische Strafprozessordnung Praxiskommentar*, 4e éd. Zurich/Saint-Gall 2023.

LEGLER Ariane, *La prolongation d'une mesure de surveillance secrète*, in : LawInside (www.lawinside.ch), 2023, p. « www.lawinside.ch/1279/ » (25 avril 2024).

PERRIER DEPEURSINGE Camille, *CPP annoté PPMin - LTF - LAVI - DPA - LOAP - CEDH*, 2e éd., Bâle 2020.

MÉTILLE Sylvain, art. 269-279 CPP, in : Jeanneret, Yvan / Kuhn, André / Perrier Depeursinge, Camille (édit.), *Commentaire romand, Code de procédure pénale suisse*, 2e éd., Bâle 2019.

TEICHMANN Fabian / GERBER Léonard, *Les cyberattaques par spyware – Poursuite et qualification en droit pénal suisse*, Sécurité & Droit 3/2021 p. 118 ss.

ZIMMERMANN Robert, *La coopération judiciaire internationale en matière pénale*, 5ème éd., Berne 2019.

Documents officiels

Message du Conseil fédéral du 21 décembre 2005 relatif à l'unification du droit de la procédure pénale, FF 2005 p. 1230 ss (cité : Message CPP).

Message du Conseil fédéral du 27 février 2013 concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), FF 2012 p. 2379 ss (cité : Message LSCPT).

Rapport rendant compte des résultats de la consultation, Révisions partielles de quatre ordonnances d'exécution de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) in : Département fédéral de justice et police (www.ejpd.admin.ch), Berne 2023,
p. « https://www.newsd.admin.ch/newsd/message/attachments/84133.pdf » (25 avril 2024) (cité : Rapport de consultation LSCPT).

Rapport annuel 2023 Service SCPT in : Service Surveillance de la correspondance par poste et télécommunication (www.li.admin.ch), Berne 2023,
p. « https://www.li.admin.ch/sites/default/files/2024-04/jahresbericht2023_fr.pdf » (20 avril 2024) (cité : Rapport annuel S-SCPT).

Introduction

Le CPP prévoit, au chapitre 8 du titre 5 (art. 269 et ss), des mesures de surveillance secrètes afin de récolter des preuves lors de procédures pénales. La surveillance de la correspondance par poste et télécommunication est l'un de ces moyens mis à disposition du ministère public. La LSCPT détaille notamment l'exécution de ces mesures de surveillance. Dans le cas où il y aurait une ou plusieurs parties étrangères, la CCC s'applique et la LRens permet la surveillance des télécommunications traversant la frontière suisse (art. 39 et ss LRens).

Le présent travail étudie les modalités d'application des mesures de surveillance secrète ainsi que les restrictions y relatives (*infra* I), étudie l'utilisation des moyens de preuve récoltés par cette surveillance (*infra* II) et finalement présente les voies de droit des parties (*infra* III).

I. Mise en œuvre des mesures de surveillance

A. Notions

La surveillance des télécommunications et de la correspondance est une infraction pénalement punissable (art. 179 et 179ter CP). L'art. 179^{octies} CP la rend licite pour les mesures valablement ordonnées[1].

La possibilité d'exécuter une mesure de surveillance est limitée par l'art. 269 CPP. Celui-ci exige notamment à ce qu'il y ait eu des mesures alternatives considérées avant la mise en place de la surveillance (art. 269 al. 1 let. c CPP).

Ces mesures sont soumises à l'autorisation du Tmc (art. 272 al. 1 CPP). Les fournisseurs de services de télécommunication ont l'obligation de collaborer (art. 2 LSCPT) et doivent aider à l'interception (art. 26 al. 1-3 LSCPT).

La surveillance se distingue en deux types. Les données sont qualifiées de primaires lorsque le contenu même des télécommunications est intercepté, tandis que les

[1] JEANNERET / KUHN, n° 14089.

données secondaires fournissent des informations sur les caractéristiques techniques de la télécommunication[2], par exemple l'indication de la localisation, la temporalité, la durée, les destinataires de l'échange, etc. (art. 60 OSCPT).

Les données secondaires sont enregistrées par les fournisseurs de services de télécommunication et conservées pendant six mois (art. 26 al. 5 LSCPT). Si le fournisseur a conservé spontanément des données utiles remontant plus loin, il doit les mettre à disposition[3].

