# Circulaire du 2 décembre 2016 de présentation des dispositions de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relative au renforcement du dispositif en matière de lutte contre la délinquance et la criminalité organisée

**NOR : JUSD1635582C**

Le garde des sceaux, ministre de la justice,

à

Pour attribution

*Mesdames et messieurs les procureurs généraux près les cours d'appel*
*Monsieur le procureur de la République près le tribunal supérieur d'appel*
*Mesdames et messieurs les procureurs de la République près les tribunaux de grande instance*
*Madame la procureure de la République financier près le tribunal de grande instance de Paris*

Pour information

*Mesdames et messieurs les premiers présidents des cours d'appel*
*Monsieur le président du tribunal supérieur d'appel*
*Mesdames et messieurs les présidents des tribunaux de grande instance*
*Monsieur le membre national d'Eurojust pour la France*

Date d'application : immédiate

Annexes : 10

La loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale complète le dispositif instauré par la loi du 9 mars 2004 en prenant en compte l'évolution des nouvelles technologies et leur emploi dans le cadre d'activités criminelles, nécessitant une adaptation des textes de procédure et de droit pénal.

En consacrant le recours à des techniques d'enquête désormais adaptées aux transformations récentes de la criminalité, certaines dispositions de cette loi offrent aux magistrats des outils permettant de lutter plus efficacement contre les organisations criminelles, lesquelles recourent à de nouveaux moyens afin de déjouer les surveillances techniques mises en place par les services enquêteurs.

En effet, à l'utilisation de téléphones « dédiés » fonctionnant en circuit fermé, se sont ajoutés d'autres modes de communication sécurisés, tels les outils VoIP (voix internet protocole) permettant de communiquer soit par Internet ou par des réseaux compatibles privés, soit à travers des échanges cryptés. De même, les messageries instantanées ne peuvent être aisément interceptées.

Par ailleurs, la loi n° 2016-731 du 3 juin 2016 adapte également les dispositions applicables en matière douanière à l'évolution des formes de délinquance, en particulier par une extension des différentes prérogatives conférées aux agents des douanes.

En dernier lieu, cette loi introduit un cadre juridique spécifique relatif à l'usage des armes par les forces de l'ordre dans l'hypothèse d'un périple meurtrier.

## 1. Des moyens d'enquête adaptés aux évolutions de la criminalité organisée et aux technologies qu'elle emploie

### *1.1. Une adaptation par l'amélioration des moyens existants*

#### 1.1.1. En matière de sonorisation et de captation d'images

En introduisant les articles 706-96 et 706-96-1 au sein du code de procédure pénale, le législateur a prévu qu'en matière de criminalité organisée, le procureur de la République puisse désormais disposer de la faculté de recourir, sur autorisation préalable du juge des libertés et de la détention, aux sonorisations dans des lieux ou véhicules privés ou publics et fixations d'images dans un lieu privé.

Les dispositifs de sonorisation et de captation d'images peuvent être autorisés de manière alternative ou cumulative par le juge des libertés et de la détention.

En vue de mettre en place le dispositif technique utilisé à ces fins, le juge des libertés et de la détention peut autoriser l'introduction dans un véhicule ou un lieu privé, y compris hors des heures autorisées pour les perquisitions, à l'insu du propriétaire ou du possesseur du véhicule ou de l'occupant des lieux.

Ces dispositifs ne peuvent être mis en œuvre :

- dans un cabinet d'avocat, à son domicile ou dans son véhicule ;
- dans les locaux ou véhicules professionnels d'une entreprise ou agence de presse ; entreprise de communication audiovisuelle, de communication au publique en ligne ;
- au domicile d'un journaliste ;
- dans les locaux d'une juridiction ;
- au domicile d'une personne exerçant des fonctions juridictionnelles ;
- dans le véhicule, au bureau ou au domicile d'un magistrat ;
- dans le véhicule, au bureau ou au domicile de parlementaires.

Ces techniques spéciales d'enquête peuvent être utilisées pour une durée d'un mois renouvelable une fois dans les enquêtes menées par le parquet et de deux mois renouvelable dans la limite de deux ans à l'instruction. Le point de départ de ce délai doit être fixé au jour de la mise en place effective de la mesure.

Les séquences ayant trait à la vie privée qui sont étrangères aux infractions visées ne peuvent être conservées en procédure (article 706-101 du code de procédure pénale).

#### 1.1.2. En matière de témoignages

L'introduction de deux nouveaux articles 706-62-1 et 706-62-2 au sein du code de procédure pénale permet désormais à un témoin de déposer publiquement sans que son identité soit révélée et de se voir offrir une protection et la possibilité de recourir à une identité d'emprunt.

- *Le témoignage anonyme devant les juridictions (article 706-62-1 du code de procédure pénale)*

Désormais, pour les procédures portant sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement, lorsque la révélation de l'identité d'un témoin est susceptible de mettre gravement en danger sa vie ou son intégrité physique ou celles de ses proches, le juge d'instruction ou le président de la juridiction de jugement statuant en chambre du conseil peut ordonner soit d'office, soit à la demande du procureur de la République ou des parties, que cette identité ne soit pas mentionnée au cours des audiences publiques et ne figure pas dans les ordonnances, jugements ou arrêts de la juridiction d'instruction ou de jugement qui sont susceptibles d'être rendus publics.

Le juge d'instruction adresse sans délai une copie de la décision ordonnant la confidentialité de l'identité du témoin, qui n'est pas susceptible de recours, au procureur de la République et aux parties.

Le témoin est alors désigné au cours des audiences ou dans les ordonnances, jugements ou arrêts par un numéro que lui attribue le juge d'instruction ou le président de la juridiction de jugement.

Le fait de révéler l'identité d'un témoin ayant bénéficié de ces dispositions ou de diffuser des informations permettant son identification ou sa localisation est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.

- *Le dispositif de protection des témoins (article 706-62-2 du code de procédure pénale)*

Pour les procédures portant sur un crime contre l'humanité, un crime ou délit de guerre, ou une infraction relevant du champ de la délinquance en bande organisée, lorsque l'audition d'un témoin est susceptible de mettre gravement en danger sa vie ou son intégrité physique ou celle de ses proches, ce témoin doit faire l'objet, en tant que de besoin, de mesures de protection destinées à assurer sa sécurité.

Ces mesures de protection sont définies, sur réquisitions du procureur de la République, par la commission nationale chargée d'assurer le suivi des mesures de protection, qu'elle peut modifier ou auxquelles elle peut mettre fin à tout moment. En cas d'urgence, les services compétents prennent les mesures nécessaires et en informent sans délai la commission nationale. Un décret en conseil d'État fixe les conditions d'application du présent article.

En cas de nécessité, le témoin peut être autorisé, par ordonnance motivée rendue par le président du tribunal de grande instance, à faire usage d'une identité d'emprunt. Toutefois, il ne peut pas être fait usage de cette identité d'emprunt pour une audition au cours de la procédure dans laquelle ce dernier est témoin.

Les membres de la famille et les proches du témoin concerné peuvent également faire l'objet de mesures de protection et être autorisés à faire usage d'une identité d'emprunt, dans les mêmes conditions.

Le fait de révéler qu'une personne fait usage d'une identité d'emprunt ou de révéler tout élément permettant son identification ou sa localisation est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende. Lorsque cette révélation a eu pour conséquence, directe ou indirecte, des violences à l'encontre de cette personne ou de son conjoint, de ses enfants ou de ses ascendants directs, les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende.

Les peines sont portées à dix ans d'emprisonnement et à 150 000 euros d'amende lorsque cette révélation a eu pour conséquence, directe ou indirecte, la mort de cette personne ou de son conjoint, de ses enfants ou de ses ascendants directs.

### 1.1.3. La création d'un nouveau critère de compétence territoriale en matière de crimes et délits commis par le biais d'un réseau de communication électronique

L'article 28 de la loi crée un nouveau critère de compétence à l'article 113-2-1 du code pénal pour les crimes et délits commis par le biais d'un réseau de communication électronique : lorsque ces faits sont tentés ou commis **au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République**, ils sont réputés commis sur le territoire de la République.

Cette nouvelle disposition n'impose pas de plainte préalable.

Les dispositions relatives à la compétence du procureur de la République, du juge d'instruction et du tribunal correctionnel ont été corrélativement modifiées[1].

### 1.1.4. L'extension des règles applicables en matière de criminalité organisée aux délits d'atteinte aux systèmes de traitement automatisé de données (STAD), de sabotage et d'évasion en bande organisée ainsi que de blanchiment aggravé

L'article 28 de la loi modifie les dispositions spécifiques de l'article 706-72 du code de procédure pénale relatif aux **atteintes aux systèmes de traitement automatisé de données** (article 323-1 à 323-4-1 du code pénal) et au **sabotage** (article 411-9 du code pénal) dans un double objectif :

- créer une compétence concurrente des juridictions parisiennes (du procureur de la République, du pôle de l'instruction, du tribunal correctionnel et de la cour d'assises de Paris) pour ces infractions ;

1 Articles 43, 52 et 382 du code de procédure pénale.

- appliquer certaines techniques spéciales d'enquête prévues en matière de criminalité organisée aux infractions précitées ainsi qu'au blanchiment de ces infractions et à l'association de malfaiteurs qui a pour objet la préparation de l'un desdits délits.

Aux termes de l'article 706-72 du code de procédure pénale, **sont ainsi possibles** les actes d'enquête suivants :

- la surveillance prévue par l'article 706-80 du code de procédure pénale ;
- l'infiltration prévue par les articles 706-81 à 706-87 du code de procédure pénale ;
- l'enquête sous pseudonyme prévue par l'article 706-87-1 du code de procédure pénale ;
- les interceptions de correspondances émises par la voie des communications électroniques prévues par les articles 706-95 à 706-95-10 du code de procédure pénale ;
- les sonorisations et fixations d'image prévues par les articles 706-96 à 706-102 du code de procédure pénale ;
- la captation de données informatiques prévue par les articles 706-102-1 du code de procédure pénale ;
- les mesures conservatoires prévues par l'article 706-103 du code de procédure pénale.

**Sont en revanche exclues** :

- les dispositions relatives à la garde à vue ;
- les dispositions relatives aux perquisitions de nuit.

L'article 28 introduit deux nouvelles infractions au sein de la liste prévue par l'article 706-73-1 du code de procédure pénale lequel prévoit désormais que le régime de la criminalité organisée, exception faite des règles relatives à la garde à vue, est applicable :

- aux atteintes aux **systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat commis en bande organisée** (prévu à l'article 323-4-1 du code pénal) ;
- au délit d'**évasion commis en bande organisée** (prévu au second alinéa de l'article 434-30 du code pénal).

Cet article autorise ainsi, pour ces deux infractions, ainsi que pour le blanchiment de ces infractions et l'association de malfaiteurs qui a pour objet leur préparation, le recours aux techniques spéciales d'enquête suivantes :

- l'infiltration (articles 706-81 et suivants) ;
- la perquisition de nuit (articles 706-89 et suivants) ;
- les écoutes téléphoniques en flagrance ou préliminaire (articles 706-95 et suivants) ;
- les sonorisations et fixations d'images (articles 706-96 et suivants) ;
- la captation de données informatiques (articles 706-102 et suivants).

#### 1.1.5. L'aggravation des peines d'amende en cas de non réponse à des réquisitions en matière de cryptologie

Les peines d'amendes prévues à l'article 434-15-2 du code pénal ont été alourdies.

Ce texte réprime le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités.

Antérieurement sanctionnés d'une peine de 45 000 euros d'amende, ces faits sont désormais punis d'une peine de 270 000 euros.

Lorsque le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine a été portée de 75 000 à 450 000 euros d'amende.

Les peines d'emprisonnement, respectivement de 3 et 5 ans, n'ont pas été modifiées.

### *1.2. Une adaptation par la création de nouveaux moyens d'enquête*

#### 1.2.1. L'accès aux correspondances électroniques

Afin de créer un régime juridique spécifique en matière de criminalité organisée permettant, au parquet avec l'autorisation préalable du juge des libertés et de la détention, et au juge d'instruction, de récupérer, à distance et à l'insu de la personne visée, les correspondances électroniques stockées et accessibles au moyen d'un identifiant informatique, le législateur a introduit un nouveau dispositif par les articles 706-95-1, 706-95-2 et 706-95-3 du code de procédure pénale.

Dans l'objectif de renforcer l'efficacité de l'ensemble des enquêtes, la possibilité d'accéder aux données informatiques stockées a été ouverte au magistrat instructeur (article 706-95-2 du code de procédure pénale) ainsi qu'au procureur de la République, sur autorisation du juge de la liberté et de la détention (article 706-95-1 du code de procédure pénale).

L'article 706-95-3 précise que ces opérations sont effectuées sous l'autorité et le contrôle du magistrat qui les a autorisées et ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans la décision de ce magistrat. Cependant, si ces opérations révèlent des infractions autres que celles visées dans la décision du magistrat qui les a autorisées, cela ne constitue pas une cause de nullité des procédures incidentes.

Pour procéder à ces opérations, le magistrat ou l'officier de police judiciaire peuvent requérir tout agent qualifié d'un service ou d'un organisme placé sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de communications électroniques autorisé.

Enfin, lorsque l'identifiant informatique est associé au compte d'un avocat, d'un magistrat, d'un sénateur ou d'un député, le dispositif rend applicable l'article 100-7 du code de procédure pénale prévoyant l'information préalable du bâtonnier, du premier président ou du procureur général ou du président de l'assemblée à laquelle il appartient.

#### 1.2.2. Le recours aux IMSI-catcher

Les articles 706-95-4 à 706-95-10 introduits par la loi instaurent un régime juridique encadrant l'utilisation de dispositifs techniques dits « IMSI-catcher » dans le cadre des enquêtes judicaires, menées par le procureur de la République, après autorisation du juge des libertés et de la détention, ou des informations judiciaires conduites par le juge d'instruction.

Le recours à l'IMSI-catcher n'est possible que dans le cadre des procédures relevant de la criminalité organisée, portant sur les infractions visées par les articles 706-73 et 706-73-1 du code de procédure pénale.

Le recours à ce dispositif technique permet :

- d'une part d'identifier les **données techniques** *de connexion* permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur (numéros de téléphone et numéros IMEI notamment) ou *de localisation* de personnes ciblées par l'enquête ;
- et d'autre part, d'**intercepter les correspondances** émises ou reçues par un équipement terminal.

Le code de procédure pénale pose le principe de la nécessité d'une autorisation délivrée par le juge des libertés et de la détention ou par le juge d'instruction prenant la forme d'une **ordonnance écrite et motivée** qui n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

Les opérations de recueil de données techniques ou d'interceptions de communications réalisées à l'aide d'un dispositif IMSI-catcher sont effectuées **sous l'autorité et le contrôle du magistrat** qui les a autorisées et ne peuvent, à peine de nullité, avoir un autre objet que la recherche et la constatation des infractions visées dans la décision de ce magistrat.

Le fait que les opérations révèlent des infractions autres que celles visées dans la décision du magistrat qui les a autorisées ne constitue pas une cause de nullité des procédures incidentes.

Les autorisations sont accordées pour des **durées** relativement courtes :

- en matière de recueil de données de connexion, l'autorisation est donnée pour un mois renouvelable une fois dans le cadre d'une enquête parquet et pour deux mois renouvelable dans la limite de 6 mois dans le cadre d'une information judiciaire ;
- en matière d'interceptions de communications, l'autorisation est accordée pour une durée de 48 heures renouvelable une fois en enquête et à l'instruction.

En **cas d'urgence** résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, le procureur de la République peut autoriser pour une durée de vingt-quatre heures le recours à l'IMSI-catcher, dans l'une ou l'autre de ses modalités[2]. Cette autorisation du procureur de la République doit comporter l'énoncé des circonstances de fait établissant l'existence du risque imminent et être confirmée par le juge des libertés et de la détention dans un délai maximal de vingt-quatre heures. À défaut, il est mis fin à l'opération, les données ou correspondances recueillies sont placées sous scellés fermés et ne peuvent pas être exploitées ou utilisées dans la procédure.

Aux termes des articles 706-95-9 du code de procédure pénale, s'agissant du recueil des données techniques, et des articles 100-4 à 100-7 du même code s'agissant des interceptions de communications, il est prévu que l'officier de police judiciaire dresse **procès-verbal** des opérations effectuées mentionnant la date et l'heure auxquelles chacune des opérations nécessaires a commencé et s'est terminée. Ce dernier doit également joindre au procès-verbal les données recueillies qui sont **utiles à la manifestation de la vérité**.

Les données recueillies à l'aide d'un dispositif IMSI-catcher sont détruites, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique ou lorsqu'une décision définitive a été rendue au fond. Il est dressé procès-verbal de l'opération de destruction.

S'agissant des enquêtes parquet, la loi pose l'exigence que le juge des libertés et de la détention qui a délivré ou confirmé l'autorisation soit informé dans les meilleurs délais par le procureur de la République des actes accomplis et des procès-verbaux dressés en exécution de son autorisation.

### 1.2.3. L'accès aux données informatiques stockées

Jusqu'à présent, les dispositions de l'article 706-102-1 du code de procédure pénale autorisaient la captation, *sans le consentement des intéressés,* des données informatiques *« telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels ».*

Le législateur a donc modifié les articles 706-102-1 et suivants du code de procédure pénale afin que la captation des données informatiques ne soit plus réservée à celles qui s'affichent sur un écran ou sont reçues et émises par des périphériques audiovisuels, mais également étendue à celles qui sont *« stockées dans un système informatique ».*

En effet, auparavant, ces dispositions ne permettaient pas de capter à distance les données stockées dans un ordinateur ou sur un serveur de type *« cloud ».*

En outre, par un arrêt en date du 8 juillet 2015, la Cour de cassation a clairement énoncé que si les dispositions des articles 100 et suivants du code de procédure pénale relatifs aux interceptions de correspondance permettaient d'enregistrer les courriels envoyés et reçus postérieurement à l'autorisation d'interception, ils ne pouvaient en revanche pas servir à consulter ceux conservés au sein d'une boite de courrier électronique[3].

2 Cette possibilité fait écho à celle offerte, par l'article 230-35 du code de procédure pénale, à un enquêteur, de procéder à la pose, en urgence, d'un dispositif de géo-localisation, et d'en aviser postérieurement le procureur de la République ou le juge d'instruction à charge pour ces derniers de prescrire la poursuite des opérations ou d'en ordonner la main levée.

Les services répressifs étaient par conséquent contraints, pour prendre connaissance de cette correspondance électronique mais également pour accéder à tout autre élément stocké dans un système de traitement automatisé de données, de procéder à une perquisition en respectant la procédure applicable à cette mesure, à savoir la présence du mis en cause ou de deux témoins.

