

Les mesures de surveillance secrètes en procédure pénale (art. 269 à 298d CPP)

Camilla Natali

avocate au Barreau de Genève, spécialiste FSA droit pénal

16 février 2026

Plan

1. Introduction: Mesures de surveillance secrètes : tour d'horizon des différentes mesures et conditions de leur mise en œuvre
2. Surveillance de la correspondance par poste et télécommunication, IMSI-Catcher et GovWare
3. Autres mesures techniques de surveillance
4. Surveillance des relations bancaires
5. Mesures de surveillance policières (observation, investigation secrète et recherches secrètes)
6. Moyens à disposition de la défense pour contester les mesures de surveillance secrètes (recours et inexploitabilité)
7. Question choisie : mesures de surveillance secrètes transfrontalières
8. Conclusion

1a. Les mesures de surveillance secrètes : Définition et lois applicables

Définition :

Mesures d'enquête prévues dans le Code de procédure pénale qui permettent d'obtenir des informations et/ou des preuves à l'insu des personnes visées, dans des cas strictement encadrés par la loi. Il s'agit d'une exception à la protection de la sphère privée garantie par la Constitution fédérale et la CEDH (art. 13 Cst. féd. Et art. 8 CEDH), qui ne peut intervenir qu'aux conditions de l'art. 36 Cst. féd.

Lois applicables :

- Constitution fédéral : art. 13 Cst. féd. (droit à la vie privée) et art. 36 Cst. féd.
- Chapitre 8 du Code de procédure pénale (CPP): art. 269 à 298d CPP
- Loi sur les télécommunications (LTC)
- Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) et ordonnances (OSCPT, OEI-SCPT, OST-SCPT, OPME-SCPT et OOC-SCPT)
- Lois cantonales sur les mesures préventives (not. Lpol Ge)

1b. Les mesures de surveillance secrètes : définition et tour d'horizon

Surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)	IMSI-catcher (art. 269bis CPP)	GovWare (art. 269ter CPP)	Identification des usagers, localisation et caractéristiques techniques de la correspondance (=données secondaires) (art. 273 CPP)	Identification de l'utilisateur (art. 21 LSCPT)
Autres dispositifs techniques (=écoutes de conversations non publiques, géolocalisation, etc.) (art. 280 et 281 CPP)	Observation (art. 282 CPP)	Surveillance des relations bancaires (art. 284 CPP)	Investigation secrète (= Agent infiltré) (art. 285a ss CPP)	Recherches secrètes (art. 298a ss CPP) et mesures policières préventives

1c. Principe cardinal : la subsidiarité

A. Subsidiarité des mesures de surveillance secrète par rapport aux autres moyens de preuves :

- Les mesures de surveillance secrètes sont **subsidiaires** par rapport aux autres mesures d'investigation (auditions de témoins, perquisitions, etc.)

B. Subsidiarité de certaines mesures de surveillance entre elles :

- IMSI Catcher est subsidiaire aux autres mesures de surveillance de la correspondance (art. 269bis al. 1 let. b CPP)
- GovWare est subsidiaire aux autres mesures de surveillance de la correspondance (art. 269ter let. c CPP)
- Investigation secrète est subsidiaire aux autres mesures

1d. Qui peut ordonner quoi ?

Police	Ministère public	TMC
• Observation secrète jusqu'à 30 jours (art. 282 CPP) • Recherches secrètes jusqu'à 30 jours (art. 298a CPP) • Identification de l'utilisateur de téléphonie ou d'internet (art. 22 LSCPT) • Investigations policières avant enquête (art. 56 ss Lpol/Ge)	• Surveillance de la correspondance par poste et télécommunication (art. 269 CPP) • IMSI Catcher (art. 269bis CPP) • GovWare (art. 269ter CPP) • Données secondaires de télécommunication (art. 273 CPP) • Dispositifs techniques de surveillance (art. 280 CPP) • Observation pour plus de 30 jours ou lorsqu'une procédure est ouverte (Art. 282 al. 2 CPP) • Investigation secrète (art. 285 CPP) • Recherches secrètes de plus de 30 jours ou lorsqu'une procédure est ouverte (art. 298a CPP)	• Surveillance des relations bancaires (art. 284 CPP)

2a. Surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)

- Surveillance «typique» : surveillance de la correspondance postale (lettres, colis) et de la télécommunication (écoutes téléphoniques, mais également surveillance de la communication via internet: p. ex: emails)
- Surveillance peut porter sur le contenu des échanges et sur les données accessoires/secondaires
- Surveillance en temps réel (y compris contenu) VS surveillance rétroactive (≠contenu mais uniquement données secondaires/accessoires) → contenu rétroactif exploitable via séquestre des téléphones, ordinateurs, etc.
- Mesures de surveillance fréquemment ordonnées en Suisse (surveillances en temps réel et surveillances rétroactives) en 2024*:
 - 43% pour élucider des infractions contre le patrimoine
 - 19% pour élucider des infractions contre la vie et l'intégrité corporelle
 - 10% pour élucider des infractions à la Lstup
 - 28% pour élucider les autres infractions confondues
- Nombres de mesures ordonnées en augmentation (+15% entre 2023 et 2024)*
 - Surveillance en temps réel en 2024: 1'818 (1'244 en 2023)
 - Surveillance rétroactives en 2024: 6'149 (4'957 en 2023)
 - Recherches en cas d'urgence en 2024 (LSCPT): 1'223 (1'022 en 2023)
 - Recherches de personnes condamnées en 2024 (LSCPT): 35 (37 en 2023)