Cet enregistrement est une atteinte au droit à la vie privée, au regard des art. 8 CEDH, 13 Cst. et 6 LPD. Le TF s'est déterminé à ce propos[4] : la conservation est requise pour une durée de six mois seulement; les conditions d'accès à ces données sont strictes; la demande est évaluée par un tribunal indépendant et la pesée des intérêts prépondérants pour la sécurité publique et la protection des droits d'autrui font que le principe de proportionnalité est respecté[5].

Ces mesures permettent de poursuivre un prévenu pour des infractions envisagées, qui se commettent en série ou dans la durée[6].

Cette surveillance est particulièrement invasive car elle est secrète : les personnes visées n'en sont informées qu'a posteriori[7]. L'atteinte à la vie privée est considérée moindre dans le cas d'une surveillance se basant sur des données secondaires uniquement[8].

Les mesures sont appliquées en temps réel (art. 269 CPP) ou rétroactivement (art. 273 CPP). Il ne faut pas les confondre avec une perquisition (art. 241 et ss CPP) ou une mise sous séquestre (art. 263 CPP et ss) : la surveillance est uniquement possible durant le transport de télécommunications. Lorsque les informations visées sont

---

[2] JEANNERET / KUHN, n° 14095 ; PERRIER DEPEURSINGE, p. 448.
[3] PERRIER DEPEURSINGE, p. 449.
[4] ATF 144 I 126, consid. 8.4, JdT 2018 I 191 (trad.).
[5] JACOT-GUILLARMOD.
[6] DELLAGANA-SABRY, p. 12.
[7] *Idem*, p. 13.
[8] PERRIER DEPEURSINGE, p. 442.

conservées dans le lieu d'origine ou de destination, dans la sphère de possession de son destinataire[9], il faut appliquer la perquisition[10] soumise au mandat (art. 241 al. 1. CPP).

Enfin, l'interception ne peut se faire qu'envers des individus clairement identifiés (art. 270 CPP) mais possiblement pas encore connus[11]. La surveillance préventive[12] tout comme la recherche exploratoire sont interdites.

B. Conditions

Les conditions cumulatives suivantes doivent être remplies pour ordonner la surveillance : la commission ou l'existence de forts soupçons, sans faire la pesée complète des éléments[13], de commission d'un acte grave faisant partie des cas définis à l'art. 269 al. 2 CPP; les tentatives de récolte de preuve par d'autres moyens n'ont pas été couronnées de succès[14] ou il n'existe pas d'autre moyen raisonnable pour les collecter[15].

Le TF a déterminé que des soupçons sont suffisants pour ordonner la surveillance, même lorsque la suspicion de délit provient d'une source anonyme[16]. Toutefois, la seule allégation d'une partie ou des suppositions générales ne sont pas suffisantes[17].

Il se peut que la personne prévenue utilise un moyen de télécommunication d'un tiers, de bonne foi ou non[18]. Il est donc possible de demander la surveillance de ce moyen à deux conditions : s'il est avéré que le prévenu utilise effectivement ce moyen de télécommunication ou que le tiers transmet ou reçoit pour le compte du prévenu des télécommunications[19] (art. 270 let. b CPP). Les moyens de communication publics ou

---

[9] JEANNERET / KUHN n° 14090.
[10] DELLAGANA-SABRY, p. 14.
[11] PERRIER DEPEURSINGE, p. 448.
[12] JEANNERET / KUHN, n° 14094.
[13] PERRIER DEPEURSINGE, p. 443.
[14] ZIMMERMANN, p. 481.
[15] JEANNERET / KUHN, n° 14094.
[16] LEGLER, p. 2.
[17] PERRIER DEPEURSINGE, p. 451.
[18] JEANNERET / KUHN, n° 14093.
[19] BULAK UYGUN, p. 141.

partagés sont assimilés à un moyen appartenant à un tiers[20]. La partie plaignante peut également être surveillée lorsqu'il y a un intérêt à intercepter les communications entre celle-ci et le prévenu[21].

Dans le cas où le prévenu se situe sur le territoire suisse mais utilise un service de télécommunication basé à l'étranger, il peut être difficile pour les autorités d'appliquer une surveillance[22].

La recherche par champ d'antenne (géolocalisation) d'auteurs inconnus est possible pour obtenir des données secondaires; mais, sans identification des personnes, l'interception des données primaires n'est pas autorisée[23].