Les règles relatives à la perquisition s'avèrent toutefois particulièrement inadaptées aux contraintes des enquêtes diligentées pour des faits de criminalité organisée ou de terrorisme dès lors qu'elles ne permettent pas de procéder à l'interception des données conservées à l'insu du propriétaire.

Ces modifications législatives, qui accroissent les pouvoirs d'enquête sous le contrôle du juge, devraient donc permettre de renforcer l'efficacité des investigations judiciaires.

Afin de renforcer l'efficacité de l'ensemble des enquêtes, la possibilité d'accéder aux données informatiques stockées a été ouverte :

- au procureur de la République, sur autorisation du juge de la liberté et de la détention (article 706-102-1 du code de procédure pénale) qui peut y procéder pour une durée d'un mois renouvelable une fois ;
- au magistrat instructeur (article 706-102-2 du code de procédure pénale) qui peut y procéder pour une durée de quatre mois renouvelable une fois.

La décision doit être prise par ordonnance motivée mentionnant l'infraction concernée, la localisation ou la description détaillée des STAD concernés.

#### 1.2.4. L'ouverture de scellés aux fins de décryptage

L'article 230-2 du code de procédure pénale, relatif à la mise au clair de données chiffrées nécessaires à la manifestation de la vérité, a été complété afin d'autoriser l'organisme technique soumis au secret de la défense nationale désigné aux fins de décryptage à procéder à l'ouverture ou à la réouverture des scellés et à confectionner de nouveaux scellés après avoir, le cas échéant, procédé au reconditionnement des supports physiques qu'il était chargé d'examiner.

Le texte prévoit en outre qu'en cas de risque de destruction des données ou du support physique qui les contient, l'autorisation d'altérer le support physique doit être délivrée par le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire.

## 2. L'adaptation des prérogatives des douanes et des douanes judiciaires

### *2. 1. L'extension du champ de compétences des officiers de douane judiciaire*

Dans le but de renforcer la coordination et la complémentarité de l'action de l'ensemble des forces de police, de gendarmerie et de douanes, l'article 28-1 du code de procédure pénale a été modifié.

Ce texte prévoit désormais que le procureur de la République ou le juge d'instruction territorialement compétent peut constituer des unités temporaires composées d'officiers de police judiciaire et d'officiers de douane judiciaire (ODJ) pour la recherche et la constatation des infractions suivantes :

- blanchiment en lien avec une entreprise terroriste (6° de l'article 421-1 du code pénal) ;
- financement d'entreprise terroriste (article 421-2-2 du code pénal).

Ces unités temporaires agissent sous la direction du procureur de la République ou du juge d'instruction mandant, conformément aux dispositions du code de procédure pénale. Elles ont compétence sur toute l'étendue du territoire national.

Dès lors, dans ce cadre, l'action du service national de la douane judiciaire (SNDJ) doit permettre de renforcer le volet financier des enquêtes portant sur les infractions en matière de terrorisme.

3 Cass. Crim., 8 juillet 2015, n° 14-88457

Pour mémoire, la constitution de telles unités est déjà possible en matière de trafic de produits stupéfiants (articles 222-34 à 222-40 du code pénal).

### *2.2. L'allègement de la charge de la preuve en matière de blanchiment douanier*

En vue d'assurer une plus grande efficacité de l'action de l'administration des douanes et de la répression pénale, il a été introduit dans le code des douanes un article 415-1 s'inspirant des dispositions de l'article 324-1-1 du code pénal.

Cet article prévoit en effet *que « les fonds sont présumés être le produit direct ou indirect d'un délit prévu au présent code ou d'une infraction à la législation sur les substances ou plantes vénéneuses classées comme stupéfiants lorsque les conditions matérielles, juridiques ou financières de l'opération d'exportation, d'importation, de transfert ou de compensation ne paraissent obéir à d'autre motif que de dissimuler que les fonds ont une telle origine. »*

Ce dispositif s'applique à la recherche du délit prévu à l'article 415, quel que soit le service concerné (douane judiciaire ou douane administrative). De plus, la présomption d'illicéité de l'origine des fonds n'est pas irréfragable : la personne peut apporter la preuve contraire par tout moyen**.**

**L'intérêt d'une telle présomption est de surmonter la difficulté, dans certaines hypothèses de transfert de fonds entre la France et l'étranger, d'établir que des fonds, dont l'origine illicite est suspectée, proviennent d'un délit douanier ou d'une infraction à la législation sur les stupéfiants.** A cette fin, ce dispositif opère un allègement de la charge de la preuve de l'origine des fonds sans modifier les éléments constitutifs de l'infraction de blanchiment douanier. Dès lors, il devra toujours être démontré l'élément intentionnel ainsi que l'existence d'une opération financière entre la France et l'étranger**.**

Par ailleurs, la mise en œuvre de cette présomption implique que les conditions de fait ou de droit de l'opération de transfert financier ne peuvent avoir d'autres objectifs que de dissimuler l'origine illicite des fonds, telle que prévue par l'article 415 du code des douanes. Autrement dit, sous réserve de l'interprétation que retiendra la jurisprudence, si les éléments rapportés doivent mettre en lumière que les mécanismes de dissimulation mis en œuvre au cours de l'opération financière visent à masquer l'origine illicite des fonds, ils doivent également permettre de retenir ou de raisonnablement supposer la nature spécifique de l'infraction d'origine : infraction à la législation sur les stupéfiants ou au code des douanes.

Le mécanisme de présomption de l'origine illicite des fonds ne peut en aucun cas servir à relever et poursuivre l'infraction d'origine, dont les fonds seraient tirés. Par exemple, la contrebande de produits stupéfiants visée à l'article 414 du code des douanes ne pourra pas être poursuivie sur la base du dispositif de présomption instauré à l'article 415-1 du même code en l'absence de preuve permettant la caractérisation du délit.

### *2.3. L'introduction de techniques spéciales d'enquête en matière de lutte contre le trafic d'armes*

L'article 27 de la loi a pour objet de modifier les articles 67 bis et 67 bis-1 du code des douanes permettant aux agents des douanes de disposer de deux techniques spéciales d'enquête supplémentaires afin de constater les infractions relatives au trafic d'armes ou d'explosifs : l'infiltration et le coup d'achat.

#### 2.3.1. L'élargissement du champ de l'infiltration (article 67 bis du code des douanes)

Comme en procédure pénale, l'infiltration en procédure douanière est une technique d'enquête permettant à un agent des douanes spécialement habilité de surveiller des personnes suspectées de commettre un délit douanier en se faisant passer, sous couvert d'une identité d'emprunt, pour l'un de leurs coauteurs, complices ou intéressés à la fraude. Cette opération, qui se déroule sous le contrôle du procureur de la République, vise à constater des infractions douanières, identifier les auteurs ou complices de ces infractions ainsi que les individus qui y sont intéressés, et à effectuer les saisies prévues au code des douanes.

Si les caractéristiques de l'infiltration douanière sont alignées sur celle de l'infiltration pénale, son champ d'application matérielle diffère. En effet, déjà autorisée pour lutter contre le trafic illicite de produits stupéfiants, de tabac manufacturé, d'alcool, de marchandises contrefaisantes, ainsi que pour constater des faits de blanchiment douanier, **cette technique est désormais ouverte à la recherche des flux de contrebande et d'importation/exportation sans déclaration d'armes ou d'éléments d'armes, de munitions et d'explosifs**.

La circonstance aggravante de bande organisée n'est pas une condition de mise en œuvre d'une infiltration par les agents des douanes.

Par ailleurs, bien que le texte ne le précise pas, la spécificité de cette procédure ainsi que sa complexité opérationnelle rendent préférable que les opérations d'infiltration ne soient principalement autorisées que par le magistrat du parquet de la juridiction interrégionale spécialisée (JIRS). Le procureur de la République local qui se verrait transmettre une telle demande, devra la porter à la connaissance du parquet de la JIRS qui appréciera, selon les circonstances de l'espèce, l'opportunité de s'en saisir.

2.3.2. L'élargissement du champ du coup d'achat (article 67 bis-1 du code des douanes)

Le coup d'achat est une technique d'enquête prévue à l'article 67 *bis*-1 du code des douanes dont les objectifs sont de constater des infractions de détention illicite, d'importation ou d'exportation de marchandises prohibées, d'en identifier les auteurs et complices ainsi que ceux qui y ont participé comme intéressés et d'effectuer les saisies prévues au code des douanes.

Comme pour le coup d'achat en procédure pénale cette technique permet aux agents des douanes spécialement habilités, après autorisation du procureur de la République territorialement compétent :

- d'acquérir des marchandises prohibées ;
- en vue de cette acquisition, à fournir des moyens juridiques, financiers ou logistiques à des personnes se livrant à des infractions données.

En aucun cas, les actes des enquêteurs ne doivent inciter à la commission d'infraction.

Par ailleurs, le 3° de l'article 67 bis-1 prévoit explicitement le cas où l'infraction est commise à l'aide d'un moyen de communication électronique. Cette disposition permet notamment de diligenter des coups d'achat sur le *darknet* en ayant recours à une identité d'emprunt.

Le champ matériel des marchandises prohibées pouvant donner lieu à la mise en œuvre de cette procédure était limité aux produits stupéfiants, aux marchandises contrefaisantes et au tabac manufacturé. **Désormais, ce champ est élargi aux armes, à leurs éléments, aux munitions et aux explosifs.**

La circonstance aggravante de bande organisée n'est pas une condition de mise en œuvre d'un coup d'achat par les agents des douanes.

Cette technique ne peut être envisagée que dans le cadre d'opérations très ponctuelles. En revanche, le recours à l'infiltration doit être privilégié lorsque les opérations s'inscrivent dans la durée et se caractérisent par une pénétration de la structure criminelle.

La procédure du coup d'achat vient compléter et s'articuler avec le dispositif douanier applicable en matière de trafic d'armes :

- en amont, l'article 67 bis-1 A du code des douanes, dont la mise en œuvre est détaillée au paragraphe suivant, qui prévoit la possibilité pour des agents des douanes spécialement habilités d'enquêter sous pseudonyme afin notamment d'identifier les individus impliqués dans un trafic d'armes et de rassembler des preuves à leur encontre ;
- en aval, les dispositions de l'article 64 du code des douanes qui permettent de procéder à la visite de tout lieu, y compris un domicile privé, en flagrance ou sur ordonnance du juge des libertés et de la détention, afin de rechercher des délits douaniers et de procéder à la saisie des marchandises prohibées ou des biens et avoirs provenant directement ou indirectement des délits recherchés.

De plus, la procédure de livraison surveillée, prévue au I de l'article 67 bis du code des douanes, est également applicable, après information du procureur de la République, pour tout délit douanier puni de deux ans d'emprisonnement au moins et notamment en matière de trafics d'armes. Ce dispositif consiste notamment à suivre des marchandises prohibées jusqu'à leur destination, en retardant l'interpellation des intermédiaires et la saisie des marchandises afin d'appréhender autant que possible les véritables commanditaires du trafic.

Il importe de préciser que les coups d'achat diligentés par la douane en matière de trafic d'armes peuvent intéresser directement le parquet au travers des développements judiciaires potentiels de la procédure douanière initiale.

### *2.4. La création d'une cyberpatrouille en matière douanière*

L'article 67 *bis*-1 A nouveau du code des douanes prévoit que des agents des douanes habilités peuvent diligenter des enquêtes sous pseudonyme sur internet, ou « *cyberpatrouilles* ».[4]

Un tel dispositif est déjà applicable aux officiers de police judiciaire ou agents de police judiciaire pour des infractions limitativement énumérées : criminalité organisée (article 706-87-1 du code de procédure pénale), traite d'être humain, proxénétisme et recours à la prostitution d'un mineur ou d'une personne vulnérable (article 706-35-1 du code de procédure pénale), infractions aux produits de santé (article 706-2-2 du code de procédure pénale) et mise en péril des mineurs (article 706-47-3 du code de procédure pénale).

Il est désormais étendu aux agents des douanes habilités[5] mettant en œuvre les pouvoirs prévus par le code des douanes.

Cette cyberpatrouille est autorisée uniquement pour les délits suivants lorsqu'ils sont commis par un moyen de communication électronique :

- contrebande de marchandises prohibées ou fortement taxées (article 414 du code des douanes) ;
- blanchiment douanier (article 415 du code des douanes) ;
- non respect des règles en matière de relations financières avec l'étranger (article 459 du code des douanes).

La cyberpatrouille vise ainsi à constater ces infractions, à en rassembler les preuves et en rechercher les auteurs, les complices ainsi que ceux qui y ont participé comme intéressés.

Pour atteindre cet objectif, les agents habilités, après information du procureur de la République et sauf opposition de ce magistrat, peuvent procéder aux actes suivants sans être pénalement responsables :

- participer sous un pseudonyme aux échanges électroniques ;
- être en contact, par voie d'échanges électroniques, avec les personnes susceptibles d'être les auteurs, les complices ou les intéressés à la fraude de ces infractions ;
- extraire, acquérir ou conserver par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs, les complices ou les intéressés à la fraude de ces infractions.

Si les nécessités de l'enquête douanière l'exigent, les agents des douanes habilités peuvent faire usage d'une identité d'emprunt. La révélation de l'identité de ces agents est pénalement réprimée[6].

A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions.

### *2.5. La rémunération des informateurs des douanes judiciaires*

L'article 15-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité a été modifié afin de prévoir que les agents des douanes habilités à effectuer des enquêtes judiciaires puissent désormais, comme les services de police et de gendarmerie, rétribuer leurs informateurs, définis comme *« toute personne étrangère aux administrations publiques qui leur a fourni des renseignements ayant amené directement soit la découverte de crimes ou de délits, soit l'identification des auteurs de crimes ou de délits. »*

4 Ce dispositif est à distinguer de celui des *« coups d'achat »* de l'article 67 bis-1 du code des douanes, qui prévoit également la possibilité de participer sous pseudonyme à des échanges avec des personnes susceptibles d'être les auteurs des infractions mais uniquement en vue de l'acquisition des marchandises prohibées.

5 Selon les conditions prévues dans le décret n°2004-976 du 15 septembre 2004 fixant les conditions d'habilitation des agents des douanes visés aux articles 67 bis à 67 bis-2 du code des douanes.

6 V de l'article 67 *bis* du code des douanes

### 3. L'usage des armes par les forces de l'ordre en cas de périple meurtrier

L'article 122-4-1 du code pénal, introduit par la loi du 3 juin, prévoit un nouveau cas d'exonération de responsabilité pénale pour le fonctionnaire de la police nationale, le militaire de la gendarmerie nationale, le militaire déployé dans le cadre du maintien de l'ordre public ou l'agent des douanes qui fait usage de son arme pour interrompre un *« périple meurtrier »*.

Cet article constitue un cas particulier d'autorisation de la loi[7] visant à permettre à un agent des forces de l'ordre de mettre hors d'état de nuire une personne armée venant de commettre un ou plusieurs meurtres ou tentatives de meurtre et dont on peut légitimement supposer qu'il se prépare à en commettre d'autres, alors même qu'elle ne constituerait pas une menace actuelle – susceptible de caractériser la légitime défense – au moment précis où ledit agent est en capacité d'intervenir.

Au regard de la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de cassation, qui se réfèrent à la notion d'*« absolue nécessité »*, les forces de l'ordre de l'ordre ne sauraient s'affranchir, pour user de leurs armes, d'une riposte proportionnée à l'atteinte dont elles-mêmes ou autrui pourraient être victimes.

L'usage de l'arme doit donc être absolument nécessaire et strictement proportionné, et doit intervenir dans le but exclusif d'empêcher la réitération, dans un temps rapproché, d'un ou plusieurs meurtres ou tentatives de meurtre venant d'être commis.

L'agent des forces de l'ordre doit avoir eu des raisons réelles et objectives d'estimer que cette réitération était probable au regard des informations dont il disposait au moment où il a fait usage de son arme.

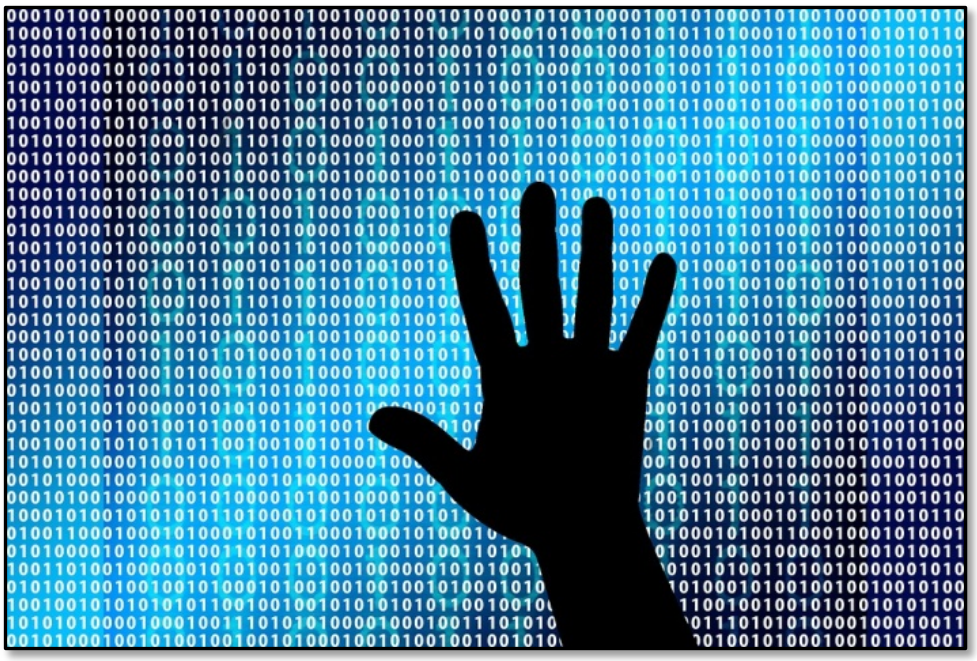
*Le directeur des affaires criminelles et des grâces,*

**Robert GELLI**

7 Article 122-4 du code de procédure pénale

# LE RECUEIL DE LA PREUVE NUMERIQUE

## Enjeux et Perspectives



# Introduction aux données numériques

**La conservation et la préservation des données numériques :**

L'obligation générale de conservation d'un an des données numériques à la charge des opérateurs de communications électroniques et des hébergeurs prévue par l'article L34-1 du code des postes et des communications électroniques (CPCE) porte « *exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux* ».

A l'inverse, l'article L 34-1 VI du CPCE exclut de l'obligation de conservation d'un an de « *certaines catégories de données techniques »,* précisées par décret, *« le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications* ».