* Données disponibles dans: Communiqué de presse – Statistiques de la surveillance des télécommunications: davantage de mesures ordonnées, publié le 29.04.2025 (<https://www.news.admin.ch/fr/newsb/Wtjqigxk2B8qf3XuhuyTs>)

2a. Surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)

Conditions

Le Ministère public peut ordonner la surveillance de la correspondance aux conditions suivantes (art. 269 al. 1 CPP) :

1. Graves soupçons de commission d'une infraction (surveillance répressive et non préventive) → Une instruction doit avoir été ouverte par le Ministère public (mais les soupçons peuvent reposer uniquement sur les rapports de police)
2. Liste des infractions permettant une surveillance: art. 269 al. 1 CPP → Attention : la surveillance ne vaut que pour les infractions visées (+ art. 273 CPP pour les données secondaires = crimes et délits)
3. Proportionnalité → Subsidiarité

2a. Surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)

Objet de la surveillance(art. 270 CPP)

- Peuvent faire l'objet d'une surveillance de la correspondance des personnes suivantes (art. 270 CPP) :
 1. prévenu
 2. tiers si le prévenu utilise son adresse postale ou son raccordement
 3. tiers s'il agit pour le prévenu
- Surveillance d'une personne tenue au secret professionnel (art. 170 – 173 CPP) : art. 271 CPP:
 - Surveillance possible si le prévenu utilise personnellement le raccordement du titulaire du secret, mais pas si le prévenu appelle le raccordement
 - Surveillance possible si graves soupçons pèsent sur le détenteur du secret professionnel lui-même (p. ex: avocat prévenu) et que des raisons particulières l'exigent
 - Tri effectué par le TMC et échanges couverts par le secret = détruits

2a. Surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)

Obligation de collaborer et données susceptibles d'être obtenues

- Fournisseurs: Obligations de collaborer = pouvoir être en mesure d'exécuter en tout temps les mesures de surveillance ordonnées (art. 2 LSCPT): fournisseurs de services postaux (poste suisse), fournisseurs de services de télécommunication au sens de la Loi sur les Télécommunications (opérateurs téléphoniques: Swisscom, Salt, Sunrise, etc.), fournisseurs de services de communications dérivés, exploitants de réseaux de télécommunications internes, personnes qui mettent leur accès à disposition de tiers (hôtels, restaurants, etc.), revendeurs professionnels de cartes SIM et de cartes d'accès internet
- **Les fournisseurs doivent conserver les données durant six mois (art. 19 al. 3, 21 al. 2, 22. al. 2 et 26 al. 5 LSCPT)**
- Attention: certaines données sont conservées plus longtemps : p. ex: données relatives à des clients et données d'identification: pendant toute la durée de la relation commerciale + six mois (art. 21 al. 2 LSCPT)
- Bon à savoir: Certaines données sont susceptibles d'être obtenues par l'utilisateur directement: art. 45 fédérale sur les télécommunications (LTC): l'utilisateur peut exiger du fournisseur de service de télécommunication qu'il lui communique les données utilisées pour la facturation des prestations (notamment ressources d'adressage, heure des communications et rémunération due) (art. 45 al. 1)

2a. Surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)

Autorisation du TMC et communication de la mesure

- Le Ministère public ordonne la surveillance (contenu de l'ordre de surveillance définit aux art. 15 et 49 OSCPT)
- Le Ministère public doit demander au TMC d'autoriser la mesure dans les 24h00 : art. 274 al. 1 CPP
- Le TMC doit autoriser la mesure dans les cinq jours: art. 274 al. 2 CPP
- Durée de l'autorisation: trois mois; prolongeable selon la même procédure : art. 274 al. 5 CPP
- Autorisation cadre possible (mais doit rester l'exception): art. 272 al. 2 CPP
- Levée de la mesure: dès que les conditions ne sont plus remplies ou que le TMC n'a pas autorisé la mesure ou sa prolongation (art. 275 CPP)
- Si autorisation refusée: informations absolument inexploitable (art. 277 al. 2 CPP). Les données doivent être détruites
- Attention: le prévenu n'est pas informé tout de suite de la mesure
- La communication au prévenu doit intervenir au plus tard à la clôture de la procédure préliminaire (art. 279 al. 1 CPP) (sauf rares exceptions: art. 279 al. 2 CPP) → TF 6B_795/2014 du 06.01.2015: communication de l'ordonnance du TMC, avec indication des voies de recours, fait partir le délai de recours (attention à la consultation du dossier). Attention ACPR/71/2019 du 02.01.2019
- Recours dans les 10 jours : art. 279 al. 3 CPP (*cf. infra* 6)

2a. Surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)

Découvertes fortuites (art. 278 CPP)

– Art. 278 Découvertes fortuites

¹ Si, lors d'une surveillance, d'autres infractions que celles qui ont fait l'objet de l'ordre de surveillance sont découvertes, les informations recueillies peuvent être utilisées à l'encontre du prévenu lorsqu'une surveillance aurait pu être ordonnée aux fins de la poursuite de ces actes.