C. Procédure

La demande d'interception est soumise au Tmc dans les 24 heures à partir du moment où la surveillance a été ordonnée (art. 274 al. 1 CPP). Elle est motivée à l'aide des éléments de preuve versés à la procédure et peut même contenir des éléments collectés durant les premières heures de la surveillance[24]. La forme peut être orale en cas d'urgence[25]. Le Tmc statue dans les cinq jours en motivant sa décision. Ce délai est une prescription d'ordre[26], un dépassement n'entraînerait en principe pas l'irrecevabilité des preuves[27]. Le Tmc peut autoriser la surveillance en l'assortissant de conditions ou à titre provisoire (art. 274 al. 2 CPP) ou encore préciser s'il est permis de pénétrer dans des locaux non publics pour réaliser l'interception[28].

L'utilisation de programmes informatiques spéciaux pour exécuter la surveillance n'est autorisée qu'à titre subsidiaire de l'interception[29] (art. 269 CPP).

---

[20] Message CPP, p. 1231.
[21] PERRIER DEPEURSINGE, p. 445.
[22] Message LSCPT p. 2404 ; ATF 143 IV 21, JdT 2018 IV 384 consid. 3.2 (rés.) ; arrêt 1B_142/2016 du 16 novembre 2016 consid. 3.2.
[23] PERRIER DEPEURSINGE, p. 448.
[24] JEANNERET / KUHN, n° 14097.
[25] JOSITSCH / SCHMID, art. 269 CPP n° 2.
[26] JEANNERET / KUHN, n° 14097.
[27] PERRIER DEPEURSINGE, p. 455.
[28] JEANNERET / KUHN, n° 14098.
[29] ZIMMERMANN, p. 481.

S'il est établi que plusieurs demandes de surveillance devront être soumises de manière rapprochée pour la même personne car celle-ci change régulièrement de fournisseur de télécommunications, il est possible de délivrer une autorisation-cadre (art. 272 al. 2. CPP). Les critères sont généralement l'utilisation de plus de trois raccordements et la volonté manifeste de la personne de ne pas être identifiée[30]. Dans ce cas, un rapport mensuel doit être établi et soumis au Tmc (art. 272 al 2 CPP).

Durant la surveillance, il se peut que des informations n'ayant pas de rapport avec la procédure soient collectées. Ces éléments sont conservés séparément et détruits après la fin de la procédure[31] (art. 276 CPP).

Si des données ont été obtenues en violation de la loi, celles-ci sont inexploitables et doivent être immédiatement détruites[32] (art. 277 CPP).

Une entité étrangère peut présenter une demande de surveillance (art. 18*a* et 18*b* EIMP) si elle respecte les conditions des art. 269 et ss CPP. Une telle surveillance assujettie à certaines conditions contraignantes pour l'entité étrangère a déjà été accordée par le passé[33].

La durée maximale de l'autorisation est de trois mois, pouvant être renouvelée pour une durée de trois mois au plus (art. 274 al. 5 CPP).

La prolongation d'une mesure de surveillance doit être demandée avant l'expiration de la durée autorisée (art. 274. al. 5 CPP). Lors du dépôt tardif d'une demande de prolongation, les données récoltées entre la fin de la première autorisation et le début de la seconde sont inexploitables et doivent être détruites[34].
Une demande tardive ne devrait pas rendre illicite l'entier de la mesure de surveillance autorisée[35].

---

[30] JOSITSCH / SCHMID, art. 272 CPP n° 4.
[31] ZIMMERMANN, p. 482.
[32] DELLAGANA-SABRY, p. 14.
[33] ZIMMERMANN, p. 285.
[34] ATF 149 IV 35, consid. 5 (non publié au JdT).
[35] LEGLER, p. 1.

Même si le propriétaire de la ligne a donné son consentement à la surveillance, le Tmc doit quand même donner son aval[36].

D. Fin des mesures

La surveillance est levée immédiatement lorsque les conditions requises ne sont plus remplies ou que l'autorisation ou sa prolongation a été refusée (art. 275 CPP).

Cependant, il n'est pas imposé de lever dès que possible la surveillance, tant que les conditions d'octroi de la mesure sont toujours remplies[37]. Lorsque les soupçons ont été confirmés ou infirmés ou que l'infraction ne figure pas dans les conditions permettant la surveillance, celle-ci doit être levée, même avant l'échéance de l'autorisation[38].

II. Utilisation des moyens de preuve

A. Récolte des données primaires et secondaires

La récolte de données est qualifiée comme étant de type passive car il s'agit uniquement d'intercepter des télécommunications transitant sur des réseaux.