Toutefois, les articles 60-2 alinéa 2 du CPP (flagrance), 77-1-2 alinéa 2 du CPP (préliminaire), et 99-4 alinéa 2 du CPP (instruction), prévoient la préservation, sur autorisation du Juge des libertés et de la détention ou du juge d'instruction, pour une durée maximum d'un an, du « *contenu des informations consultées par les personnes utilisatrices des services fournies par les opérateurs* ».

Ces articles ne visent donc pas « *le contenu des correspondances échangées* ».
Le nouveau régime légal de recueil des correspondances numériques stockées (*voir infra*) doit permettre d'obtenir directement le contenu de ces dernières sans qu'il soit nécessaire de les préserver en amont.

Pour autant, les pays signataires de la convention dite de Budapest du Conseil de l'Europe doivent permettre « *la conservation*[1] *rapide de données informatiques de données stockées* » (article 29 de ladite convention). Les Etats-Unis et le Canada ont ratifié cet instrument international. Sur ce fondement, il peut être demandé de « geler » des données situées à l'étranger, même si elles concernent des correspondances afin d'éviter un effacement de la part de l'utilisateur (exemple : conversations sur Facebook).

Plus largement et concernant la conservation des données numériques, la situation est loin d'être homogène au sein de l'Union européenne, ce qui est susceptible de limiter l'efficacité de l'entraide pénale[2].

Il convient de rappeler que la Cour de justice de l'Union européenne (CJUE) a annulé la directive 2006/24 du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, par un arrêt du 8 avril 2014, au motif qu'elle « *[…] couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ou exception soient opérées en fonction de l'objectif de lutte contre les infractions graves. […] Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans*

[1] Le terme « conservation » correspond ici davantage à un mécanisme de « préservation » au sens du droit interne.
[2] Même si des perspectives intéressantes pourraient se concrétiser avec la transposition de la directive européenne sur l'acte européen d'enquête («European Investigation Order »), par exemple pour l'identification d'une personne détentrice d'une adresse IP.

*l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire* ».

A ce jour, aucun projet de nouvelle directive « conservation de données » n'est en cours.

**Une typologie des données numériques en construction :**

La convention dite de Budapest distingue trois catégories de données : celles « *relatives aux abonnées* » (comme les informations données par l'utilisateur à l'ouverture d'un compte), celles de « *trafic* » et celles de « *contenu* ».

Cette nomenclature internationale n'est pas exactement reprise en droit interne, même si la volonté d'accorder un régime plus protecteur à certaines données est également présente, comme l'illustre le régime des correspondances en droit français.

Ainsi, le Conseil constitutionnel a indiqué dans sa décision n°2015-713 DC du 23 juillet 2015 que la notion de « *données de connexion* », telle qu'elle figure à l'article L. 851-1 du code de la sécurité intérieure, « *ne peut être entendue comme comprenant le contenu de correspondances ou les informations consultées* »[3].

Une typologie des données semble ainsi s'établir par une scission nette entre le « *contenant* » et le « *contenu* », ce qui est explicitement formulé dans la délibération n°1/2016 du 14 janvier 2016 de la Commission nationale de contrôle des techniques de renseignement (CNCTR) : « *les données de connexion, par opposition au contenu de correspondances échangées ou d'informations consultées, désignent le «* contenant *», c'est-à-dire les données permettant l'acheminement d'une communication électronique.* »

La CNCTR se livre à un examen poussé de la typologie des données de connexion, en référence à des normes techniques internationales.

En réalité, la frontière entre « contenant » et « contenu » est parfois délicate, comme le démontre l'appréciation de la CNIL relative à la nature des adresses « URL » (communément appelées « adresse internet ») dans sa délibération n° 2015-455 du 17 décembre 2015, qu'elle considère comme « *nécessaire[s] à l'acheminement d'une communication* » tout en étant « *porteuse[s] par nature des informations consultées* ».

Le recours à l'IMSI Catcher fait l'objet d'une « *f*iche technique DACG» distincte et ne sera pas traité dans le présent document. Cette technique de recueil des données de connexion sera toutefois intégrée dans le tableau synthétique en annexe 1.

Enfin, le régime juridique des données numériques se croise partiellement avec celui des données personnelles. Un arrêt récent de la CJUE concernant la nature de l'adresse IP en est l'illustration[4].

[3] Considérant n°55.

[4] CJUE affaire C-582/14, 19 octobre 2016 : la conservation de données à caractère personnel, telles que notamment l'adresse de protocole Internet dynamique d'un visiteur (adresse IP), par un site Internet est licite, par exception, dans la mesure où il est nécessaire à la réalisation de l'intérêt légitime poursuivi, en l'occurrence le bon fonctionnement d'un site Internet.

# Les régimes juridiques du recueil de la preuve numérique[5]

## 1. Le régime de la perquisition « informatique »

### Cadre légal

Dans le cadre de la perquisition, certaines dispositions concernent spécifiquement les « données informatiques ».

Ainsi l'article 56 alinéa 2 du CPP autorise la prise de connaissance par l'OPJ des données informatiques avant de procéder à leur saisie[6].

De même, la saisie des données informatiques peut se faire soit en plaçant sous main de justice le support physique de ces données (par exemple : ordinateur, tablette, téléphone, disque dur, clés USB…), soit en réalisant une copie en présence des personnes qui assistent à la perquisition (art 56 alinéa 5 CPP). Dans cette dernière hypothèse, le procureur (ou le juge d'instruction) peut ordonner l'effacement définitif des données sur le support physique qui n'a pas été placé sous main de justice (art 56 alinéa 6 CPP).

Mais surtout, l'article 57-1 du CPP dispose que « *les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, au cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.*

*Ils peuvent également, dans les conditions de perquisition prévues au présent code, accéder par un système informatique implanté dans les locaux d'un service ou d'une unité de police ou de gendarmerie à des données intéressant l'enquête en cours et stockées dans un autre système informatique, si ces données sont accessibles à partir du système initial.*

*S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur.* »

### Mise en oeuvre

La difficulté principale se pose en pratique dans le cas de données stockées dans un autre système informatique, si ces données sont accessibles pour le système initial (par exemple : si l'ordinateur est connecté à un compte de réseau social type Facebook, Twitter…).

[5] Hors entraide pénale internationale.

[6] Cette prise de connaissance doit cependant en pratique se faire avec précaution afin de ne pas altérer lesdites données.

Il ressort de l'article 57-1 CPP que lors d'une perquisition, si le matériel informatique permet une connexion à un service distant (par exemple un stockage type *Cloud*), les enquêteurs peuvent en principe y accéder.

De même, s'ils ont en leur possession les identifiants et mots de passe, ils pourront obtenir les informations en se connectant depuis un système informatique installé dans leur service d'enquête (57-1 alinéa 2).

Dans l'hypothèse où des données saisies seraient des correspondances numériques (boîte mail), il ne semble pas qu'il soit obligatoire de recourir au nouveau régime de la loi du 3 juin 2016, visant le recueil des correspondances numériques stockées, puisque les garanties inhérentes à la perquisition sont déjà présentes.

S'il est préalablement avéré que les données sont stockées en dehors du territoire national, renvoi est fait aux engagements internationaux en vigueur, en l'espèce l'article 32 de la convention de Budapest.

L'application de l'article 32 de la convention de Budapest conduit à recueillir l'assentiment de la personne concernée par les données. En effet, l'expression « *consentement légal et volontaire de la personne légalement autorisée à divulguer ces données* » ne saurait concerner le prestataire privé « simple gardien » des données[7].Afin de contourner cette difficulté, et seulement dans l'hypothèse où les données à saisir seraient des correspondances numériques stockées à l'étranger, et sous réserve de remplir les conditions légales, il pourrait être tenté de recourir au nouveau régime issu de la loi du 3 juin 2016 (706-95-1 et 706-95-2 CPP, *voir infra*) qui permet justement de se passer du consentement de la personne (« *à l'insu de la personne visée* ») lors d'un accès « à distance ».

Cependant, il n'apparaît pas que les enquêteurs soient légalement obligés de vérifier systématiquement si les données sont stockées à l'étranger. En cas de doute légitime, le 3ème alinéa de l'article 57-1 du CPP ne semble pas pouvoir être opposé.

Concernant la problématique de l'accès au contenu stocké dans un terminal verrouillé et placé sous scellé à l'issue de la perquisition, il sera renvoyé à la « *fiche technique DACG : le recours au Centre technique d'assistance (CTA)* ».

## 2. Le régime de la réquisition

### Cadre légal

Les articles 60-1 du CPP (flagrance), 77-1-1 du CPP (préliminaire) et 99-3 du CPP (instruction) permettent au juge d'instruction, au procureur de la République ou à l'officier de police judiciaire,

[7] « *Il est peu probable que les prestataires de services remplissent les conditions d'un consentement valide et volontaire concernant la divulgation des données de leurs utilisateurs dans les conditions de l'article 32. En général, les prestataires de services ne sont que les dépositaires de ces données. Ils n'en ont pas le contrôle ni la propriété et ne sont donc pas dans la capacité de donner un consentement valide.* » (note d'orientation n°3 du comité T-CY relative à l'article 32)

par tout moyen, de « *requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel. […]*».

Au-delà des possibilités de réquisition, l'article 60-2 alinéa 1 du CPP prévoit la possibilité d'une « mise à disposition » de ces informations suite à une demande d'un OPJ « *intervenant par voie télématique ou informatique* ». Cette souplesse est toutefois conditionnée à la mise en place de protocoles avec les organismes visées (opérateur de communication électronique, établissement bancaires…). Cette « mise à disposition » a vocation à se développer dans les prochaines années.

## Mise en oeuvre

A titre liminaire, il sera remarqué que ces textes ne distinguent ni les catégories de données numériques, de type « contenu » ou « contenant », ni leur localisation.

La Cour de cassation a donc posé certaines limites.

Ainsi, l'arrêt « Ciprelli » du 6 novembre 2013 (12-87.130) indique, à la lumière de la convention de Budapest, que « les juges ont fait une exacte application de l'article 77-1-1 du code de procédure pénale et du texte conventionnel invoqué, dès lors que la remise de documents au sens du premier de ces textes s'entend également de la communication, sans recours à un moyen coercitif, de documents issus d'un système informatique ou d'un traitement de données nominatives, tels ceux détenus par le gestionnaire d'un système de messagerie électronique, hors, comme en l'espèce, le contenu des correspondances échangées, et que l'ingérence ainsi apportée dans l'exercice du droit au respect de la vie privée et familiale n'excède pas ce qui est nécessaire, dans une société démocratique, à la recherche et à la poursuite des infractions. »

Ainsi, lorsque les données sont stockées à l'étranger, les réquisitions sur le fondement des articles 60-1 du CPP, 77-1-1 du CPP et 99-3 du CPP correspondent à une demande de remise de données, sans caractère contraignant, et en dehors des données de contenu des correspondances.

En effet, si les données sont stockées à l'étranger, il est probable qu'une demande d'entraide pénale soit rapidement nécessaire pour prévenir les difficultés liées à un conflit de lois.

Dans ce cadre, il convient de préciser que la loi américaine interdit à un prestataire américain de délivrer à une autorité étrangère des données de contenu (et donc les correspondances) en dehors de l'entraide pénale internationale, sauf en cas d'urgence vitale (enlèvement, risque d'attentat imminent).

L'introduction d'un nouveau régime pour les correspondances (*cf infra*) exclut désormais d'user des réquisitions afin d'obtenir des correspondances, même si elles sont stockées en France.

S'agissant de données autres que de contenu, une plus grande souplesse de la part des opérateurs privés est constatée.

## 3. Le nouveau régime des correspondances numériques

### ➔ L'interception des correspondances numériques <u>futures</u>

### Cadre légal

Article 100 du CPP (instruction) : « En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques. »

Article 706-95 du CPP (parquet) : « Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques selon les modalités prévues par les articles 100, deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée. »

### Mise en oeuvre

Il s'agit en effet du même régime que les écoutes téléphoniques traditionnelles, puisque la Cour de Cassation valide désormais l'utilisation de l'article 100 du CPP (et donc des dispositions de l'article 706-95 du CPP) pour intercepter des courriels[8].

Si les enquêteurs obtiennent les identifiants et mots de passe d'une boîte mail, ces bases juridiques peuvent être utilisées pour l'interception de courriels futurs. Pour conserver une certaine furtivité, il conviendrait de contacter le prestataire privé pour lui demander, si possible, de ne pas alerter l'utilisateur d'une connexion à son compte par un système informatique étranger.

Au demeurant, en l'absence du mot de passe, certains opérateurs privés sont en théorie en capacité d'initialiser un nouveau mot de passe, mais au risque d'alerter l'utilisateur de la messagerie dont le propre mot de passe ne serait plus fonctionnel.

La mise en œuvre pratique de cette technique d'enquête nécessite une certaine imagination (voire une ingénierie sociale) et les difficultés rencontrées devront être signalées immédiatement à la Direction des affaires criminelles et des grâces pour analyse.

Concernant la question de l'interception des services de messagerie instantanée, la Cour de Cassation[9] précise que « *les messages instantanés échangés entre plusieurs personnes au moyen*

[8] Arrêt 14-88.457 du 8 juillet 2015 : dans un attendu de principe a contrario : « n'entrent pas dans les prévisions de ces textes [art. 100 et s cpp] l'appréhension, l'enregistrement et la transcription de correspondances émises ou reçues par la voie des télécommunications antérieurement à la date de la décision écrite d'interception prise par le juge d'instruction, lesquels doivent être réalisés conformément aux dispositions légales relatives aux perquisitions ». Il s'agissait en l'occurrence de la copie du contenu d'une boîte mail.

[9] Notamment Cass. Crim. 16 déc. 2015, 15-82.643, dans une espèce où le service BlackBerry Messenger (BBM) avait été intercepté sur commission rogatoire d'un juge d'instruction grâce à la collaboration de la société BlackBerry.

*d'une liaison sécurisée par un dispositif de cryptage (sic) constituent des correspondances par la voie des télécommunications au sens de l'article 100 du code de procédure pénale et sont, comme telles, susceptibles d'être appréhendées sur la décision et sous l'autorité et le contrôle d'un juge* ».

Cet attendu de principe peut être transposé à tous les services de messagerie instantanée comme Imessage, Whatsapp, Viber, Messenger. Toutefois, ces interceptions réalisées sur la base des articles 100 et 706-95 du code de procédure pénale sont dépendantes de la bonne volonté des sociétés privés en question (à notre connaissance, seule la société BlackBerry a pu accepter de collaborer dans ce cadre) et la mise en œuvre pratique se heurte en réalité au chiffrement de bout en bout de ces communications[10].

### ➔ Le recueil des correspondances numériques stockées

## Cadre légal

Afin de répondre aux exigences jurisprudentielles tirées de par l'arrêt de la cour de cassation du 8 juillet 2015, la loi 3 juin 2016 consacre le principe de l'accès furtif à des correspondances numériques stockées, c'est-à-dire antérieures à la décision d'interception du juge.

Ainsi l'article 706-95-1 du CPP (parquet) précise-t-il : « Si les nécessités de l'enquête relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention peut, à la requête du procureur de la République, autoriser par ordonnance motivée l'accès, à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique. Les données auxquelles il a été permis d'accéder peuvent être saisies et enregistrées ou copiées sur tout support. »

De même, l'article 706-95-2 du CPP (instruction) dispose que: « Si les nécessités de l'information relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge d'instruction peut autoriser par ordonnance motivée l'accès, à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique. Les données auxquelles il a été permis d'accéder peuvent être saisies et enregistrées ou copiées sur tout support. »

## Mise en œuvre

Les mêmes réserves formulées pour la mise en œuvre des interceptions de correspondances numériques futures sont applicables au recueil des correspondances numériques stockées.

Une difficulté supplémentaire est la mise en place dans certains services de messageries d'une fonction de suppression automatique des messages après une période de temps prédéterminée (de quelques secondes à 24 heures). Comme exposé en introduction, il n'existe à l'heure actuelle aucune obligation légale pour les opérateurs de conserver les correspondances et aucune possibilité d'ordonner judiciairement leur préservation sur la base de l'article 60-2 du CPP, dès lors qu'il ne s'agit pas « *d'informations consultées* ».

[10] Voir les développements relatifs à la « captation de données informatiques », *infra*.

Toutefois, l'article 706-95-3 du CPP permet la réquisition de tout « *agent qualifié d'un service ou d'un organisme placé sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de communications électroniques* » pour la mise en œuvre des articles 706-95-1 et 706-95-2 du CPP.

Cette disposition est l'équivalent de l'article 100-3 du CPP pour les interceptions de correspondances numériques futures (et les écoutes traditionnelles classiques), mais dans ce cas de figure, il pourrait être utile de tenter de requérir la préservation des correspondances afin d'éviter un effacement par l'utilisateur, si les données en question sont dupliquées ou conservées dans les serveurs de l'opérateur.

Une réquisition devrait également en théorie permettre d'imposer à l'opérateur de préserver, si possible, le caractère furtif de la technique d'enquête en bloquant les messages de notification à titre de sécurité.

Une difficulté grandissante est que la plupart des sociétés de messagerie électronique ne se considèrent pas comme des « fournisseurs de services de communications ». Un débat est en cours au niveau de l'Union européenne sur un nouveau cadre règlementaire concernant ces nouveaux acteurs, communément appelés « Over The Top »[11].

***Remarques sur le champ infractionnel de ces textes***

***Par le biais de l'article 706-1-1 du CPP, de nombreuses infractions financières bénéficient de ces techniques d'enquêtes, au-delà de l'article 706-73-1 CPP.***

***D'autre part, dans le cadre d'informations judiciaires, ce nouveau régime crée une asymétrie notable entre le champ infractionnel du recueil correspondances antérieures (« stockées ») et celui des correspondances futures. Concrètement, dans une affaire de meurtre simple ou de viol, le juge d'instruction pourra faire intercepter les correspondances futures mais pas les correspondances antérieures, ces dernières étant réservées au régime dérogatoire 706-95-2 du CPP.***

## 4. Le régime de la captation de données informatiques

### Cadre légal

Les articles 706-102-1 du CPP (parquet sur autorisation du juge des libertés et de la détention) et 706-102-2 du CPP (instruction) autorisent la mise en place d'« *un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de*

[11] Une société « OTT-1 » est une société qui n'est pas légalement un fournisseur de services de communication mais qui potentiellement offre des services comparables aux consommateurs.

*traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels.*

Le procureur de la République et le juge d'instruction peuvent désigner toute personne physique ou morale habilitée et inscrite sur l'une des listes prévues à l'article 157 du CPP, en vue d'effectuer les opérations techniques permettant la réalisation du dispositif technique mentionné au premier alinéa du présent article.