^{1bis} Si, lors d'une surveillance au sens des art. 35 et 36 LSCPT¹⁹⁹, des infractions sont découvertes, les informations collectées peuvent être utilisées aux conditions fixées aux al. 2 et 3.²⁰⁰

² Les informations concernant une infraction dont l'auteur soupçonné ne figure pas dans l'ordre de surveillance peuvent être utilisées lorsque les conditions requises pour une surveillance de cette personne sont remplies.

³ Dans les cas visés aux al. 1, ^{1bis} et 2, le ministère public ordonne immédiatement la surveillance et engage la procédure d'autorisation.²⁰¹

⁴ Les documents et enregistrements qui ne peuvent être utilisés au titre de découvertes fortuites doivent être conservés séparément et détruits immédiatement après la clôture de la procédure.

⁵ Toutes les informations recueillies lors d'une surveillance peuvent être utilisées pour rechercher une personne signalée.

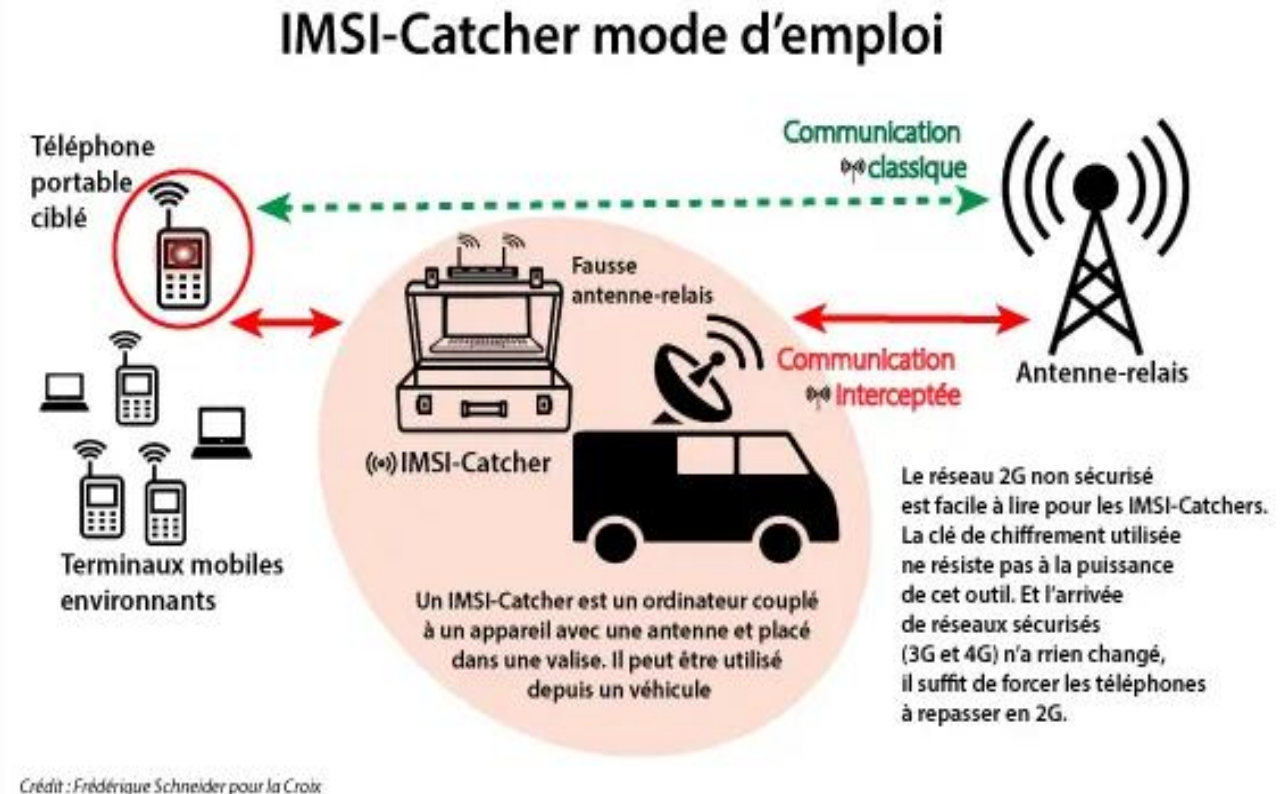
- Pour que les découvertes fortuites soient exploitables, vérifier que la surveillance aurait pu être prononcée à cet égard (en particulier: infractions listées)
- Dès que découverte fortuite contre une personne non visée : la surveillance contre cette personne doit être mise en œuvre (ATF 144 IV 254; TF 1B_211/2012) (→ mais pas une inexploitable automatique: prescription d'ordre ou règle de validité? TF 7B_44/2024 du 14.07.25)
- Conservation séparée des documents et enregistrements découverts fortuitement qui ne respectent pas les conditions de l'art. 278 CPP et destruction