Le TF a précisé que, tel que décrit dans le message CPP, dans le cas d'une boîte courriels, la différence doit être faite entre les courriels que le propriétaire n'a pas encore relevés, lesquels doivent être placés sous surveillance en temps réel bien qu'ils soient déjà conservés sur le serveur de destination, et les courriels déjà relevés, lesquels doivent être mis sous séquestre[39]. La mise sous séquestre ne nécessite pas l'accord du Tmc. La différence entre ces procédures est principalement de ne pas avoir préalablement saisi ou mis en sûreté le support de données[40].

Des mesures de protection du secret professionnel doivent être prises lors de la surveillance (art. 271 CPP, art. 16 let. e LSCPT et art. 5 let. a OSCPT). Un tiers désigné

---

[36] PERRIER DEPEURSINGE, p. 449.
[37] *Idem*, p. 452.
[38] JEANNERET / KUHN, n° 14098.
[39] Message CPP, p. 1232 ; ATF 140 IV 181, consid. 2, JdT 2015 IV 167 (trad.).
[40] ZIMMERMANN, p. 481.

devra trier les informations afin d'en retirer les secrets de fonction[41] et s'assurera que le ministère public n'ait accès qu'aux informations pertinentes pour la procédure[42].

Les communications entre deux parties non visées par les mesures de surveillance mais dont l'une est visée par les catégories professionnelles énumérées aux art. 170 à 173 CPC et dont le sujet porte sur la personne visée doivent être éliminées (art. 271 al. 3 CPP).

B. Utilisation de programmes spéciaux de surveillance

La récolte de données par l'utilisation de programmes spéciaux de surveillance est qualifiée de type active, car il s'agit de faire installer un programme par les forces de l'ordre dans un système d'information ou de télécommunication (art. 269ter CPP).

Ces programmes « GovWare » permettent d'identifier ou de localiser une personne ou une chose, d'écouter, d'enregistrer ou de transférer des télécommunications sans la collaboration du fournisseur de télécommunications[43]. Grâce à eux, les données primaires et secondaires sont interceptées[44]. Ils sont utilisés notamment lorsque les données sont chiffrées avant leur transmission[45].

Des exigences particulières sont requises pour garantir leur fiabilité et leur traçabilité (269^{quater} CPP).

C. Découvertes fortuites

Il arrive de faire des découvertes fortuites incriminant des tiers exclus de l'autorisation de surveillance initiale. Elles peuvent être exploitées lorsqu'une surveillance aurait pu être ordonnée sur ces tiers et sur ces infractions (art. 278 CPP) et pour autant qu'une nouvelle demande d'autorisation ait été octroyée a posteriori; sans quoi, cela deviendrait une « *fishing expedition* » illégale[46].

---

[41] Message CPP, p. 1231 ss.
[42] JEANNERET / KUHN, n° 14103.
[43] *Idem*, n° 14090.
[44] ZIMMERMANN, p. 482.
[45] TEICHMANN / GERBER, p. 122.
[46] JEANNERET / KUHN, n° 14104 ss.

Les autorités ne doivent pas tarder à déposer la demande d'autorisation, sous peine de ne pas pouvoir exploiter les preuves récoltées. Un dépôt dans un délai de deux mois est considéré comme acceptable[47] bien que disputé car trop généreux selon certains auteurs[48]. Un délai de plus de six mois entre la constatation de l'infraction et le dépôt de la demande d'autorisation est en revanche considéré comme un dépôt tardif[49].

III. Voies de droit

A. Des personnes visées

Les personnes visées par des mesures de surveillance doivent être informées a posteriori de l'objet de la surveillance, au plus tard à la clôture de la procédure préliminaire (art. 279 al. 1 CPP). Dans certains cas et avec l'autorisation du tribunal, il est possible de différer ou renoncer à l'information (art. 279 al. 2 CPP) notamment si la recherche est infructueuse. La notification doit avoir une forme officielle, le simple fait de faire écouter au prévenu un extrait intercepté ne comptant pas comme tel[50].

Des auteurs défendent que la personne visée devrait être notifiée même si la recherche est infructueuse, car cela pourrait lui permettre d'amener des preuves à sa décharge[51].

La notification aux personnes visées a pour but de permettre à celles-ci d'exécuter leurs droits, notamment de recours (art. 279 al. 3 CPP). Aussi, le dossier pénal doit contenir toutes les mesures de surveillance mises en œuvre[52] et les enregistrements eux-mêmes[53]. La doctrine a précisé le contenu typique de la notification[54].