Le procureur de la République ou le juge d'instruction peut également prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au chapitre Ier du titre IV du livre Ier.

### Mise en œuvre

Ce mécanisme est assimilable à un logiciel dit « espion » qui prend partiellement le contrôle du terminal informatique visé, afin d'en extraire certaines données de façon furtive. Cette solution a notamment l'avantage de contourner le chiffrement des communications.

La loi du 3 juin 2016 a étendu la catégorie des données récupérables aux données stockées dans un système informatique, ce qui permet en théorie de rechercher à distance dans le disque dur du terminal ciblé des informations utiles pour la manifestation de la vérité.

L'injection du dispositif peut se faire à distance, ou par contact physique avec le terminal. Dans ce dernier cas, les mêmes garanties que celles prévues dans le cadre de l'installation d'un micro-espion s'appliquent, à savoir notamment l'autorisation supplémentaire du juge des libertés et de la détention pour accéder à un lieu d'habitation en dehors des heures légales.

Le ministère de la justice œuvre activement afin de permettre aux magistrats prescripteurs de bénéficier dans un délai raisonnable de cette technique spéciale d'enquête très prometteuse mais devant être réservée, dans un premier temps, à des dossiers prioritaires comme la lutte contre le terrorisme.

## Le support de la preuve numérique

Les nouveaux articles 60-3 du CPP (flagrance), 77-1-3 du CPP (préliminaire) et 99-5 du CPP (instruction) issus de la loi du 3 juin 2016 permettent « lorsqu'ont été placés sous scellés des objets qui sont le support de données informatiques », au procureur de la République ou à l'officier de police judiciaire (le cas échéant avec l'autorisation expresse du juge d'instruction) , par tout moyen, de « requérir toute personne qualifiée inscrite sur une des listes prévues à l'article 157 ou ayant prêté par écrit le serment prévu à l'article 60 de procéder à l'ouverture des scellés pour réaliser une ou plusieurs copies de ces données, afin de permettre leur exploitation sans porter atteinte à leur intégrité. La personne requise fait mention des opérations effectuées dans un rapport établi conformément aux articles 163 et 166 ».

Cette nouvelle possibilité évite au magistrat de saisir lui-même un expert pour réaliser de simples copies de données d'un scellé judiciaire, et sans la lourdeur procédurale du régime général des expertises.

De façon générale, en matière d'exploitation de données informatiques, les copies de travail sont souvent indispensables.

Il est fortement conseillé d'avoir en toute circonstance un scellé contenant les données présentes sur les copies de travail, afin d'éviter une assimilation automatique de ces copies de travail à l'original de la procédure, qui peut poser des difficultés lors de la transmission du dossier à la chambre de l'instruction et porter atteinte au droit de la défense[12].

De même, sauf autorisation expresse du magistrat, les enquêteurs ne peuvent conserver des copies de travail après la fin de leur mission sur commission rogatoire[13].

## L'exploitation de la preuve numérique : périmètre de l'expertise

La tendance est à simplifier certaines opérations techniques sur les données numériques qui passaient autrefois par une expertise non pas pour permettre une analyse plus aboutie de l'expert mais simplement pour permettre le bris de scellé.

Comme indiqué précédemment, la loi du 3 juin 2016 permet désormais, non seulement la réalisation de copie de travail comme le ferait un expert, mais également au Centre technique d'Assistance de briser les scellés pour les opérations de mise au clair de données chiffrées (voir le Focus DACG dédié).

Ces opérations, proches de la catégorie classique des « simples mesures de recherches et de constatations »[14], sont donc en dehors du champ classique de l'expertise.

Le recours à l'expertise judiciaire devra être privilégié si les données numériques sont potentiellement déterminantes pour le fond du dossier afin d'obtenir le maximum de garanties.

L'on pense bien sûr à la suspicion de documents pédopornographiques, de consultations de sites faisant l'apologie du terrorisme, de documents falsifiés sur ordinateur, d'échange de messages avec la victime ou les complices, à la récupération de données effacées…

La pratique conduit parfois à nommer un « ICC » (Investigateur en cybercriminalité de la police nationale) ou un « NTECH » (gendarmerie nationale) comme expert personne physique devant prêter serment, pour exploiter les supports numériques placés sous scellés en cours de garde à vue, au-delà d'une simple extraction de données. La question de sa partialité pourrait se poser[15].
Par précaution, il conviendra de s'assurer que ce technicien ne travaille pas directement sur le dossier en dehors de son examen technique.

---

[12] Cass Crim. 6 janvier 2015 n°14-86719 ; Cass.Crim. 12 nov. 2015 n°15-85266.
[13] Voir dans le cadre de copies de travail issues d'une sonorisation : Cass. Crim. 8 juillet 2015 n°15-81731.
[14] Cass. Crim. 4 nov. 1987.
[15] A ce sujet, Cass. Crim 13 janv. 2013 relatif à des agents de l'OLAF nommés comme experts informatiques par le juge d'instruction, pratique validée au motif que « *les requérants n'invoquaient pas, pour mettre en cause l'impartialité des experts, dont les constatations sont soumises à discussion, d'autres éléments que leur appartenance à l'OLAF, organisme d'enquête dont l'indépendance, à l'égard de la Commission représentant l'Union européenne, partie civile, est institutionnellement garantie, d'autre part, les juges ont pu déduire des rapports déjà transmis par ledit organisme que les experts ne s'étaient pas fondés sur des éléments d'information ne figurant pas au dossier* .»

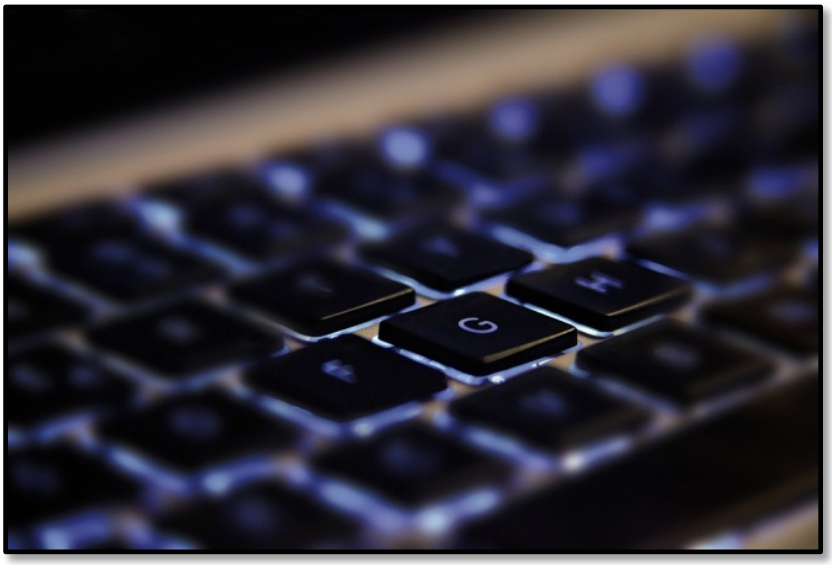
## Les perspectives en matière de preuve numérique

Sans prétendre à l'exhaustivité, trois points méritent d'être mentionnés :

- Le débat sur le chiffrement : sont en cours des réflexions au niveau de l'Union européenne sur le régime règlementaire des nouveaux acteurs Internet (« OTT-1 ») ;

- L'amélioration de l'accès transfrontalier aux preuves numérique : à la fois par une optimisation des procédures actuelles, et par les réflexions menées au sein du Conseil de l'Europe ou encore la perspective de traités bilatéraux ;

- Le nouveau prérequis de la localisation des données, préalable à toute demande d'entraide pénale à destinations des Etats-Unis (conséquence de l'arrêt Microsoft du 14 juillet 2016, voir le Guide pratique « *Obtention des données électroniques aux Etats-Unis* », actualisé par le BEPI de la DACG).



*

## *Annexe 1: tableau synthétique du recueil de la preuve numérique*

| | MESURES | Articles du code de procédure pénale | Recueil de données « stockées » | Interception Flux actif de données |
|---|---|---|---|---|
| **Droit commun** | **Réquisitions aux fins d'obtenir (exemples):**<br>les facturations détaillées des communications<br>la localisation d'un téléphone (a posteriori)<br>les données stockées sur un cloud<br>les données publiées via des réseaux sociaux<br>les données de connexion en général<br>**(si données à l'étranger, limite aux données autres que de contenu et absence de caractère contraignant ; en aucun cas pour les correspondances même en France)** | Articles 60-1, 60-2 (flagrance)<br>Articles 77-1-1, 77-1-2 (préliminaire)<br>Articles 99-3, 99-4 (instruction) | X | |
| | **Perquisition « informatique » (si données à l'étranger, besoin du consentement)** | Article 57-1 (flagrance) ; Article 76-3 (préliminaire) ; Article 97-1 (instruction) | X | |
| | **Désignation d'une personne qualifiée pour mise au clair des données chiffrées (dont CTA)** | Article 230-1<br>(flagrance, préliminaire, instruction) | X | |
| | **Localisation en temps réel d'un terminal** | Articles 230-32 et suivants | | X |
| | **Interception des correspondances numériques futures** | Article 100 (instruction) | | X |
| **régime dérogatoire**<br><br>(Infractions visées aux articles 706-73 et 706-73-1 du C.P.P., ainsi que celles de 706-1-1 CPP) | **Réquisitions aux fins d'accès aux correspondances stockées** à distance et **à l'insu de la personne** | Article 706-95-1 (préliminaire, flagrance)<br>Article 706-95-2 (instruction) | X | |
| | **Captation des données par logiciel :**<br>Données stockées, s'affichant à l'écran, introduites par saisie de caractères, reçues ou émises par périphériques audiovisuels | Article 706-102-1 (préliminaire, flagrance)<br>Article 706-102-2 (instruction) | X | X |
| | **IMSI Catcher :** Recueil des données de connexion, de localisation et/ou interception des correspondances émises ou reçues | Article 706-95-4 | | X |
| | **Interception des correspondances numériques futures** | Article 706-95 (flagrance ou préliminaire) | | X |

# LA MISE AU CLAIR DES DONNEES CHIFFREES
# (Rôle du Centre Technique d'Assistance)

## Présentation du dispositif

Sous l'impulsion d'une économie numérique nécessitant un haut degré de confiance entre ses utilisateurs, l'emploi de moyens de chiffrement[1] s'est rapidement généralisé dans les matériels et applications destinés au grand public.

Historiquement sujettes à un contrôle strict des autorités gouvernementales, la libéralisation totale de l'usage de ces techniques de chiffrement par la loi LCEN du 21 juin 2004[2] a certes profité à la sécurisation des échanges électroniques, mais l'autorité judiciaire a semblé en partie démunie devant ce changement de paradigme.

---

[1] **Chiffrement** : processus de transformation des informations de façon à les rendre inintelligibles à toute personne autre que le destinataire (le terme « cryptage » est impropre).

- **de type « bout en bout » (« End to End »)** : Les messages envoyés au destinataire sont chiffrés localement avant même d'être envoyés sur le réseau. Le serveur ne fait rien d'autre que relayer le message chiffré puisque le client du destinataire déchiffre le message, la transaction est ainsi sécurisée indépendamment du serveur (exemple : protocole Signal).
- **de type « full disk encryption »** : intégré directement dans les disques durs. Certains smartphones haut de gamme sont dotés de cette technologie (exemple : Iphone).
- **symétrique :** une même clé est utilisée pour chiffrer et déchiffrer. Exemples : méthodes DES, Triple DES et AES.
- **asymétrique :** système basé sur une paire de clés, à savoir une *clé publique*, servant au chiffrement, et d'une *clé privée*, servant à déchiffrer. Le point fondamental soutenant cette décomposition publique/privée est l'impossibilité calculatoire de déduire la clé privée de la clé publique. Exemple : méthode RSA ou PGP.

[2] La fourniture, l'importation et l'exportation sont encore soumis, sauf exception, à déclaration ou à une demande d'autorisation auprès de l'ANSSI (agence nationale de la sécurité des systèmes d'information). Un premier assouplissement avait eu lieu en 1998 pour les systèmes dont la clé ne dépassait pas 128 bits.

Fort de ce constat, et afin de réaliser les opérations de déchiffrement dans le cadre des enquêtes judiciaires, un centre technique d'assistance (CTA), dépendant officiellement de la direction générale de la sécurité intérieure (DGSI), a été créé en application de l'article 230-2 du code de procédure pénale.

Celui-ci, sur saisine des magistrats et des enquêteurs, tente de mettre au clair les données chiffrées ou d'accéder aux données contenues dans un terminal verrouillé.

Peu sollicité jusqu'à présent, les saisines du CTA devraient s'amplifier dans les prochains mois, en raison d'assouplissements juridiques liés aux modalités de saisine et à la gestion des scellés judiciaires, de la montée en puissance des capacités de traitement du CTA lui-même et d'une sensibilisation renouvelée des magistrats prescripteurs.

## Cadre légal

Le recours au CTA est conditionné aux nécessités de l'enquête et à une peine encourue égale ou supérieure à deux ans d'emprisonnement (art 230-1 al 3 CPP). Dans le cas d'une peine inférieure, seul le recours à une personne physique ou morale qualifiée est envisageable (art 230-1 al 1 et 2 CPP).

La loi du 13 novembre 2014 a élargi la saisine du CTA, désormais possible non seulement au procureur de la République et à la juridiction d'instruction, mais également à *« l'officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction* » ou la juridiction de jugement.

La loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale a intégré la possibilité pour le CTA de briser et d'exploiter les scellés judiciaires.

Ainsi l'article 230-2 du code de procédure pénale dispose désormais qu'*« aux fins de réaliser les opérations de mise au clair, l'organisme technique mentionné au premier alinéa du présent article est habilité à procéder à l'ouverture ou à la réouverture des scellés et à confectionner de nouveaux scellés après avoir, le cas échéant, procédé au reconditionnement des supports physiques qu'il était chargé d'examiner. En cas de risque de destruction des données ou du support physique qui les contient, l'autorisation d'altérer le support physique doit être délivrée par le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire.* »

D'autre part, l'articulation entre la PNIJ[3] et le CTA a été clarifiée.

En effet, l'article 88 de ladite loi a modifié également l'article 230-2 afin de prévoir expressément que lorsque l'interception judiciaire est réalisée au moyen de la PNIJ, la réquisition de mise au clair de données chiffrées obtenues dans le cadre de ces interceptions de communications électroniques est transmise directement au centre technique d'assistance (CTA). Cette disposition entrera en vigueur le 1er janvier 2017.

## Doctrine d'emploi

Très fréquent en pratique, le démontage du matériel (smartphone, tablette…) faisant l'objet d'une réquisition au CTA devrait être systématiquement autorisé par le magistrat prescripteur.

[3] Plateforme Nationale des Interceptions Judiciaires.

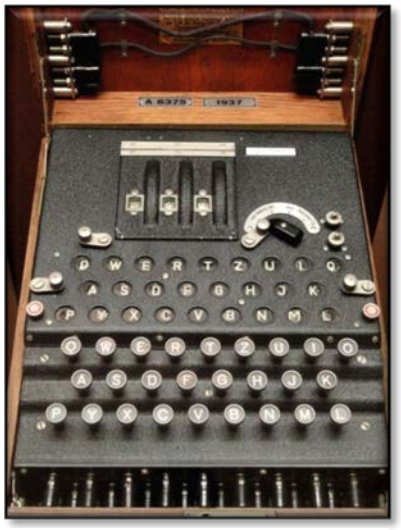
Afin d'améliorer les chances de la mise au clair, le magistrat ou l'enquêteur devra prendre attache avec le CTA, en amont de la saisine, pour déterminer les informations et matériels devant être transmis.

A titre d'exemple, un téléphone portable pouvant être synchronisé[4] avec un ordinateur, le CTA parviendra plus facilement à accéder au contenu du téléphone s'il est transmis avec l'ordinateur.

Concernant le délai à accorder au CTA pour sa mission, il est préconisé de le porter à 6 mois (et non seulement 3 mois comme constaté en pratique). En cas d'urgence à expliciter, le délai pourra être plus court, mais ce point devra être discuté avec le CTA pour une véritable prise en compte, ainsi qu'une complète information du magistrat sur les conséquences d'un délai raccourci dans les opérations de calcul (« force brute » et assimilé).

Enfin, il convient de souligner que **le rapport technique du CTA ne doit pas être assimilé à une expertise**. En conséquence, il est vivement conseiller de confier les données mises au clair placées sous scellés par le CTA à un expert informatique dont le régime juridique est assorti des garanties procédurales indispensables à l'exercice des droits de la défense (notamment la notification des missions de l'ordonnance de commission d'expertise, ainsi que des conclusions du rapport final).

Toutefois, l'IRCGN propose également des prestations de démontage des téléphones pour accéder aux données de terminaux. Le cadre légal est alors celui de l'expertise.



**Machine Enigma, utilisée par l'armée allemande pendant la 2nd guerre mondiale**

[4] Les données présentes sur un terminal sont dupliquées régulièrement sur un second terminal (voire un « nuage de données » type iCloud) avec lequel il est synchronisé.

# Lexique en matière de cryptographie

*

**Algorithme de cryptographie :** également appelé chiffre, il s'agit une fonction mathématique utilisée pour le chiffrement ou le déchiffrement.

**Algorithme de Shor** : algorithme quantique pour factoriser un entier naturel, pouvant théoriquement être utilisé par un calculateur quantique pour casser des cryptosystèmes à clé publique, tels le chiffrement RSA.

**Attaque par force brute** : méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles.

**Attaque « arc en ciel »** : basée sur une structure de données permettant de retrouver un mot de passe à partir de son « empreinte » (issue d'une fonction de hachage).

**Attaque « homme du milieu »** : attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Ce type d'attaque nécessite de sécuriser l'échange de clés.

**Chiffrement** : processus de transformation des informations de façon à les rendre inintelligibles à toute personne autre que le destinataire (le terme « cryptage » est impropre).

- **de type « bout en bout » (« End to End »)** : Les messages envoyés au destinataire sont chiffrés localement avant même d'être envoyés sur le réseau. Le serveur ne fait rien d'autre que relayer le message chiffré puisque le client du destinataire déchiffre le message, la transaction est ainsi sécurisée indépendamment du serveur (exemple : protocole Signal).
- **de type « full disk encryption »** : intégré directement dans les disques durs. Certains smartphones haut de gamme sont dotés de cette technologie (exemple : Iphone).
- **RSA :** algorithme populaire de cryptographie asymétrique (nommé par les initiales de ses trois inventeurs, Rivest, Shamir et Adleman).
- **symétrique :** une même clé est utilisée pour chiffrer et déchiffrer. Exemples : méthodes DES, Triple DES et AES.
- **asymétrique :** système basé sur une paire de clés, à savoir une *clé publique*, servant au chiffrement, et d'une *clé privée*, servant à déchiffrer. Le point fondamental soutenant cette décomposition publique/privée est l'impossibilité calculatoire de déduire la clé privée de la clé publique. Exemple : méthode RSA ou PGP.