2a. Surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP) - Délimitations

- Attention ≠ mesures de surveillance secrètes :
 - Saisie d'un ordinateur ou d'un téléphone portable (ATF 143 IV 270, c. 4,6) ;
 - Obtention du code PUK et du code PIN pour débloquent les téléphones auprès de l'opérateur (ATF 141 IV 423, c. 1)→ Dans ces cas: règles sur le séquestre
- Surveillance de la correspondance par poste et télécommunication VS dépôt/séquestre :
 - **Courriers** : = art. 269 CPP: pendant l'envoi / ≠ Art. 269 CPP et application des règles sur le séquestre dès réception (= dépôt dans la boîte aux lettres ou accès à la case postale par le destinataire) (ATF 140 IV 181, c. 2.4 et 2.5)
 - **Emails** : = art. 269 CPP : pour emails non relevés / ≠ Art. 269 CPP et application des règles sur le séquestre dès que le prévenu a relevé les emails sur l'appareil par le destinataire (ATF 143 IV 270, c. 4.6, ATF 140 IV 181, c. 2.4) → Attention : qu'en est-il des emails reçus mais non lus?

2b. IMSI Catcher (art. 269bis CPP)

- Aucune intervention des opérateurs mobiles
- Très utiles quand le numéro de téléphone, SIM, IMSI ou IMEI est inconnu.
- Selon la même procédure que celle décrite pour la surveillance de la correspondance et aux mêmes conditions (art. 269 CPP)
- Subsidiaire aux autres mesures
- Autorisation de l'Office fédéral de la communication (OFCOM) pour chaque appareil pour ne pas perturber le réseau (art. 269bis al.1 let. c CPP) (mais pas d'autorisation spécifique par procédure)
- Utilisé 171 fois en Suisse en 2024 (160 en 2023)*



*Données disponibles dans: Communiqué de presse – Statistiques de la surveillance des télécommunications: davantage de mesures ordonnées, publié le 29.04.2025 (<https://www.news.admin.ch/fr/newsb/Wtjqigxk2B8qf3XuhuyTs>)

*Illustration: Frédérique SCHNEIDER in IMSI-Catcher, ou comment les téléphones portables sont écoutés, La Croix, publication du 03.02.2016

2c. GovWare (art. 296ter CPP)

- GovWare: Programmes informatiques spéciaux = Government Software (GovWare) → programme informatique installé à l'insu du détenteur du système informatique et qui permet de prendre le contrôle à distance et d'en surveiller le contenu en temps réel («Cheval de Troie»)
- Introduction de ces programmes dans un système informatique: but = intercepter et lire le contenu des communications cryptées
- Aucune intervention des opérateurs mobiles
- Peut être ordonné aux mêmes conditions que l'art. 269 CPP (mais liste d'infractions restreintes = art. 269ter al. 1 let. b CPP → Infractions listées à l'art. 286 al. 2 CPP)
- Subsidiaire aux autres mesures
- Obligations particulières concernant l'établissement de l'ordre de surveillance
- En pratique: l'implantation se fait par la police, sur ordre du Ministère public
- Selon la même procédure que celle décrite pour la surveillance de la correspondance et des télécommunications
- L'utilisation de GovWare est soumise à des conditions techniques particulières: art. 269quater CPP
- Utilisé 12 fois en Suisse en 2024 (160 en 2023)* (cher et requiert des compétences informatiques)

*Données disponibles dans: Communiqué de presse – Statistiques de la surveillance des télécommunications: davantage de mesures ordonnées, publié le 29.04.2025 (<https://www.news.admin.ch/fr/newsb/Wtjqigxk2B8qf3XuhuyTs>)

3. Autres mesures techniques de surveillance: art. 280 et 281 CPP

- Art. 280 CPP: Le ministère public peut utiliser d'autres dispositifs techniques de surveillance aux fins de :
 - a) d'écouter ou d'enregistrer des conversations non publiques → par exemple micros, amplificateurs de sons, caméras, etc.
 - b) d'observer ou d'enregistrer des actions se déroulant dans des lieux qui ne sont pas publics ou qui ne sont pas librement accessibles → par exemple micros ou caméras dans une maison ou dans une voiture
 - c) De localiser une personne ou une chose → par exemple balise de géolocalisation sur une voiture
- Art. 281 al. 4 CPP = renvoi aux dispositions régissant la surveillance de la correspondance (art. 269 et ss CPP) → Mêmes conditions (autorisation du TMC; délais de recours, etc.)
- Ne peuvent être ordonnées qu'à l'encontre du prévenu (mais possible de surveiller des locaux ou véhicules de tiers si le prévenu se trouve dans les locaux ou utilise les véhicules)
- Pas possible pour enregistrer le comportement d'un prévenu en détention à des fins probatoires ou surveiller les locaux ou véhicules d'un tiers appartenant à l'une des catégories professionnelles visées aux art. 170 à 173 CPP (art. 281 al. 3 CPP)
- Exécution: directement par la police → Attention: si la police récupère la séquence vidéo d'une installation déjà en place = séquestre (art. 263 CPP) et ≠ art. 280-281 CPP