---

[47] Arrêt 1B_92/2019 du 2 mai 2019 consid. 2.5.
[48] MÉTILLE, art. 274 CPP n° 28.
[49] Arrêt 1B_107/2022 du 3 janvier 2023 consid. 3.3.
[50] PERRIER DEPEURSINGE, p. 457.
[51] CAPUS / BALLY, pp. 356-357.
[52] *Ibidem*.
[53] JEANNERET / KUHN, n° 14102.
[54] MÉTILLE, art. 279 CPP n°14.

Une documentation lacunaire du dossier devrait amener à un vice de procédure et donc à ne pas pouvoir utiliser le dossier à la charge du prévenu[55].

Lorsque le contenu intercepté a été traduit, il est d'autant plus important que les personnes visées aient accès au dossier pour vérifier que les transcriptions ne présentent pas de défauts[56] ainsi que les qualifications de l'interprète[57].

Le recours est admissible et doit être déposé dans les 10 jours après la notification. Il permet d'analyser la licéité et la proportionnalité de la surveillance, avant l'analyse du fond[58].

B. Des tiers

Les tiers enregistrés ne sont pas parties à la procédure, mais ont toutefois un droit de recours en démontrant une préjudice irréparable, dans le sens où ils auraient un intérêt à ce que les éléments interceptés soient immédiatement détruits pour éviter que des tiers en prennent connaissance[59].

C. Des fournisseurs de services de télécommunication

Les personnes obligées de collaborer n'ont pas de droit de recours sur la légalité de la surveillance (art. 42 al. 2 LSCPT). Elles peuvent demander l'examen de la légalité de la décision uniquement sur des éléments techniques ou organisationnels concernant l'exécution de la surveillance[60]. Compte tenu du caractère généralement urgent de ce type de demandes, le recours contre une décision de surveillance n'a pas d'effet suspensif[61].

Le fournisseur de services de télécommunication est tenu au secret au sujet de la surveillance (art. 39 al. 1 let. d LSCPT).

---

[55] CAPUS / BALLY, p. 361.
[56] *Idem*, pp. 359-360.
[57] GAUDERON, p. 1440 ; JOSITSCH / SCHMID, art. 276 CPP n°2.
[58] JEANNERET / KUHN, n° 14100 ; PERRIER DEPEURSINGE, p. 457.
[59] JEANNERET / KUHN, n° 14100.
[60] *Idem*, p. n° 14101.
[61] Message LSCPT, p. 2397.

Les fournisseurs de services de télécommunication sont indemnisés pour la mise en place des mesures de surveillance (art. 38 al. 2 LSCPT).

Enfin, tout fournisseur ne répondant pas à la demande de surveillance, répondant tardivement, n'ayant pas conservé les données nécessaires ou violant son devoir de secret est passible d'une amende (art. 39 al. 1 LSCPT).

D. Du ministère public

Le ministère public peut faire recours contre décision de refus du Tmc au TF (art. 81. al. 1 let. b LTF), faute d'autre voie de droit. Il a un intérêt digne de protection, car un préjudice irréparable peut être causé vu que les données ne sont conservées que pour une durée limitée[62].

Conclusion

Les mesures de surveillance secrètes, bien que controversées, sont des outils puissants dont l'utilisation est en constante augmentation[63].

Il faut souligner que le TF a adopté[64] une position contraire à celle de la CJUE[65] sur l'interprétation du principe de proportionnalité concernant l'interception des données secondaires de télécommunication. Un tel enregistrement systématique est considéré par la CJUE et par la CourEDH comme excédant le principe de proportionnalité.

Enfin, il est difficile de ne pas évoquer les récentes modifications à la LSCPT qui ont fait l'objet d'une consultation publique[66] avec des prises de positions parfois diamétralement opposées.
Une révision du CPP est prévue courant 2024, laquelle pourrait également affecter ces mesures, probablement en les renforçant.

---

[62] JEANNERET / KUHN, n° 14101 ; PERRIER DEPEURSINGE, p. 451.
[63] Rapport annuel S-SCPT.
[64] ATF 144 I 126, JdT 2018 I 191 (trad.).
[65] Arrêt de la CourEDH du 8 avril 2014, Digital Rights Ireland, C-293/12 et C-594/12, point 69.
[66] Rapport de consultation LSCPT.