**Cryptographie post quantique :** branche de la cryptographie visant à garantir la sécurité même face à un attaquant *quantique* en utilisant les ordinateurs dit *classiques*. Ex : la société Google teste de nouveaux algorithmes dans certaines versions du navigateur Chrome depuis juillet 2016.

**Cryptographie quantique** : branche de la cryptographie visant à utiliser des méthodes *quantiques* pour protéger d'un adversaire *quantique*. Ex : la Chine a lancé mi-aout 2016 un premier satellite de communication quantique.

**Déchiffrement** : processus inverse du chiffrement, il sert à transformer les informations de façon à les rendre à nouveau intelligibles.

**Décryptage** : opération consistant à retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement.

**HTTPS** : L'HyperText Transfer Protocol Secure, plus connu sous l'abréviation HTTPS — littéralement « protocole de transfert hypertexte sécurisé » — est la combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS. HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification, et garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur. Utilisé pour les transactions financières, la consultation des courriers électroniques, et plus récemment par les réseaux sociaux.

**Informatique quantique (calculateurs)**: Les opérations ne sont plus basées sur la manipulation de bits dans un état 1 ou 0, mais de « qubits » *en même temps* dans un état 1 et 0. La mise au point de ces machines, pour le moment largement théoriques, entraîne l'allocation de budgets conséquents de la part de certains Etats (USA, CHINE…).

**PGP (Pretty Good Privacy)**: un des premiers logiciels de chiffrement disponibles sur l'Internet, longtemps été interdit en France, car considéré jusqu'en 1996 comme une arme de guerre de deuxième catégorie. La législation française a d'abord été assouplie (le chiffrement symétrique avec des clés aussi grandes que 128 bits avait été autorisé) puis la loi pour la confiance dans l'économie numérique du 21 juin 2004 a totalement libéré l'utilisation des moyens de cryptologie (en revanche leur importation ou exportation est soumise à déclaration ou autorisation).

**Protocole Signal** : protocole d'application de messageries instantanées et d'appels voix sur IP cryptés (application éponyme Signal), mais dont la technologie est utilisée également par l'application WhatsApp et (en option) par l'application Messenger, toutes deux propriétés de la société Facebook et totalisant plus d'un milliard d'utilisateurs. Libre d'utilisation et développé par Open Whisper Systems.

FICHE TECHNIQUE

# INTERCEPTIONS DE COMMUNICATIONS ELECTRONIQUES
# Dans le cadre d'une enquête dirigée par le parquet

## Définition juridique

**Fondement légal** :

- l'article 706-95 du code de procédure pénale (CPP)
- l'article 74-2 du CPP

Tous deux issus de la loi du 9 mars 2004, ces textes ont été récemment modifiés par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

**Définition** :
La définition des interceptions de correspondances émises par la voie des communications électroniques est identique, quel que soit le cadre d'enquête, que celles-ci soient ordonnées dans le cadre d'une information judiciaire ou dans le cadre d'une enquête menée par le parquet.

L'article 100 du CPP, modifié par la loi du 3 juin 2016, vise « *l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques* ».

Selon l'article 32 du code des postes et communications électroniques (CPCE), les communications électroniques correspondent à « *toute transmission, émission ou réception de signes, signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, optique, radioélectricité ou autres systèmes électromagnétiques* ».
Est donc concernée l'interception des correspondances émises ou reçues sur des différents supports tels que les téléphones fixes ou mobiles, les tablettes ou les ordinateurs.

Les opérations visées aux articles 100 et suivants du CPP sont réalisées grâce à des dispositifs d'interception qui supposent l'intervention de spécialistes des communications électroniques. Toutefois, la jurisprudence y assimile les écoutes effectuées sans l'emploi de procédés particuliers.

**Entrent ainsi dans le champ d'application de l'article 100 du CPP:**

- l'enregistrement puis la transcription par des OPJ de conversations téléphoniques par apposition d'un dispositif relié au combiné de l'appareil avec l'accord d'un des correspondants *(Cass. crim., 27 févr. 1996) ;*
- les messages instantanés échangés entre plusieurs personnes au moyen d'une liaison sécurisée par un dispositif de cryptage de type BLACKBERRY MESSENGER (*Cass. Crim. 16 déc. 2015).*

**En sont en revanche exclus** :

- l'appréhension, l'enregistrement et la transcription de correspondances émises ou reçues par la voie des télécommunications antérieurement à la date de la décision écrite d'interception ordonnée par le juge d'instruction, lesquels doivent être réalisés

conformément aux dispositions légales relatives aux perquisitions *(Cass. crim., 8 juill. 2015, n° 14-88.457*) ;

- le simple compte rendu de propos entendus par des policiers au cours d'une conversation téléphonique qui s'est déroulée en leur présence, sans artifice ni stratagème *(Cass. crim., 2 avr. 1997) ;*
- l'écoute et l'enregistrement des conversations tenues par la personne mise en examen au parloir de la maison d'arrêt *(Cass. crim., 12 déc. 2000, Bull. crim. 2000, n° 369)*.

Le procureur de la République peut solliciter du juge des libertés et de la détention (JLD) l'autorisation d'intercepter des correspondances dans deux cas :

- Dans le cadre d'une enquête préliminaire ou de flagrance (article 706-95 du CPP),

- Dans le cadre d'une enquête pour recherche d'une personne en fuite (article 74-2 CPP).

# Champ d'application

## 1. Dans le cadre d'une enquête préliminaire ou de flagrance

L'article 706-95 du CPP prévoit que le JLD peut autoriser l'interception *« selon les modalités des articles 100 alinéa 2, 100-1 et 100-3 à 100-7 du CPP* ».

### Conditions de fond

➔ **Autorité compétente**

L'initiative de la procédure incombe au procureur de la République. Il lui appartient d'adresser une requête au JLD, lequel peut autoriser ou non l'interception, l'enregistrement et la transcription des correspondances.

➔ **Nature de l'infraction motivant l'interception**

Il s'agit des seules infractions entrant dans le champ des articles 706-73 et 706-73-1 du CPP.

➔ **Nécessités de l'enquête**

Le JLD peut autoriser l'interception « *si les nécessités de l'enquête l'exigent* ».

Comme pour les interceptions ordonnées par le juge d'instruction, cette condition est librement appréciée par le JLD qui n'est pas tenu de motiver sa décision.

➔ **Personnes concernées**

L'article 706-95 du CPP ne définit pas les personnes dont les correspondances peuvent être interceptées.

A plusieurs reprises *(Cass. crim., 17 juill. 1990, Cass. crim., 26 nov. 1990 et Cass. crim., 9 déc. 1991)*, la Cour de cassation a rappelé que peuvent être mises sur écoutes les personnes intéressées « *qui ne sont pas seulement celles sur lesquelles pèsent des indices de culpabilité* ».
Il s'agit ainsi des personnes suspectes mais également de toute personne paraissant avoir participé aux faits ou susceptible de détenir des renseignements relatifs à ceux-ci.

Les dispositions protectrices de l'article 100-7 du CPP sont applicables dans le cadre d'une enquête préliminaire ou de flagrance.

➔ **Interdiction des artifices et stratagèmes**

La Cour de cassation estime que l'absence d'artifice ou de stratagème est une des conditions de validité de la décision d'interception *(Cass. crim., 9 oct. 1980 : Bull. crim. 1980, n° 255)*.

Dans un arrêt du 14 avril 2015 *(Cass. crim., 14 avr. 2015, n° 14-88.515 : JurisData n° 2015-008123)*, elle a considéré que le recueil des renseignements obtenus par les enquêteurs, lors d'une conversation fortuite du suspect avec un tiers, à l'occasion d'une interception téléphonique régulièrement autorisée par le juge d'instruction, n'avait pas constitué un procédé de recherche des preuves déloyal ou portant une atteinte illégale à la vie privée.

➔ **Durée de l'interception**

Les interceptions peuvent être ordonnées pour une durée maximale d'**1 mois renouvelable une fois** dans les mêmes conditions de forme et de durée.

- *Point de départ du délai*

La mesure d'interception a pour point de départ le jour de la mise en place effective du dispositif d'écoute (*Cass. crim., 10 mai 2012, n° 11-87.328, F-P+B : JurisData n° 2012-011301 ; Bull. inf. C. cass. 15 oct. 2012, n° 1110*).

- *Appréciation de la durée*

La durée de l'interception s'applique à la ligne téléphonique interceptée et non à la personne qui en est titulaire (*Cass. crim., 8 juill. 2015, n° 15-81.731 : JurisData n° 2015-016435*).
La Cour de cassation a considéré que l'interception successive ou cumulée de différentes lignes téléphoniques utilisées par une même personne pouvait excéder la durée de 2 mois prévue par l'article 706-95 CPP aux motifs qu'il s'agit d'une mesure nécessaire à la défense de l'ordre et à la prévention des infractions pénales.

## Conditions de forme

➔ **Une décision écrite**

La décision du JLD ne peut être prise que par ordonnance. Elle doit être datée et signée. Elle n'a pas de caractère juridictionnel et est insusceptible de recours.

➔ **Contenu de la décision**

Conformément à l'article 100-1 du CPP, la décision du JLD doit mentionner, outre l'infraction qui motive le recours à l'interception et la durée de cette dernière,

- *Tous les éléments d'identification de la liaison à intercepter*

La Cour de cassation a reconnu la validité d'une commission rogatoire ne comportant pas l'identification du titulaire de la ligne placée sous surveillance aux motifs que les mentions relatives au numéro de la ligne et à l'identité de ceux qui l'utilisent sont suffisantes au regard des exigences de l'article 100-1 du CPP *(Cass. crim., 25 févr. 2003 : Juris-Data n° 2003-018634)*.

Interception d'une ligne étrangère
Il est possible d'intercepter et d'enregistrer les conversations émises à partir du territoire français à destination d'une ligne étrangère, entrant sur le territoire national en provenance d'une ligne étrangère ou transitant sur le réseau d'un opérateur de téléphonie français (*Cass. crim., 1er févr. 2011, n° 10-83.523 : JurisData n° 2011-001693*).

En revanche, la mise en œuvre d'une opération d'interception à l'étranger suppose qu'une demande d'entraide soit adressée aux autorités compétentes de l'Etat concerné. De jurisprudence constante, la Cour de cassation considère que le magistrat instructeur n'a pas à se

prononcer sur la régularité des actes accomplis à l'étranger par une autorité étrangère (*Crim. 27 juin 2001, n° 01-82.578*).

Toutefois, dans un récent arrêt du 19 octobre 2016 (*Crim. 19 oct. 2016, F-P+B, n° 16-81.920*), la Cour de cassation a estimé que les autorités d'un État membre de l'Union pouvaient remettre aux autorités judiciaires françaises, un CD-Rom contenant la transcription d'écoutes téléphoniques réalisées à l'étranger sans demande préalable des autorités françaises aux motifs que l'article 7 de la décision-cadre du 18 décembre 2006, transposé à l'article 695-9-38 CPP, prévoit « *la possibilité pour un État membre, dans des conditions qui sont réunies en l'espèce, de remettre à un autre État membre, en dehors de toute demande, des renseignements pouvant contribuer à l'identification de l'auteur d'un meurtre* ».

## 2. Dans le cadre d'une enquête pour recherche et découverte d'un individu en fuite

En application de l'article 74-2 du CPP, le procureur de la République peut solliciter du JLD qu'il autorise une interception afin de rechercher et de découvrir une personne en fuite.
L'alinéa 2 de cette disposition prévoit que le JLD peut autoriser l'interception « *selon les modalités prévues par les articles 100, 100-1 et 100-3 à 100-7 du CPP* ».

### Conditions de fond

➔ **Autorité compétente**

Il convient de se reporter aux développements précédents.

➔ **Catégories de personnes recherchées**

Les dispositions de l'article 74-2 du CPP ne peuvent être mises en œuvre que pour rechercher certaines catégories de personnes limitativement énumérées. Cette liste a été récemment élargie par la loi du 3 juin 2016.

Il s'agit ainsi de :

1° Personne faisant l'objet d'un mandat d'arrêt délivré par le juge d'instruction, le juge des libertés et de la détention, la chambre de l'instruction ou son président ou le président de la cour d'assises, alors qu'elle est renvoyée devant une juridiction de jugement ;

2° Personne faisant l'objet d'un mandat d'arrêt délivré par une juridiction de jugement ou par le juge de l'application des peines ;

3° Personne condamnée à une peine privative de liberté sans sursis supérieure ou égale à un an ou à une peine privative de liberté supérieure ou égale à un an résultant de la révocation d'un sursis assorti ou non d'une mise à l'épreuve, lorsque cette condamnation est exécutoire ou passée en force de chose jugée ;

4° Personne inscrite au fichier judiciaire national automatisé des auteurs d'infractions terroristes ayant manqué aux obligations prévues à l'article 706-25-7 ;

5° Personne inscrite au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes ayant manqué aux obligations prévues à l'article 706-53-5 ;

6° Personne ayant fait l'objet d'une décision de retrait ou de révocation d'un aménagement de peine ou d'une libération sous contrainte, ou d'une décision de mise à exécution de l'emprisonnement prévu par la juridiction de jugement en cas de violation des obligations et interdictions résultant d'une peine, dès lors que cette décision a pour conséquence la mise à exécution d'un quantum ou d'un reliquat de peine d'emprisonnement supérieur à un an.

➔ **Nécessités de l'enquête**

Il convient de se reporter aux développements précédents.

➔ **Personnes concernées par l'interception**

L'article 74-2 du CPP ne définit pas les personnes dont les correspondances peuvent être interceptées. Il s'agit vraisemblablement de toutes les personnes qui seraient susceptibles de fournir des renseignements sur la retraite de la personne en fuite.

Les dispositions protectrices de l'article 100-7 CPP sont applicables.

➔ **Interdiction des artifices et stratagèmes**

Il convient de se reporter aux développements précédents.

➔ **Durée de l'interception**

Les interceptions peuvent être ordonnées pour une durée maximale de **2 mois renouvelables** dans les mêmes conditions de forme et de durée.

En matière correctionnelle, la durée totale de l'interception ne peut excéder **6 mois**.

### Conditions de forme

Il convient de se reporter aux développements précédents.

## Mise en œuvre pratique

Les articles 74-2 et 706-95 du CPP disposent que, pour l'application des articles 100-3 à 100-5 du CPP, les attributions confiées par ces textes au juge d'instruction ou à l'OPJ commis par lui sont exercées par le procureur de la République ou l'OPJ requis par lui.

C'est donc au procureur de la République ou à l'OPJ requis par lui qu'il appartient de :

- requérir les agents habilités afin de procéder à l'installation du dispositif d'interception,

- dresser procès-verbal de chacun des opérations d'interception,

- retranscrire les correspondances utiles à la manifestation de la vérité.

Toutefois, les opérations sont réalisées sous l'autorité et le contrôle du JLD qui est informé sans délai des actes accomplis par le procureur de la République ou l'officier de police judiciaire requis.

Dans un arrêt du 23 mai 2006 (*Bull crim. N°139*), la Cour de cassation a précisé que l'article 706-95 du CPP n'exige pas que le JLD exerce un contrôle immédiat sur le déroulement de l'écoute mais

seulement qu'il soit informé sans délai par le procureur de la République à l'issue de l'opération d'interception.

### ➔ Agents et services habilités

Le procureur de la République ou l'OPJ requis par lui peut requérir tout agent qualifié d'un service ou organisme placé sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de communications électroniques autorisé, en vue de procéder à l'installation d'un dispositif d'interception.

- En dehors de la PNIJ

En pratique, la mise en œuvre d'une interception suppose :
- une réquisition à un opérateur de communication électronique (OCE),
- une réquisition à un fournisseur de plateforme d'interception.

L'agent qualifié requis pour procéder à des opérations d'interception de communications téléphoniques n'est pas tenu de prêter serment. (Cass. crim., 23 mai 2006, n° 06-81.705 : JurisData n° 2006-034215 ; Bull. crim. 2006, n° 141).

*Recours à un prestataire non habilité*

La Cour de cassation a validé le recours à un prestataire non habilité au motif « *qu'aucune violation des dispositions légales en matière d'interception de communications téléphoniques ne saurait résulter de la simple fourniture à un service de police du matériel technique lui permettant d'y procéder par un prestataire qui n'accomplit aucun acte de procédure* » (*Cass. crim., 22 mars 2016, n° 15-83.207 : JurisData n° 2016-004951*).

- *Recours à la PNIJ*

La PNIJ se substitue aux dispositifs d'écoute et d'enregistrement fournis par des prestataires privés et au système de transmission des interceptions judiciaires (STIJ) mis en œuvre par le ministère de la justice.

En outre, elle permet une transmission automatisée des réquisitions adressées aux OCE.

A compter du 1er janvier 2017, en application de l'article 230-45 du CPP, ces réquisitions devront, sauf impossibilité technique, être adressées via la plateforme.

### ➔ Formalisme des opérations

En vertu de l'article 100-4 du CPP, le procureur de la République ou l'OPJ requis par lui dresse un procès-verbal de chacune des opérations d'interception et d'enregistrement, et précise la date et l'heure auxquelles les opérations ont commencé et se sont terminées.

### ➔ Retranscription

Conformément à l'article 100-5 du CPP, le procureur de la République ou l'OPJ requis par lui transcrit les seules correspondances utiles à la manifestation de la vérité.

Ne peuvent être transcrites à peine de nullité :

- les correspondances avec un avocat relevant de l'exercice des droits de la défense ;
- celles avec un journaliste permettant d'identifier une source en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse.

➢ *Recours à la PNIJ*

L'OPJ rédige directement les procès-verbaux de retranscription dans la PNIJ. Il les édite ensuite pour les joindre à la procédure.
Le procureur de la République a accès aux interceptions en cours et peut consulter les communications interceptées sur la PNIJ.

➔ **Conservation des enregistrements**

➢ *En dehors de la PNIJ*

En vertu des articles 100-4 alinéa 2 et 100-6 du CPP, ces enregistrements sont placés sous scellés fermés et ne sont détruits, à la diligence du procureur de la République ou du procureur général, qu'à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction.