4. Surveillance des relations bancaires: art. 284 et 285 CPP

- Art. 284 CPP : Le TMC peut autoriser la surveillance des relations entre une banque ou un établissement similaire et un prévenu (existence de soupçons suffisants)
 - Doit être ordonnée directement par le TMC (sur demande du Ministère public)
 - Peut viser à élucider toutes les infractions (pas de liste spécifique)
 - Communication : au plus tard au moment de la clôture de la procédure préliminaire (art. 285 al. 3 CPP *cum* art. 279 CPP)
 - Recours: art. 285 al. 4 CPP (*cf. infra* 6)
- Rare. En pratique : plutôt séquestres (art. 263 CPP) ou ordres de dépôt (art. 265 CPP) adressés aux banques

5. Mesures de surveillance policières

Observation art. 282 CPP

Observation secrète de personnes et de choses dans des lieux accessibles (enregistrement audio et vidéo)

→ Ordonnée directement par la police (autorisation du MP quand plus de 30 jours)
≠ autorisation du TMC

Investigation secrète art. 285a CPP

Agents infiltrés avec identité d'emprunt

→ Ordonnée par le Ministère public
→ Autorisation du TMC

Recherches secrètes art. 298a CPP

Intervention policière sans fausse identité (p. ex: faux consommateurs)

→ Ordonnées directement par la police (autorisation du MP quand plus de 30 jours)
≠ autorisation du TMC

Missions de couverture effectuées par la police indépendamment d'une procédure pénale (sans soupçon d'infraction concret)
(p. ex: observation des milieux criminels ou prévention des infractions) ≠ CPP, mais régies par les lois de police cantonale ou fédérale (art. 56 ss Lpol/Ge; Directive du Procureur général D.8 → autorisation du MP quand plus de 30 jours)

5A. Observation: art. 282 ss CPP

- Art. 282 al. 1 CPP: **Le Ministère public**, et pendant l'investigation policière, **la police**, peuvent observer secrètement des personnes et des choses **dans des lieux librement accessibles** et effectuer des enregistrements audio et vidéo (=filature, photographies et enregistrements dans des lieux publics) → Observation = sans contact, à distance et dans des lieux publics (mais observation d'un balcon depuis un lieu public peut être admissible : ATF 137 I 327)
- Conditions:
 - Indices laissant présumer que des **crimes ou des délits** ont été commis (≠ contraventions) (≠ soupçons concrets nécessaires)
 - d'autres formes d'investigation n'auraient aucune chance d'aboutir ou seraient excessivement difficiles (subsidiarité)
- Peut être ordonnée par la police pendant l'investigation pour **un mois maximum** (large pouvoir d'appréciation de la police). Plus d'un mois: autorisation du Ministère public.
- Communication: au moment de la clôture de la procédure préliminaire (sauf exceptions): art. 283 CPP
- Appréciation de la validité des preuves:
 - Observations illicites (par exemple dans un lieu privé ou après la fin du délai d'un mois): inexploitabilité relative (art. 141 al. 2 CPP)
 - Nécessité d'une délégation du Ministère public en cours de procédure : prescription d'ordre = exploitabilité (art. 141 al. 3 CPP) (arrêt du Tribunal fédéral 6B_284/2022 du 16.11.2022)
 - Défaut de documentation d'une observation = exploitabilité relative des informations recueillies (art. 141 al. 2 CPP) (Arrêt du Tribunal fédéral 7B_1059/2023 du 26.03.2025)

5B. L'investigation secrète: art. 285a ss CPP

- Art. 285a CPP: Il y a investigation secrète lorsque des membres du corps de police ou des personnes engagées à titre provisoire pour accomplir des tâches de police **nouent de manière trompeuse, sous le couvert d'une fausse identité attestée par un titre (identité d'emprunt)**, des contacts avec des individus dans l'intention d'instaurer avec eux **une relation de confiance et d'infiltrer un milieu criminel afin d'élucider des infractions particulièrement graves** → **Agents infiltrés** (art. 288 CPP)
- Conditions (art. 286 CPP) :
 - Des soupçons laissent présumer que l'une des infractions visées à l'art. 286 al. 2 CPP a été commise (liste plus restrictive que pour la surveillance de la correspondance: 22 infractions en moins)
 - Proportionnalité : la mesure se justifie au regard de la gravité de l'infraction
 - Subsidiarité: quand les autres actes d'instruction accomplis jusqu'alors n'ont pas abouti ou que les recherches, à défaut de l'investigation secrète, n'auraient aucune chance d'aboutir
- Ordonnée par le Ministère public et autorisation du TMC dans les 24h00 (art. 289 CPP). Autorisation du TMC accordée pour un an au plus (art. 289 al. 5 CPP). Refus d'autorisation = inexploitabilité absolue et destruction immédiate (art. 289 al. 4 CPP)
- Découvertes fortuites: exploitables si une investigation secrète aurait pu être ordonnée pour ces nouveaux faits (art. 296 al. 1 CPP). Le Ministère public rend sans délai une décision ordonnant l'investigation secrète et engage la procédure d'autorisation (art. 296 al. 2 CPP).
- Communication: au plus tard au moment de la clôture préliminaire (exceptions possibles) : art. 298 CPP
- Appréciation de la validité des preuves: inexploitabilité absolue (art. 140 et 141 al. 1; art. 289 al. 6 CPP) ou relative (art. 141 al. 2 CPP)
- Recours dans les 10 jours : art. 298 al. 3 CP (cf. infra 6)

5B. L'investigation secrète:

art. 285a ss CPP – Mission de l'agent

- Mission de l'agent :
 - La police dote l'agent d'une identité d'emprunt (art. 288 al.1 CPP)
 - Possible de garantir l'anonymat du policier même durant le procès (art. 288 al. 2 CPP)
 - L'agent infiltré est soumis aux instructions de la personne de contact (= commandement de la police): intermédiaire entre agent infiltré et autorités de poursuite pénales (art. 291 CPP)
 - Exemption de peine de l'agent (art. 294 CPP) (infractions à la LStup + art. 197 al. 4 et 5 CPP)
 - **L'agent doit se conformer aux instructions données (art. 292 CPP)**
 - **Interdiction de l'agent provocateur (art. 293 CPP) :**
 - L'agent infiltré ne doit avoir qu'un rôle mineur sur la décision du tiers de commettre une infraction (pas d'encouragement à commettre une infraction): TF 6B_832/2024 du 02.04.24
 - Si dépassement des limites. Le juge doit en tenir compte dans la fixation de la peine concernant la nouvelle infraction ; il peut aussi libérer de toute peine la personne influencée (art. 293 al. 4 CPP). Poursuite contre l'agent infiltré pour instigation ou complicité possible

5B. L'investigation secrète:

art. 285a ss CPP – Respect des principes de base

- L'agent infiltré doit respecter les principes de base du CPP: art. 3 et 113 CPP (interdiction d'utiliser des méthodes d'enquête abusives et respect du droit de ne pas s'auto-incriminer) (art. 6 CEDH; Arrêt Grba c. Croatie (74074/12) sur 23.11.2017) → Valable lorsque le prévenu refuse de répondre ou ment sur son implication dans le cadre de la procédure (ATF 148 IV 202, c. 2.5.3; TF 6B_1294/2023 du 23.10.2025, c. 1.5.3)
- ATF 148 IV 205 (JdT 2023 IV 96): Affaire de spiritisme :
 - Interdiction pour les agents d'obtenir des aveux par une méthode interdite (recours à la force, menaces, promesses, tromperies et moyens susceptibles de restreindre les facultés intellectuelles ou le libre arbitre) et en contournement du droit de ne pas s'auto-incriminer → dans un tel cas: inexploitableté absolue des déclarations (art. 140 CPP et art. 141 al. 1 C PP). Inexploitableté absolue des déclarations si un agent infiltré incite un prévenu à faire des déclarations en exerçant des pressions excessives et en éludant son droit à ne pas s'auto-incriminer → Contournement du droit de ne pas s'auto-incriminer lorsque l'agent secret pousse le prévenu à faire des aveux qu'il n'aurait pas fait spontanément (≠contournement lorsque le prévenu fait des aveux spontanés)
- TF 6B_1294/2023 du 23.10.2025: Exploitableté d'aveux obtenus par des agents infiltrés car par d'interrogatoire sous pression et exploitableté des aveux obtenus lorsqu'un prévenu a consommé de l'alcool mais n'était pas ivre
- Agent infiltré dans une cellule à Champ-Dollon → Licite? Pas tranché car pas de recours formé dans les 10 jours (AARP/443/2019). Exploitableté des déclarations? ≠ tranché par le TF: TF 6B_247/2020 du 25.05.2020