➢ *Recours à la PNIJ*

En application de l'article 230-45 du CPP (qui n'entrera en vigueur que le 1er janvier 2017), les dispositions précitées ne sont pas applicables aux données conservées dans la PNIJ. Dans ce cas en effet, l'article R.40-49 CPP prévoit que les données relatives aux interceptions judiciaires sont placées sous scellés au sein de la PNIJ qui joue le rôle d'un coffre-fort numérique.

Le procureur de la République peut donc consulter les scellés dans la PNIJ. Il lui suffit de solliciter de la délégation aux interceptions judiciaires (DIJ) le transfert du scellé depuis le coffre-fort numérique. Il peut également demander à la DIJ une copie chiffrée du scellé sur support physique, qui lui sera transmise par voie postale ou par porteur.

Ces données sont détruites à l'expiration du délai de prescription de l'action publique.

Aux termes des dispositions de l'article 20 de la Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne, la mise en œuvre d'une interception téléphonique depuis un « Etat interceptant » dans un autre Etat membre[1], doit être notifiée à ce dernier, lequel dispose d'un délai de 96 heures pour autoriser la poursuite de l'interception ou demander son interruption. Cette notification est susceptible d'intervenir antérieurement ou postérieurement à la réalisation de l'interception.

[1] Dès lors que l'assistance technique de l'Etat membre n'est pas requise.

FICHE TECHNIQUE

# INTERCEPTIONS DE COMMUNICATIONS ELECTRONIQUES
# Dans le cadre d'une information judiciaire

## Définition juridique

**Fondement légal :**

- **Les articles 100 à 100-7 du code de procédure pénale (CPP)** issus de la loi du 10 juillet 1991 et récemment modifiés par la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale ;
- **L'article 80-4 du CPP** issu de la loi du 9 septembre 2012.

**Définition** :
L'article 100 du CPP, modifié par la loi du 3 juin 2016, vise « *l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques* ».

Selon l'article 32 du Code des postes et communications électroniques (CPCE), les communications électroniques correspondent à « *toute transmission, émission ou réception de signes, signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, optique, radioélectricité ou autres systèmes électromagnétiques* ».

Est donc concernée l'interception des correspondances émises ou reçues sur différents supports tels que les téléphones fixes ou mobiles, les tablettes ou les ordinateurs.

Les opérations visées aux articles 100 et suivants du CPP sont réalisées grâce à des dispositifs d'interception qui supposent l'intervention de spécialistes des communications électroniques. Toutefois, la jurisprudence y assimile des écoutes effectuées sans l'emploi de procédés particuliers.

**Entrent ainsi dans le champ d'application de l'article 100** :

- l'enregistrement puis la transcription par des OPJ de conversations téléphoniques par apposition d'un dispositif relié au combiné de l'appareil avec l'accord d'un des correspondants *(Cass. crim., 27 févr. 1996) ;*
- les messages instantanés échangés entre plusieurs personnes au moyen d'une liaison sécurisée par un dispositif de cryptage de type BLACKBERRY MESSENGER (*Cass. Crim. 16 déc. 2015).*

**En sont en revanche exclus** :

- l'appréhension, l'enregistrement et la transcription de correspondances émises ou reçues par la voie des télécommunications antérieurement à la date de la décision écrite d'interception ordonnée par le juge d'instruction, lesquels doivent être réalisés conformément aux dispositions légales relatives aux perquisitions *(Cass. crim., 8 juill. 2015, n° 14-88.457*) ;

- le simple compte rendu de propos entendus par des policiers au cours d'une conversation téléphonique qui s'est déroulée en leur présence, sans artifice ni stratagème *(Cass. crim., 2 avr. 1997 ) ;*
- l'écoute et l'enregistrement des conversations tenues par la personne mise en examen au parloir de la maison d'arrêt *(Cass. crim., 12 déc. 2000, Bull. crim. 2000, n° 369)*.

Le juge d'instruction peut ordonner l'interception de correspondances dans deux cas :

- en matière criminelle et correctionnelle ;
- dans le cadre d'une information pour recherches des causes de la mort ou des causes d'une disparition.

# Champ d'application

## 1. En matière correctionnelle et criminelle

### Conditions de fond

➔ **Autorité compétente**

L'article 100 du CPP mentionne uniquement le juge d'instruction.

Toutefois, les articles 205 et 283 du CPP attribuent respectivement cette compétence à la chambre de l'instruction et au président de la cour d'assises lorsqu'ils procèdent à des suppléments d'information.

➔ **Nature de l'infraction**

En application de l'article 100 du CPP, une interception ne peut être ordonnée que si l'infraction qui la motive est punie d'une peine égale ou supérieure à 2 ans d'emprisonnement.

➔ **Nécessités de l'instruction**

L'article 100 du CPP dispose que le juge d'instruction peut prescrire l'interception « *lorsque les nécessités de l'information l'exigent* ».

Cette condition est librement appréciée par le magistrat instructeur qui n'est d'ailleurs pas tenu de motiver sa décision.

➔ **Personnes concernées**

Les articles 100 et suivants du CPP ne définissent pas les catégories de personnes susceptibles de faire l'objet d'écoutes téléphoniques.

A plusieurs reprises *(Cass. crim., 17 juill. 1990, Cass. crim., 26 nov. 1990 et Cass. crim., 9 déc. 1991)*, la Cour de cassation a rappelé que peuvent être mises sur écoutes les personnes intéressées « *qui ne sont pas seulement celles sur lesquelles pèsent des indices de culpabilité* ».

Il s'agit ainsi des personnes mises en examen mais également de toute personne paraissant avoir participé aux faits ou susceptible de détenir des renseignements relatifs à ces derniers.

En revanche, **la loi protège certaines catégories de personnes**.

Ainsi, conformément à l'article 100-7, aucune interception ne peut avoir lieu :

- sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction ;

- sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction ;
- sur une ligne dépendant du cabinet d'un magistrat ou de son domicile sans que le premier président ou le procureur général de la juridiction où il réside en soit informé.

Ces formalités sont prescrites à peine de nullité.

➔ **Interdiction des artifices et stratagèmes**

La Cour de cassation considère l'absence d'artifice ou de stratagème comme une des conditions de validité de la décision d'interception *(Cass. crim., 9 oct. 1980 : Bull. crim. 1980, n° 255)*.

Dans un arrêt du 14 avril 2015 *(Cass. crim., 14 avr. 2015, n° 14-88.515 : JurisData n° 2015-008123)*, elle a estimé que le recueil des renseignements obtenus par les enquêteurs, lors d'une conversation fortuite du suspect avec un tiers, à l'occasion d'une interception téléphonique régulièrement autorisée par le juge d'instruction, n'avait pas constitué un procédé de recherche des preuves déloyal ou portant une atteinte illégale à la vie privée.

➔ **Durée de la mesure :**

La décision d'interception est prise pour une durée maximale de **4 mois**. Elle peut être renouvelée dans les mêmes conditions de forme et de durée.
La loi du 3 juin 2016 a limité la durée totale de l'interception. Désormais, la durée totale d'une interception ne peut excéder **1 an.** Toutefois, si l'infraction qui a motivé l'interception est une infraction relevant de la criminalité organisée (art.706-73 et 706-73-1 du CPP), cette durée est portée à **2 ans.**

- *Point de départ du délai*

La mesure d'interception a pour point de départ le jour de la mise en place effective du dispositif d'écoute (*Cass. crim., 10 mai 2012, n° 11-87.328, F-P+B : JurisData n° 2012-011301 ; Bull. inf. C. cass. 15 oct. 2012, n° 1110*).

- *Appréciation de la durée*

La durée de l'interception s'applique à la ligne téléphonique interceptée et non à la personne qui en est titulaire (*Cass. crim., 8 juill. 2015, n° 15-81.731 : JurisData n° 2015-016435*).
Dès lors, en cas d'interception d'un boitier auquel sont associées plusieurs puces, il convient de s'assurer que la durée d'interception de chacune des lignes (c'est à dire de chacune des puces associées au boîtier) n'excède pas la durée maximale fixée par l'article 100-2 du CPP.

- *Articulation avec les interceptions ordonnées dans le cadre d'une enquête menée par le parquet*

La limitation de durée des écoutes téléphoniques fixée par les nouvelles dispositions de l'article 100-2 du CPP ne concerne que les interceptions se déroulant dans le cadre de l'information judiciaire.
D'ailleurs, s'agissant des interceptions téléphoniques autorisées par le juge des libertés et de la détention, l'article 706-95 du CPP ne renvoie aucunement aux dispositions de l'article 100-2 du CPP.

Dès lors, sous réserve de la jurisprudence ultérieure, il apparaît que les dispositions précitées consacrent l'existence de deux régimes autonomes, celui des interceptions autorisées dans le cadre des enquêtes conduites par le parquet et celui des interceptions ordonnées par le magistrat instructeur.

La durée des interceptions conduites lors de l'enquête préliminaire ou de flagrance ne s'impute donc pas sur celle des écoutes ordonnées au cours de l'information judiciaire.

### Conditions de forme

➔ **Une décision écrite**

Comme tous les actes du juge d'instruction, la décision d'interception doit être datée et signée. En revanche, la loi n'exige pas qu'elle soit motivée. Cette décision n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

➔ **Contenu de la décision**

Conformément à l'article 100-1 du CPP, la décision doit mentionner, outre l'infraction qui motive le recours à l'interception et la durée de cette dernière,

- *Tous les éléments d'identification de la liaison à intercepter*

La Cour de cassation a reconnu la validité d'une commission rogatoire ne comportant pas l'identification du titulaire de la ligne placée sous surveillance aux motifs que les mentions relatives au numéro de la ligne et à l'identité de ceux qui l'utilisent sont suffisantes au regard des exigences de l'article 100-1 du CPP *(Cass. crim., 25 févr. 2003 : Juris-Data n° 2003-018634)*.

Interception d'une ligne étrangère

Il est possible d'intercepter et d'enregistrer les conversations émises à partir du territoire français à destination d'une ligne étrangère, entrant sur le territoire national en provenance d'une ligne étrangère ou transitant sur le réseau d'un opérateur de téléphonie français (*Cass. crim., 1er févr. 2011, n° 10-83.523 : JurisData n° 2011-001693*).

En revanche, la mise en œuvre d'une opération d'interception à l'étranger suppose qu'une commission rogatoire internationale soit adressée aux autorités compétentes de l'Etat concerné. De jurisprudence constante, la Cour de cassation considère que le magistrat instructeur n'a pas à se prononcer sur la régularité des actes accomplis à l'étranger par une autorité étrangère (*Crim. 27 juin 2001, n° 01-82.578*).

Toutefois, dans un récent arrêt du 19 octobre 2016 (*Crim. 19 oct. 2016, F-P+B, n° 16-81.920*), la Cour de cassation a considéré que les autorités d'un État membre de l'Union pouvaient remettre aux autorités judiciaires françaises, un CD-Rom contenant la transcription d'écoutes téléphoniques réalisées à l'étranger sans demande préalable des autorités françaises aux motifs que l'article 7 de la décision-cadre du 18 décembre 2006, transposé à l'article 695-9-38 du CPP, prévoit *« la possibilité pour un État membre, dans des conditions qui sont réunies en l'espèce, de remettre à un autre État membre, en dehors de toute demande, des renseignements pouvant contribuer à l'identification de l'auteur d'un meurtre* ».

## 2. Dans le cadre d'une information pour recherches des causes de la mort ou des causes d'une disparition

Le juge d'instruction peut ordonner de telles interceptions :

- Lorsqu'il est requis en application de l'article 74 du CPP, d'informer pour recherche des causes de la mort ;

- Lorsqu' il est requis, en application de l'article 74-1 du CPP, d'informer pour recherche des causes de la disparition, après que la disparition d'un mineur ou d'un majeur protégé est intervenue ou a été constatée.

L'article 80-4 du CPP précise que les interceptions sont effectuées dans les conditions prévues au deuxième alinéa de l'article 100 et aux articles 100-1 à 100-7 du CPP.

### Conditions de fond

Il convient de se reporter aux développements précédents à l'exception de ceux relatifs à la durée de l'opération.

➔ **Durée de la mesure**

Dans ce cas, les interceptions ne peuvent excéder une durée de **2 mois renouvelables**.

### Conditions de forme

Il convient de se reporter aux développements précédents.

## Mise en œuvre des mesures

Sans modifier le régime des interceptions judiciaires, le déploiement de la plateforme nationale des interceptions judiciaires (PNIJ) a une incidence sur la mise en œuvre pratique des opérations d'interception.

➔ **Agents et services habilités**

Conformément à l'article 100-3 du CPP, le juge d'instruction ou l'OPJ commis par lui peut requérir tout agent qualifié d'un service ou organisme placé sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de communications électroniques autorisé, en vue de procéder à l'installation d'un dispositif d'interception.

➢ <u>En dehors de la PNIJ</u>

En pratique, la mise en œuvre d'une interception suppose :
- une réquisition à un opérateur de communication électronique (OCE) ;
- une réquisition à un fournisseur de plateforme d'interception.

L'agent qualifié requis pour procéder à des opérations d'interception de communications téléphoniques n'est pas tenu de prêter serment. (Cass. crim., 23 mai 2006, n° 06-81.705 : JurisData n° 2006-034215 ; Bull. crim. 2006, n° 141).

*<u>Recours à un prestataire non habilité</u>*
La Cour de cassation a validé le recours à un prestataire non habilité au motif *« qu'aucune violation des dispositions légales en matière d'interception de communications téléphoniques ne saurait résulter de la simple fourniture à un service de police du matériel technique lui permettant d'y procéder par un prestataire qui n'accomplit aucun acte de procédure »*(*Cass. crim., 22 mars 2016, n° 15-83.207 : JurisData n° 2016-004951*).

➢ *Recours à la PNIJ*

La PNIJ se substitue aux dispositifs d'écoute et d'enregistrement fournis par des prestataires privés et au système de transmission des interceptions judiciaires (STIJ) mis en œuvre par le ministère de la justice. En outre, elle permet une transmission automatisée des réquisitions adressées aux OCE. A compter du 1er janvier 2017, en application de l'article 230-45 du CPP, ces réquisitions devront, sauf impossibilité technique, être adressées via la plateforme.

### ➔ Formalisme des opérations

En vertu de l'article 100-4 du CPP, le juge d'instruction ou l'OPJ commis par lui dresse un procès-verbal de chacune des opérations d'interception et d'enregistrement, et précise la date et l'heure auxquelles les opérations ont commencé et se sont terminées.

### ➔ Retranscription

Conformément à l'article 100-5 du CPP, le juge d'instruction ou l'OPJ transcrit les seules correspondances utiles à la manifestation de la vérité.

Ne peuvent être transcrites à peine de nullité :

- les correspondances avec un avocat relevant de l'exercice des droits de la défense ;
- celles avec un journaliste permettant d'identifier une source en violation de l'article 2 de la loi du 29 juillet 1881 sur la liberté de la presse.

➢ *Recours à la PNIJ*

L'OPJ rédige directement les procès-verbaux de retranscription dans la PNIJ. Il les édite ensuite pour les joindre à la procédure. Le magistrat instructeur a accès aux interceptions en cours et peut consulter les communications interceptées sur la PNIJ.

### ➔ Conservation des enregistrements

➢ *En dehors de la PNIJ*

En vertu des articles 100-4 alinéa 2 et 100-6 du CPP, ces enregistrements sont placés sous scellés fermés et ne sont détruits, à la diligence du procureur de la République ou du procureur général, qu'à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction.

➢ *Recours à la PNIJ*

En application de l'article 230-45 du CPP (qui n'entrera en vigueur que le 1er janvier 2017), les dispositions précitées ne sont pas applicables aux données conservées dans la PNIJ. Dans ce cas en effet, l'article R.40-49 CPP prévoit que les données relatives aux interceptions judiciaires sont placées sous scellés au sein de la PNIJ qui joue le rôle d'un coffre-fort numérique. Le magistrat instructeur peut donc consulter les scellés dans la PNIJ. Il lui suffit de solliciter de la délégation aux interceptions judiciaires (DIJ) le transfert du scellé depuis le coffre-fort numérique.

Il peut également demander à la DIJ une copie chiffrée du scellé sur support physique, qui lui sera transmise par voie postale ou par porteur.

Ces données sont détruites à l'expiration du délai de prescription de l'action publique.

Aux termes des dispositions de l'article 20 de la Convention du 29 mai 2000 relative à l'entraide judiciaire en matière pénale entre les Etats membres de l'Union européenne, la mise en œuvre d'une interception téléphonique depuis un « Etat interceptant » dans un autre Etat membre[1], doit être notifiée à ce dernier, lequel dispose d'un délai de 96 heures pour autoriser la poursuite de l'interception ou demander son interruption. Cette notification est susceptible d'intervenir antérieurement ou postérieurement à la réalisation de l'interception.

[1] Dès lors que l'assistance technique de l'Etat membre n'est pas requise.

FICHE TECHNIQUE

# LA GEOLOCALISATION
# Dans le cadre d'une enquête dirigée par le parquet

## Définition juridique

**Fondement légal :** les articles **230-32** à **230-44** et suivants du CPP *(issus de la loi du 28 mars 2014).*

**Définition et champ d'application**

La géolocalisation est le recours à tout moyen technique destiné à localiser en temps réel, sur l'ensemble du territoire national, une personne à son insu, un véhicule ou tout autre objet, sans le consentement de son propriétaire ou de son possesseur.

Tout objet peut être géolocalisé[1]. Comme en matière d'interceptions téléphoniques, la mesure de géolocalisation n'est pas limitée aux personnes soupçonnées d'avoir commis une infraction[2].

Entrent dans le champ d'application de cette technique d'enquête (et donc des articles 230-32 et s.) :

- le suivi dynamique de tout objet (téléphone mobile, tablette, système GPS autonome ou intégré à un appareil de télécommunication ou à un véhicule…) ;
- l'utilisation d'un dispositif dédié de géolocalisation (balise) placé sur un moyen de transport ou tout autre objet ;

N'entrent pas dans le champ d'application de cette technique d'enquête (car relevant du pouvoir de réquisition) :

- les opérations permettant a *posteriori* de retracer les déplacements d'un objet ou d'un individu, par la communication des données conservées (notamment les bornes déclenchées) par les opérateurs de télécommunication ou toute personne ou organisme public ou privé ;
- le suivi dynamique d'un terminal de télécommunication, d'un véhicule ou de tout autre objet dont le propriétaire ou le possesseur légitime est la personne disparue ou encore la victime de l'infraction sur laquelle porte l'enquête, dès lors que ces opérations ont pour objet de retrouver la victime, l'objet qui lui a été dérobé ou encore la personne disparue (article 230-44 du CPP).

## Conditions de l'autorisation

### ➔ Conditions de fond

Le recours à la géolocalisation est possible dans le cadre d'une enquête flagrante ou préliminaire[3] lorsque la procédure est relative à l'une des infractions suivantes revêtant une certaine gravité :

- un délit contre les personnes (livre II du CP) puni d'au moins trois ans d'emprisonnement ;
- délit d'évasion (article 434-27 du CP) ou de recel de malfaiteurs (article 434-6 du CP) ;
- autres crimes ou délits lorsqu'ils sont punis d'au moins cinq ans d'emprisonnement.

Les mesures de géolocalisation peuvent également être effectuées dans le cadre des enquêtes :
- en recherche des causes de la mort ou des blessures (article 74 du CPP) ;
- en recherche des causes de la disparition (article 74-1 du CPP) ;
- en recherche d'une personne en fuite (article 74-2 du CPP).

[1] Soit par l'exploitation de sa propre technologie, soit à travers la pose d'une balise.
[2] La mesure de géolocalisation peut être diligentée à l'encontre de tout individu dès lors que les nécessités de l'enquête l'exigent.
[3] Ainsi que dans le cadre d'une information judiciaire (cf. fiche technique « géolocalisation phase instruction »).

En outre, l'article 67 bis 2 du code des douanes prévoit la possibilité, pour les agents des douanes habilités, de mettre en place une mesure de géolocalisation dès lors que le délit douanier est puni d'une peine d'emprisonnement supérieure ou égale à cinq ans.

➔ **Conditions de forme**

Dans le cadre des enquêtes diligentées par le procureur de la République, ce dernier peut autoriser les opérations de géolocalisation, lesquelles doivent être prolongées par le juge des libertés et de la détention.

L'autorisation du procureur de la République ou du juge des libertés et de la détention doit :

- être écrite et horodatée ;
- comporter les éléments permettant d'identifier l'objet géolocalisé (pour un téléphone : n° IMSI, IMEI ; pour un véhicule : n° d'immatriculation, modèle) ;
- prévoir la durée maximale de la mesure ;
- mentionner le cadre de l'enquête, et le cas échéant l'infraction visée (*conformément aux conditions de fond*) ; étant précisé que la révélation - au cours des opérations - d'autres infractions non visées par cette autorisation ne font encourir aucune nullité pour les éventuelles procédures incidentes.

*Cette décision n'a pas de caractère juridictionnel et est insusceptible de recours.*

➔ **Durée de la mesure** (230-33 du CPP)

La durée maximale de l'autorisation délivrée par le parquet est de **15 jours consécutifs**.
Si le délai de 15 jours s'écoule à compter de la mise en place effective de la mesure de géolocalisation, il ne peut être interrompu par la survenance de difficultés liées au recueil des données (pannes techniques ou départ de la personne ciblée à l'étranger).
A l'issue de ce délai de 15 jours, la mesure de géolocalisation ne peut se poursuivre que sur autorisation du juge des libertés et de la détention, saisi par requête du procureur de la République et ce pour une durée (maximale) d'**un mois** renouvelable dans les mêmes formes sans limitation.
L'article 230-33 du CPP n'impose pas que la décision du JLD intervienne dans la continuité directe de l'autorisation du procureur de la République, de telle sorte que la mesure de géolocalisation peut s'être interrompue à l'expiration de l'autorisation du parquet avant d'être prolongée par le juge des libertés et de la détention.

➔ **Introduction dans les lieux privés aux fins d'installation ou de retrait d'un dispositif technique de géolocalisation**

Lorsque les nécessités de l'enquête l'exigent, l'introduction dans des lieux privés peut être autorisée, aux seules fins de mettre en place ou de retirer le moyen technique de géolocalisation.
La réalisation de perquisitions et saisies concomitantes est exclue.
La décision autorisant cette intrusion doit mentionner le lieu de l'installation du dispositif, des éléments relatifs aux investigations d'ores et déjà conduites et la nécessité de recourir à une mesure de géolocalisation.

Peut être autorisée, y compris en dehors des heures prévues par l'article 59 du CPP, l'introduction dans :

- les **lieux privés destinés** ou utilisés **à l'entrepôt** de véhicules, fonds, valeurs, marchandises ou matériels (parking, conteneur, hangar…), ou dans un **véhicule situé sur la voie publique** ou dans de tels lieux.
  Cette intrusion qui est permise dans tous les cadres procéduraux, doit être autorisée par décision écrite du procureur de la République ;

- tout **autre lieu privé** (notamment les locaux professionnels : banque ; administration, entreprise) à l'exception des lieux d'habitation.
  Le procureur de la République doit autoriser par écrit cette intrusion qui ne peut s'inscrire que dans le cadre d'une enquête relative à un délit puni d'au moins cinq ans d'emprisonnement ou diligentée dans le cadre des articles 74 à 74-2 du CPP (enquête en recherche des causes de la mort/des blessures, en recherche des causes de la disparition, en recherche d'une personne en fuite) ;

- un **lieu d'habitation** (maisons et appartements ainsi que leurs annexes et dépendances).
  L'intrusion doit être autorisée par décision écrite du juge des libertés et de la détention, saisi par le procureur de la République dans le cadre d'une enquête relative à un délit puni d'au moins cinq ans d'emprisonnement ou d'une procédure en recherche des causes de la mort/des blessures, des causes de la disparition, ou d'une personne en fuite.

➔ **Lieux prohibés** (article 230-34 du CPP) :

Il ne peut être mis en place moyen de géolocalisation dans les lieux suivants :
- le cabinet ou le domicile d'un avocat (56-1 du CPP) ;
- les locaux et véhicules d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne ou d'une agence de presse, ou encore le domicile d'un journaliste (56-2 du CPP) ;
- le cabinet d'un médecin, d'un notaire, d'un huissier (56-3 du CPP) ;
- un lieu abritant des éléments couverts par le secret de la défense nationale (56-4 du CPP) ;
- les locaux d'une juridiction ou au domicile d'une personne exerçant des fonctions juridictionnelles (magistrat professionnel ou non professionnel) (56-5 du CPP) ;
- le bureau ou le domicile d'un député, d'un sénateur ou d'un avocat (100-7 du CPP).

➔ **Cas particulier : l'urgence** (230-35 du CPP)

La mise en place de moyen de géolocalisation en temps réel peut être effectuée ou prescrite par l'**OPJ seul** , sans autorisation préalable du procureur de la République, **en cas d'urgence** liée au risque imminent de dépérissement des preuves ou d'atteintes graves aux personnes ou aux biens.

Informé immédiatement[4], le procureur de la République dispose de 24 heures pour :
- ordonner l'interruption de la mesure sans formalisme particulier;
- autoriser la poursuite de la mesure par décision écrite comportant, en plus des conditions de forme précédemment décrites, les circonstances de fait établissant l'existence du risque imminent.

A l'issue du délai de 24 heures et à défaut d'autorisation, il est mis fin à la mesure de géolocalisation. Les opérations déjà réalisées ne peuvent être utilisées ou retranscrites en procédure.

L'OPJ peut s'introduire de sa propre initiative dans les lieux privés tels que définis précédemment, à l'exception des lieux d'habitation pour lesquels il doit recueillir préalablement l'accord du juge des libertés et de la détention, saisi à cette fin par le procureur de la République. L'autorisation du JLD et la requête du procureur de la République, écrites, devront alors intervenir dans un délai de 24 heures. Compte tenu des délais prévus, ces décisions devront être horodatées.

## Mise en œuvre des mesures

➔ **Agents et services habilités :**

La géolocalisation est mise en place par un OPJ ou, sous sa responsabilité, par un APJ, ou prescrite sur réquisitions de l'officier de police judiciaire.
Le procureur de la République peut requérir tout agent qualifié relevant de la liste fixée par l'article D15-1-5 à D15-1-7 du CPP.

➔ **Formalisme des opérations :**

L'OPJ ou APJ dresse procès-verbal de chacune des opérations de mise en place du moyen technique de géolocalisation et des opérations d'enregistrement des données de localisation. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

[4] L'OPJ doit en informer immédiatement le procureur de la République par tout moyen et mention doit en être faite en procédure.

L'OPJ ou l'APJ décrit ou transcrit, dans un procès-verbal versé au dossier, les données enregistrées qui sont utiles à la manifestation de la vérité (230-39 du CPP).

➔ **Conservation des scellés :**

Les enregistrements sont placés sous scellés fermés. Si le moyen technique ne permet pas l'enregistrement, cette impossibilité doit être précisée par procès-verbal.

Les enregistrements de données de localisation sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction (230-43 du CPP).

➔ **La poursuite ou l'activation d'une géolocalisation en dehors des frontières du territoire national :**

La poursuite ou l'activation dynamique au-delà des frontières nationales d'un terminal de télécommunication ou le suivi à distance, hors du territoire national, d'un dispositif dédié de géolocalisation placé sur un moyen de transport ou tout autre objet, nécessite l'émission d'une demande d'entraide pénale internationale qui sera exécutée selon la loi de l'Etat requis.

Le contrôle de la régularité d'un acte d'exécution au regard de la loi du for est assuré par les autorités du for - c'est-à-dire les autorités étrangères.
Les actes réalisés à l'étranger étant régis par la loi de l'Etat requis, leur validité ne peut pas être appréciée au regard des dispositions de la loi française. Néanmoins, la Cour de cassation admet un contrôle minimum dont l'objet n'est pas d'examiner si les dispositions techniques de l'une ou l'autre des législations en présence ont été respectées, mais de s'assurer que *"les actes n'ont pas été accomplis en violation des droits de la défense, ni d'aucun principe général du droit"* (Crim. 4 novembre 1997, bull. n° 366).

Concernant la poursuite ou l'activation d'une géolocalisation en temps réel en dehors des frontières du territoire national, la Cour de cassation a pu estimer que les éléments recueillis ne peuvent être exploités en procédure que si la mesure de géolocalisation a été autorisée préalablement ou concomitamment par l'Etat concerné, ou que celui-ci a, postérieurement à la mesure, autorisé son exploitation, en exécution d'une demande d'entraide pénale (Crim. 9 février 2016).

FICHE TECHNIQUE

# LA GEOLOCALISATION
# Dans le cadre d'une information judiciaire

## Définition juridique

**Fondement légal :** les articles **230-32** à **230-44** et suivants du CPP *(issus de la loi du 28 mars 2014).*

**Définition et champ d'application**

La géolocalisation est le recours à tout moyen technique destiné à localiser en temps réel, sur l'ensemble du territoire national, une personne à son insu, un véhicule ou tout autre objet, sans le consentement de son propriétaire ou de son possesseur.

Tout objet peut être géolocalisé[1]. Comme en matière d'interceptions téléphoniques, la mesure de géolocalisation n'est pas limitée aux personnes soupçonnées d'avoir commis une infraction[2].

Entrent dans le champ d'application de cette technique d'enquête (et donc des articles 230-32 et s.) :

- le suivi dynamique de tout objet (téléphone mobile, tablette, système GPS autonome ou intégré à un appareil de télécommunication ou à un véhicule…) ;
- l'utilisation d'un dispositif dédié de géolocalisation (balise) placé sur un moyen de transport ou tout autre objet ;

N'entrent pas dans le champ d'application de cette technique d'enquête (car relevant du pouvoir de réquisition) :

- les opérations permettant a *posteriori* de retracer les déplacements d'un objet ou d'un individu, par la communication des données conservées (notamment les bornes déclenchées) par les opérateurs de télécommunication ou toute personne ou organisme public ou privé ;
- le suivi dynamique d'un terminal de télécommunication, d'un véhicule ou de tout autre objet dont le propriétaire ou le possesseur légitime est la personne disparue ou encore la victime de l'infraction sur laquelle porte l'enquête, dès lors que ces opérations ont pour objet de retrouver la victime, l'objet qui lui a été dérobé ou encore la personne disparue (article 230-44 du CPP).

## Conditions de l'autorisation

### ➔ Conditions de fond

Le recours à la géolocalisation est possible dans le cadre d'une instruction[3] relative à l'une des infractions suivantes revêtant une certaine gravité :

- un délit contre les personnes (livre II du CP) puni d'au moins trois ans d'emprisonnement ;
- le délit d'évasion (article 434-27 du CP) ou de recel de malfaiteurs (article 434-6 du CP) ;
- tous autres crimes ou délits lorsqu'ils sont punis d'au moins cinq ans d'emprisonnement.

Les mesures de géolocalisation peuvent également être effectuées dans le cadre d'une instruction :
- en recherche des causes de la mort ou des blessures (articles 74 et 80-4 du CPP) ;
- en recherche des causes de la disparition (articles 74-1 et 80-4 du CPP).

[1] Soit par l'exploitation de sa propre technologie, soit à travers la pose d'une balise.
[2] La mesure de géolocalisation peut être diligentée à l'encontre de tout individu dès lors que les nécessités de l'enquête l'exigent.
[3] Ainsi que dans le cadre d'une enquête flagrante ou préliminaire (cf. fiche technique « géolocalisation phase parquet »).

En outre, l'article 67 bis 2 du code des douanes prévoit la possibilité, pour les agents des douanes habilités, de mettre en place une mesure de géolocalisation dès lors que le délit douanier est puni d'une peine d'emprisonnement supérieure ou égale à cinq ans.

➔ **Conditions de forme**

L'autorisation du juge d'instruction doit :

- être écrite et horodatée ;
- comporter les éléments permettant d'identifier l'objet géolocalisé (pour un téléphone : n° IMSI, IMEI ; pour un véhicule : n° d'immatriculation, modèle) ;
- prévoir la durée maximale de la mesure ;
- mentionner le cade de l'information, et le cas échéant l'infraction visée (*conformément aux conditions de fond*) ; étant précisé que la révélation - au cours des opérations - d'autres infractions non visées par cette autorisation ne font encourir aucune nullité pour les éventuelles procédures incidentes.

*Cette décision n'a pas de caractère juridictionnel et est insusceptible de recours.*

En plus de l'ordonnance d'autorisation, le juge d'instruction doit délivrer une **commission rogatoire spécifique** aux OPJ qu'il désigne pour y procéder.

➔ **Durée de la mesure** (230-33 du CPP)

La durée maximale de l'autorisation délivrée par le juge d'instruction est de **4 mois consécutifs**.
Si le délai de 4 mois s'écoule à compter de la mise en place effective de la mesure de géolocalisation, il ne peut être interrompu par la survenance de difficultés liées au recueil des données (pannes techniques ou départ de la personne ciblée à l'étranger).
A l'issue de ce délai de 4 mois, la mesure de géolocalisation ne peut se poursuivre que sur autorisation du juge d'instruction, sous les mêmes conditions de forme et de délai (sans limitation du nombre de renouvellement).
Compte tenu de la jurisprudence relative aux prolongations d'autorisation de sonorisation *(Crim 13 nov. 2008)*, le renouvellement de l'autorisation doit intervenir avant l'expiration de la mesure précédente.

➔ **Introduction dans les lieux privés aux fins d'installation ou de retrait d'un dispositif technique de géolocalisation**

Lorsque les nécessités de l'information l'exigent, l'introduction dans des lieux privés peut être autorisée, aux seules fins de mettre en place ou de retirer le moyen technique de géolocalisation.
La réalisation de perquisitions et saisies concomitantes est exclue.
La décision autorisant cette intrusion doit mentionner le lieu de l'installation du dispositif, des éléments relatifs aux investigations d'ores et déjà conduites et la nécessité de recourir à une mesure de géolocalisation.

Peut être autorisée, y compris en dehors des heures prévues par l'article 59 du CPP, l'introduction dans :

- les **lieux privés destinés** ou utilisés **à l'entrepôt** de véhicules, fonds, valeurs, marchandises ou matériels (parking, conteneur, hangar…), ou dans un **véhicule situé sur la voie publique** ou dans de tels lieux.
  Cette intrusion doit être autorisée par décision écrite du juge d'instruction ;

- tout **autre lieu privé** (notamment les locaux professionnels : banque ; administration, entreprise) à l'exception des lieux d'habitation.
  Le juge d'instruction doit autoriser par écrit cette intrusion qui ne peut s'inscrire que dans le cadre d'une information relative à un délit puni d'au moins cinq ans d'emprisonnement ou d'une information en recherche des causes de la mort/des blessures/des causes de la disparition ;

- un **lieu d'habitation** (maisons et appartements ainsi que leurs annexes et dépendances).

Cette intrusion n'est possible que dans le cadre d'une information relative à un délit puni d'au moins cinq ans d'emprisonnement ou d'une procédure en recherche des causes de la mort/des blessures/des causes de la disparition.
Entre 6 heures et 21 heures, cette intrusion doit être autorisée par le juge d'instruction.
Entre 21 heures et 6 heures, cette intrusion doit être autorisée par le juge des libertés et de la détention, saisi par le juge d'instruction.

➔ **Lieux prohibés** (article 230-34 du CPP) :

Il ne peut être mis en place de moyen de géolocalisation dans les lieux suivants :

- le cabinet ou le domicile d'un avocat (56-1 du CPP) ;
- les locaux et véhicules d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne ou d'une agence de presse, ou encore le domicile d'un journaliste (56-2 du CPP) ;
- le cabinet d'un médecin, d'un notaire, d'un huissier (56-3 du CPP) ;
- un lieu abritant des éléments couverts par le secret de la défense nationale (56-4 du CPP) ;
- les locaux d'une juridiction ou au domicile d'une personne exerçant des fonctions juridictionnelles (magistrat professionnel ou non professionnel) (56-5 du CPP) ;
- le bureau ou le domicile d'un député, d'un sénateur ou d'un avocat (100-7 du CPP).

➔ **Cas particulier : l'urgence** (230-35 du CPP)

La mise en place de moyen de géolocalisation en temps réel peut être effectuée ou prescrite par l'**OPJ seul,** sans autorisation préalable du juge d'instruction, **en cas d'urgence** liée au risque imminent de dépérissement des preuves ou d'atteintes graves aux personnes ou aux biens.

Informé immédiatement, le juge d'instruction dispose de 24 heures pour :

- ordonner l'interruption de la mesure sans formalisme particulier;
- autoriser la poursuite de la mesure par décision écrite comportant, en plus des conditions de forme précédemment décrites, les circonstances de fait établissant l'existence du risque imminent.

A l'issue du délai de 24 heures et à défaut d'autorisation, il est mis fin à la mesure de géolocalisation. Les opérations déjà réalisées ne peuvent être utilisées ou retranscrites en procédure.

L'OPJ peut s'introduire de sa propre initiative dans les lieux privés tels que définis précédemment, à l'exception des lieux d'habitation entre 21 heures et 6 heures pour lesquels il doit recueillir préalablement l'accord du juge des libertés et de la détention, saisi à cette fin par le juge d'instruction. L'autorisation du JLD et la saisine du juge d'instruction, écrites, devront alors intervenir dans un délai de 24 heures. Compte tenu des délais prévus, ces décisions devront être horodatées.