5C. Recherches secrètes: art. 298a CPP

- Art. 298a CPP: Membres du corps de police tentent d'élucider des **crimes ou des délits** dans le cadre d'interventions de **courte durée** où leur identité et leur fonction ne sont pas reconnaissables (≠ identité d'emprunt), notamment en **concluant des transactions fictives** ou en donnant l'illusion de vouloir conclure de telles transactions
- P. ex: policiers qui se font passer pour de faux consommateurs pour acheter de la drogue ou pour des jeunes sur des chats pour entrer en contact avec des pédophiles. Pas d'identité d'emprunt ni d'anonymat
- Conditions et mise en œuvre: similaire aux observations: peuvent se faire par la police en investigation policière pendant un mois, puis avec autorisation du ministère public (art. 298b CPP). Pas de durée maximale. Mais il faut des soupçons suffisants qu'un crime ou un délit a été commis ou est en cours (≠ contraventions → art. 172ter CP)
- ≠ forme prévue pour la mise en œuvre des recherches secrètes par la police
- Pas d'autorisation du TMC
- Inexploitabilité relative en cas de défaut d'autorisation par le Ministère public au-delà d'un mois (art. 141 al. 2 CPP) → Pesée des intérêts
- Interdiction de l'agent provocateur:
 - Fin de la recherche secrète: art. 298d al. 1 let. c CPP
 - Atténuation de la peine: art. 298c al. 2 *cum* art. 293 al. 4 CPP
 - Inexploitabilité des informations recueillies : art. 140 et 141 CPP
 - Eventuellement: procédure pénale contre l'agent pour complicité/incitation
- Communication: art. 298d CPP, renvoi à l'art. 298 al. 1 et 3 CPP: au plus tard au moment de la clôture de la procédure préliminaire.
- Recours dans les 10 jours: art. 298d al. 4 *cum* art. 298 al. 3 CPP (*cf. infra* 6)

5D. Recherches secrètes vs Investigation secrète – Appréciation au cas par cas

	Recherches secrètes (art. 298a ss CPP)	Investigation secrète (art. 285a ss CPP)
Durée	Engagement de courte durée	Infiltration de longue durée du milieu criminel
Confiance	Pas de lien de confiance	Agent infiltré: établissement d'un lien de confiance dans le but d'atteindre les objectifs fixés
Identité	Identité réelle, mais fonction non reconnaissable	Fausse identité soutenue par des actes/documents authentiques
Autorisation	Ordonnées par la police ou le ministère public; pas de procédure d'autorisation du TMC	Soumise à l'autorisation du TMC

5E. Recherches secrètes vs investigation secrète

Participation de la police à un chat

- ATF 143 IV 25 (JdT 2017 IV 275) :
 - Enquêteur de police qui se fait passer pour «Sabrina», 14 ans, sur un forum de discussion pour enfants et adolescents sur internet. «Sabrina» commence à chater avec X, un utilisateur du chat au hasard. A ce stade ≠ soupçon concret de la commission d'une infraction ≠ CPP, mais activité de prévention fondée sur la Loi sur la police zurichoise. La conversation entre «Sabrina» et X est orientée par X sur un contenu à caractère sexuel. X demande l'adresse email de «Sabrina» et lui envoie une photographie de son pénis → Envoi de la photographie = soupçon de tentative de pornographie → TF = recherches secrètes (≠ investigation secrète) car l'utilisation de pseudonyme sur un chat ≠ création de titre prouvant une identité d'emprunt + courte durée (discussion : 9 jours), ≠ véritable relation de confiance car pas de rencontre et ≠ infiltration d'un milieu criminel → Pas besoin de l'autorisation du TMC → informations obtenues = exploitables
- ATF 151 IV 211 :
 - Enquêteur de police qui analyse un chat sur internet (= enquête policière). Enquêteur se faisant passer pour un garçon de 14 ans, répond à une annonce publiée par A qui indique «*Quarantenaire je cherche fiston obéissant, soumis, qui souhaite passer de bons moments sous la couette avec son papounet. Pas crad, pas de violence, mais respect et hygiène*». L'enquêteur propose un rdv et A. se rend à ce rdv → Tentative d'actes d'ordre sexuel avec des enfants (art. 187 CP). D'abord: recherches préventives secrètes (Lpol/Fr), puis recherches secrètes (art. 298a CPP). Mêmes conditions. TF: les soupçons n'ont pas besoin d'être concrets. Pas de provocation ici car l'agent infiltré a simplement répondu à l'annonce publiée par A → Exploitabilité des informations recueillies

6. Moyens à disposition de la défense pour contester les mesures de surveillance secrètes

	Recours art. 279 al. 3, 285 al. 4 , 298 al. 3, 298d al. 4 CPP	Inexploitabilité art. 140 et 141, 269ter al. 3, 271 al. 43, 277 al. 2, 278 al. 4, 289 al. 6 CPP
Objet	Recours contre l'ordonnance de la mesure de surveillance Motif: contester la légalité/la licéité de la mesure (p.ex: infraction hors catalogue, soupçons insuffisants, défaut proportionnalité et subsidiarité, non respect des règles formelles, etc.)	Vise la validité des informations/preuves recueillies par le biais de la mesure de surveillance Motif: on attaque l'illégalité de la mesure sur le fond (p. ex: violation grave des règles de procédure, violation du droit au silence, surveillance non autorisée, agent provocateur, découvertes fortuites non valables, infractions hors catalogue, mesure à l'étranger non autorisée, etc.)
Délai	Recours à déposer dans les 10 jours dès la connaissance de la mesure (=communication; attention à la consultation de dossier (TF 1B_40/2016))	Demande de constatation de l'inexploitabilité et retranchement des pièces du dossier: en tout temps Recours contre refus de retranchement dans les 10 jours (art. 393 al. 1 let. a CPP) → Recours au Tribunal fédéral si préjudice irréparable
Conséquence	Annulation des mesures de surveillance → Inexploitabilité absolue des informations recueillies (art. 141 al. 1 CPP) → Destruction	Inexploitabilité absolue des informations recueillies (art. 141 al. 1 CPP) → Destruction immédiate Inexploitabilité relative (art. 141 al. 2 CPP) → Pesée des intérêts Exploitabilité (art. 141 al. 3 CPP) → Exploitabilité

6a. Moyens à disposition de la défense pour contester les mesures de surveillance secrètes – Inexploitabilité

- Distinction: inexploitabilité absolue (art. 140 et 141 CPP: art. 289 al. 6, 269ter al. 3 CPP, 271 al. 3, 277 al. 2, 278 al. 4, 281 al. 4, 289 al. 6 CPP), inexploitabilité relative (art. 141 al. 2 CPP) et exploitabilité (art. 141 al. 3 CPP)
- Demander l'inexploitabilité des preuves recueillies et le retranchement des preuves du dossier → *timing*?
- Recours au Tribunal fédéral ouvert contre les décisions refusant l'inexploitabilité, lorsque la loi prévoit la restitution immédiate ou la destruction immédiate des preuves illicites (p. ex: art. 271 al. 3, 277 al. 2 et art. 289 al. 6 CPP): ATF 141 IV 284, c. 2.3) → P. ex: recours au Tribunal fédéral contre décision refusant l'inexploitabilité et la destruction d'écoutes effectuées sans droit à l'étranger (TF 1B_164/2019 du 15.11.2019)
- Pas de recours direct au Tribunal fédéral contre la décision d'exploitabilité concernant une observation (art. 282 CPP) (TF 1B_450/2017 du 29.03.2018)

7. Question choisie: mesures de surveillance secrètes transfrontalières

- Entraide:
 - Surveillance de la correspondance par poste et télécommunication en cas d'entraide: art. 18a EIMP → Également soumise aux conditions des art. 269 ss CPP
 - Surveillance effectuée à l'étranger par l'état étranger ≠ soumise à autorisation mais il faut démontrer que la surveillance a respecté le droit appliqué dans le pays concerné.
- SMS envoyés par des agents suisses à un prévenu situé à l'étranger → Exploitabilité : ATF 150 IV 308
- Mesures de surveillance ordonnées en Suisse mais menées en France (par exemple: balises et micros posés dans une voiture en Suisse qui dépasse la frontière) => En principe inexploitable (violation du principe de la territorialité). Admissibles seulement si autorisées par (ATF 150 IV 308, ATF 146 IV 36, ATF 138 IV 169):
 - L'EIMP: ATF 146 IV 36: Données récoltées à l'étranger: transmission d'informations en temps réel (surveillance en temps réel) = exclue en droit suisse donc exclue pour l'étranger (réciprocité; art. 30 EIMP) → Quid de l'art. 80d bis EIMP?
 - Un accord international: pour l'observation transfrontalière: art. 40 de la Convention d'application de l'accord Schengen + Accords avec les Etats voisins (p. ex: Accord bilatéral de coopération policière avec la France (art. 12) (RS 0.360.349.1)) : Accord a posteriori possible pour l'observation transfrontalière à demander dans les 12h00 (TF 1B_302/2020). Quid pour les autres mesures?
 - Un accord préalable de l'Etat étranger sur le sol duquel les mesures sont recueillies → Accord a posteriori possible pour l'observation transfrontalière à demander dans les 12h00: TF 1B_302/2020 du 15.02.2021. Application p.a pour les autres mesures de surveillance? Quel délai? Non tranché par le TF (ACPR/417/2025 du 02.06.2025)

8. Conclusion

- Conseiller les client-e-s en connaissance de cause; les informer des mesures qui ont été potentiellement ordonnées (avant la communication)
- Dès communication: vérifier que les mesures ont été ordonnées correctement (respect de la légalité et du cadre formel) → Recours dans les 10 jours
- Vérifier l'exploitabilité des mesures et demander le retranchement des informations recueillies inexploitable → *Timing* et conséquences sur la procédure
- Attention aux aveux avant la communication des mesures de surveillance

Questions ?

Merci de votre attention !

Camilla Natali
Avocate – Associée
Spécialiste FSA droit pénal
cnatali@harari-avocats.ch

Harari Avocats
Rue Ferdinand-Hodler 23
Case postale
1211 Genève 3

T. +41 (0) 22 819 40 00
info@harari-avocats.ch
www.harari-avocats.ch