## Mise en œuvre des mesures

➔ **Agents et services habilités :**

La géolocalisation est mise en place par un OPJ ou, sous sa responsabilité, par un APJ, ou prescrite sur réquisitions de l'officier de police judiciaire. Le juge d'instruction peut requérir tout agent qualifié relevant de la liste fixée par les articles D15-1-5 à D15-1-7 du CPP.

➔ **Formalisme des opérations :**

L'OPJ ou APJ dresse procès-verbal de chacune des opérations de mise en place du moyen technique de géolocalisation et des opérations d'enregistrement des données de localisation. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.

L'OPJ ou l'APJ décrit ou transcrit, dans un procès-verbal versé au dossier, les données enregistrées qui sont utiles à la manifestation de la vérité (230-39 du CPP).

➔ **Conservation des scellés :**

Les enregistrements sont placés sous scellés fermés. Si le moyen technique ne permet pas l'enregistrement, cette impossibilité doit être précisée par procès-verbal.

Les enregistrements de données de localisation sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il est dressé procès-verbal de l'opération de destruction (230-43 du CPP).

➔ **La poursuite ou l'activation d'une géolocalisation en dehors des frontières du territoire national :**

La poursuite ou l'activation dynamique au-delà des frontières nationales d'un terminal de télécommunication ou le suivi à distance, hors du territoire national, d'un dispositif dédié de géolocalisation placé sur un moyen de transport ou tout autre objet, nécessite l'émission d'une demande d'entraide pénale internationale qui sera exécutée selon la loi de l'Etat requis.

Le contrôle de la régularité d'un acte d'exécution au regard de la loi du for est assuré par les autorités du for - c'est-à-dire les autorités étrangères.
Les actes réalisés à l'étranger étant régis par la loi de l'Etat requis, leur validité ne peut pas être appréciée au regard des dispositions de la loi française. Néanmoins, la Cour de cassation admet un contrôle minimum dont l'objet n'est pas d'examiner si les dispositions techniques de l'une ou l'autre des législations en présence ont été respectées, mais de s'assurer que *"les actes n'ont pas été accomplis en violation des droits de la défense, ni d'aucun principe général du droit"* (Crim. 4 novembre 1997, bull. n° 366).

Concernant la poursuite ou l'activation d'une géolocalisation en temps réel en dehors des frontières du territoire national, la Cour de cassation a pu estimer que les éléments recueillis ne peuvent être exploités en procédure que si la mesure de géolocalisation a été autorisée préalablement ou concomitamment par l'Etat concerné, ou que celui-ci a, postérieurement à la mesure, autorisé son exploitation, en exécution d'une demande d'entraide pénale (Crim. 9 février 2016).

➔ **La protection des personnes ayant permis l'installation d'un moyen de géolocalisation (décret d'application du 29 juin 2016)**

Afin de garantir l'anonymat des personnes ayant aidé les services enquêteurs à installer un dispositif de géolocalisation dans le cadre d'une information judiciaire relative à l'une des infractions relevant de la criminalité organisée, le JLD peut autoriser, sur saisine du juge d'instruction, après avis du procureur de la République, la consignation dans un dossier distinct des éléments suivants qui n'apparaîtront pas dans le dossier de la procédure:

- la date, l'heure et le lieu où le moyen technique a été installé ou retiré ;
- les éléments permettant l'identification de la personne ayant concouru à l'installation ou au retrait du moyen technique.

La requête du juge d'instruction doit:

- être motivée et préciser les raisons justifiant la création d'un dossier secret (les informations qui y seront consignées sont susceptibles de mettre gravement en danger la personne ou ses proches ; ces informations ne sont ni utiles à la manifestation de la vérité, ni indispensables à l'exercice des droits de la défense).
- comporter la liste des pièces devant y figurer.

La décision du JLD autorisant le versement de certaines pièces dans un dossier distinct est jointe à la procédure.

Dans le dossier distinct figurent le procès-verbal mentionnant les informations devant rester secrètes, ainsi que la requête du juge d'instruction.

Le dossier distinct et le registre[4] sont conservés par le président du TGI ou le juge délégué par lui. Ils ne peuvent être communiqués qu'au JLD, au juge d'instruction, à la chambre de l'instruction et, lorsque la

[4] Les informations sont également inscrites sur un registre côté et paraphé.

personne mise en examen ou le témoin assisté conteste le recours à la procédure du dossier distinct[5], au président de la chambre de l'instruction.

[5] Conformément aux dispositions de l'article 230-41 du CPP, la personne mise en examen ou le témoin assisté peut contester devant le président de la chambre d'instruction le recours à cette procédure ;

FICHE TECHNIQUE

# SONORISATION ET CAPTATION D'IMAGE
# Dans le cadre d'une enquête dirigée par le parquet

## Définition juridique

L'article **706-96** du code de procédure pénale introduit par la loi du 3 juin 2016 offre désormais la possibilité au procureur de la République de recourir aux dispositifs de sonorisation ou de captation d'images, sur autorisation du juge des libertés et de la détention, dans le cadre des enquêtes relevant de la criminalité organisée, portant sur les infractions visées par les articles 706-73 et 706-73-1 du code de procédure pénale.

➔ **La sonorisation** consiste à mettre en place un dispositif technique ayant pour objet de capter, fixer, transmettre et enregistrer, sans le consentement du ou des intéressés, leurs **paroles** prononcées à titre privé ou confidentiel, dans des **lieux ou véhicules privés ou publics.**

N'entrent pas dans le champ d'application de cette technique d'enquête, les enregistrements sonores réalisés par un particulier, lesquels ne constituent pas des actes de procédure (au sens de l'article 170 du code de procédure pénale) dès lors qu'ils n'émanent pas d'un magistrat ou d'un service d'enquête, mais des moyens de preuve qui peuvent être discutés contradictoirement (*Crim. 7 mars 2012*).

➔ **La captation d'image** vise la mise en place d'un dispositif technique ayant pour objet de capter, fixer, transmettre et enregistrer, sans le consentement de la ou des personnes concernées, leurs **images** alors qu'elles se trouvent dans un **lieu privé**.

Doivent ainsi être réalisées dans le respect des dispositions des articles 706-96 et suivants du code de procédure pénale :

- les photographies réalisées par un enquêteur de véhicules situés dans une propriété privée non visibles depuis la voie publique *(Crim. 21 mars 2007)* ou de personnes se trouvant à l'intérieur d'une propriété privée close à partir de points hauts situés à l'extérieur de ladite propriété *(Crim. 25 juin 2014)* ;
- l'installation et l'utilisation par un enquêteur d'un dispositif de captation d'images dans les parties communes d'une copropriété (en l'espèce un parking souterrain assimilé à un lieu privé) *(Crim. 27 mai 2009)* ;
- l'utilisation par un enquêteur d'un endoscope permettant d'observer l'intérieur d'un box fermé (*Crim. 23 janvier 2013*).

N'entrent pas dans le champ d'application de cette technique d'enquête car relèvent des pouvoirs généraux d'investigation :

- la photographie de véhicules situés dans une propriété privée visible depuis la voie publique *(Crim. 15 avril 2015) ;*
- l'exploitation des enregistrements d'une vidéosurveillance installée par le propriétaire dans les parties communes de son immeuble *(Crim. 6 mars 2013)* ;
- les constatations visuelles réalisées par un enquêteur après s'être régulièrement introduit dans un parking souterrain avec l'accord d'une personne titulaire d'un droit d'accès (*Crim. 23 octobre 2013*);
- les constatations visuelles effectuées par un enquêteur au sujet de personnes se trouvant à l'intérieur d'une propriété privée close, observées à partir de points hauts situés à l'extérieur de ladite propriété (*Crim. 25 juin 2014*).

La jurisprudence a ainsi précisé les notions de :

- dispositif technique, comme étant celui permettant de capter des images qui ne sont pas accessibles, visibles à l'œil nu ;
- lieu privé, incluant les parties communes d'une copropriété ;

➔ **Le respect du principe de loyauté des preuves.** Les sonorisations ou captations d'images ne doivent pas s'inscrire dans le cadre de stratagèmes.

A ainsi été considérée comme irrégulière la sonorisation, en dehors du cadre d'audition, de deux personnes placées en garde à vue dans des cellules contiguës (*communiqué de la Cour de cassation en date du 6 mars 2015*).

En revanche, ont été considérées comme régulières la sonorisation d'un parloir de prison (*Crim, 1er mars 2006*) et la sonorisation d'une cellule occupée par deux individus mis en examen dans le cadre d'une même information judiciaire dès lors que la détention commune de ces deux personnes n'avait pas été provoquée mais relevait du choix du détenu et du profil similaire que présentait les deux mis en examen *(Crim. 17 mars 2015)***.**

## Conditions d'autorisation

Un OPJ ou un APJ ne peut procéder à une sonorisation ou une captation d'images qu'après y avoir été **autorisé par ordonnance du juge des libertés et de la détention**, saisi par requête du procureur de la République.

➔ **Conditions de fond**

L'acte de sonorisation ou de captation d'images doit être effectué pour les « nécessités » de l'enquête, dans le cadre d'une procédure visant au moins une qualification des articles 706-73 ou de 706-73-1 du code de procédure pénale.

➔ **Conditions de forme**

L'autorisation du juge des libertés et de la détention concerne de manière alternative ou cumulative les dispositifs de sonorisation et de captation d'images.
Elle doit être délivrée par ordonnance écrite et motivée « *au regard des éléments précis et circonstanciés résultant de la procédure* » (*Crim. 6 janvier 2015*).
Elle doit comporter les éléments permettant d'identifier les véhicules ou lieux visés, la durée de la mesure ainsi que la ou les infractions motivant l'acte.

Il convient de préciser que la révélation au cours de ces opérations d'autres infractions que celles visées dans l'autorisation du juge des libertés et de la détention, ne constitue par une cause de nullité des procédures incidentes.

➔ **Durée de la mesure**

En vertu de l'article 706-98 du code de procédure pénale, la durée d'autorisation (maximale) est de 1 mois, renouvelable une fois dans les mêmes conditions.
Le point de départ de la mesure de sonorisation ou de captation d'images doit être fixé au jour de sa mise en place effective (le jour de l'installation du dispositif) et non à la date de l'autorisation du juge des libertés et de la détention. Le renouvellement de l'autorisation doit nécessairement intervenir avant l'expiration de la mesure précédente *(Crim 13 nov. 2008).*

➔ **Introduction dans les lieux privés**

Afin de mettre en place le dispositif technique de sonorisation et/ou de captation d'images, le juge des libertés et de la détention peut autoriser l'OPJ ou l'APJ à s'introduire dans un véhicule ou dans un lieu privé, y compris en dehors des heures prévues à l'article 59 du code de procédure pénale, et ce à l'insu du propriétaire, du possesseur ou de l'occupant.

Dans cette hypothèse, le procureur de la République sera amené à solliciter dans sa requête une double autorisation, et le juge des libertés et de la détention à se prononcer expressément sur les deux autorisations.

Cette introduction dans un lieu privé doit avoir pour seule finalité la mise en place du dispositif technique.

Toutefois, l'OPJ ou l'APJ peut dresser un procès-verbal relatant les constatations réalisées lors de l'installation du dispositif technique à l'intérieur du véhicule ou du lieu privé, dès lors qu'il se contente de transcrire ses constatations visuelles, sans procéder à aucune recherche et sans effectuer de photographies (*Crim 23 janvier 2013*).

➔ **Lieux prohibés**

Il ne peut être mis en place de dispositif technique de sonorisation ou de captation d'images dans les lieux suivants :

- le cabinet ou le domicile d'un avocat (56-1 du CPP) ;
- les locaux et véhicules d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne ou d'une agence de presse, ou encore le domicile d'un journaliste (56-2 du CPP) ;
- le cabinet d'un médecin, notaire, huissier (56-3 du CPP) ;
- les locaux d'une juridiction ou le domicile d'une personne exerçant des fonctions juridictionnelles (magistrat professionnel ou non professionnel) (56-5 du CPP) ;
- le véhicule, le bureau ou le domicile d'un député, d'un sénateur ou d'un avocat (100-7 du CPP).

## Mise en œuvre des mesures

➔ **Formalisme des opérations**

En vertu de l'article 706-100 du code de procédure pénale, le procureur de la République ou l'OPJ doit dresser un procès-verbal pour chaque opération de mise en place d'un dispositif technique de sonorisation ou de captation d'image, en mentionnant la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée. Les enregistrements ainsi réalisés doivent être placés sous scellés fermés (ce qui suppose un procès-verbal de placement sous scellés).

En vertu de l'article 706-101 du code de procédure pénale, le procureur de la République ou l'OPJ décrit ou transcrit, dans un procès-verbal qui est versé au dossier, les images ou les conversations enregistrées qui sont utiles à la manifestation de la vérité. Aucune séquence relative à la vie privée étrangère aux infractions visées dans la décision autorisant la mesure ne peut être conservée dans le dossier de la procédure *(conformément à la décision du conseil constitutionnel du 2 mars 2004).*

➔ **Conservation des scellés**

Les enquêteurs ne doivent pas conserver, après l'exécution de leur mission, une copie des enregistrements effectués à l'occasion d'une mesure de sonorisation (*Crim 8 juillet 2015 : arrêt concernant une mesure ordonnée dans le cadre d'une instruction, mais motivé par l'obligation – applicable à tout cadre d'enquête - de placer les enregistrements sous scellé fermé*).

En vertu de l'article 706-102 du code de procédure pénale, les enregistrements sonores ou audiovisuels doivent être détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il doit être dressé procès-verbal de cette opération de destruction.

➔ **Agents et services habilités (art.706-99 du code de procédure pénale)**

Les services, unités et organismes, visés à l'article 706-99 du code de procédure pénale, pouvant procéder aux opérations d'installation des dispositifs techniques mentionnés à l'article 706-96 sont précisés à l'article D.15-1-5 du code de procédure pénale :
- la direction centrale de la police judiciaire et ses directions interrégionales et régionales ;
- la direction générale de la sécurité intérieure ;
- les offices centraux de police judiciaire ;
- la force d'intervention de la police nationale ;
- la sous-direction de la police judiciaire de la gendarmerie nationale ;
- les sections de recherches de la gendarmerie nationale ;
- le groupe d'intervention de la gendarmerie nationale ;

- les sections d'appui judiciaire de la gendarmerie nationale ;
- les pelotons d'intervention interrégionaux de la gendarmerie nationale ;
- les groupes de pelotons d'intervention de la gendarmerie nationale ;
- le service chargé du soutien opérationnel et technique de la direction du renseignement de la préfecture de police ;
- les services et unités de la direction opérationnelle des services techniques et logistiques de la préfecture de police.

Les agents ainsi habilités sont autorisés à détenir des appareils ou dispositifs techniques permettant de procéder à la sonorisation ou la captation d'image sans le consentement des personnes concernées (*Faits prévus et réprimés par l'article 226-3 du code pénal*).

➔ **Poursuite de la sonorisation en dehors des frontières du territoire national :**

Si la poursuite transfrontalière d'une mesure de sonorisation prévue par l'article 706-96 du code de procédure pénale n'est pas spécifiquement encadrée par les instruments conventionnels régissant l'entraide judiciaire, ni par les dispositions du code de procédure pénale, les dispositions encadrant la mise en œuvre des mesures de géolocalisation en dehors des frontières du territoire national, moins attentatoires aux libertés individuelles que les sonorisations, paraissent applicables lorsqu'est envisagée la poursuite transfrontalière d'une sonorisation de véhicule.

Ainsi, il apparaît nécessaire d'émettre une demande d'entraide pénale internationale qui sera exécutée selon la loi de l'Etat requis.

Le contrôle de la régularité d'un tel acte exécuté au regard de la loi du for est assuré par les autorités du for - c'est-à-dire les autorités étrangères.

Les actes réalisés à l'étranger étant régis par la loi de l'Etat requis, leur validité ne peut pas être appréciée au regard des dispositions de la loi française. Néanmoins, la Cour de cassation admet un contrôle minimum dont l'objet n'est pas d'examiner si les dispositions techniques de l'une ou l'autre des législations en présence ont été respectées, mais de s'assurer que *"les actes n'ont pas été accomplis en violation des droits de la défense, ni d'aucun principe général du droit"* (Crim. 4 novembre 1997, bull. n° 366).

Concernant la poursuite ou l'activation d'une géolocalisation en temps réel en dehors des frontières du territoire national, la Cour de cassation a pu estimer que les éléments recueillis ne peuvent être exploités en procédure que si la mesure de géolocalisation a été autorisée préalablement ou concomitamment par l'Etat concerné, ou que celui-ci a, postérieurement à la mesure, autorisé son exploitation, en exécution d'une demande d'entraide pénale (Crim. 9 février 2016).

FICHE TECHNIQUE

# SONORISATION ET CAPTATION D'IMAGE
# Dans le cadre d'une information judiciaire

## Définition juridique

L'article **706-96-1** du code de procédure pénale introduit par la loi du 3 juin 2016 reprend les dispositions de l'ancien article 706-96 du code de procédure pénale issu de la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité ayant consacré le recours aux dispositifs de sonorisation et de captation d'images par le juge d'instruction.

➔ **La sonorisation** consiste à mettre en place un dispositif technique ayant pour objet de capter, fixer, transmettre et enregistrer, sans le consentement du ou des intéressés, leurs **paroles** prononcées à titre privé ou confidentiel, dans des **lieux ou véhicules privés ou publics.**

N'entrent pas dans le champ d'application de cette technique d'enquête, les enregistrements sonores réalisés par un particulier, lesquels ne constituent pas des actes de procédure (au sens de l'article 170 du code de procédure pénale) dès lors qu'ils n'émanent pas d'un magistrat ou d'un service d'enquête, mais des moyens de preuve qui peuvent être discutés contradictoirement (*Crim. 7 mars 2012*).

➔ **La captation d'image** vise la mise en place d'un dispositif technique ayant pour objet de capter, fixer, transmettre et enregistrer, sans le consentement du ou des personnes concernées, leurs **images** alors qu'elles se trouvent dans un **lieu privé**.

Doivent ainsi être réalisés dans le respect des dispositions des articles 706-96 et suivants du code de procédure pénale :

- les photographies réalisées par un enquêteur de véhicules situés dans une propriété privée non visibles depuis la voie publique *(Crim. 21 mars 2007)* ou de personnes se trouvant à l'intérieur d'une propriété privée close à partir de points hauts situés à l'extérieur de ladite propriété *(Crim. 25 juin 2014)* ;
- l'utilisation par un enquêteur d'un dispositif de captation d'images dans les parties communes d'une copropriété (en l'espèce un parking souterrain assimilé à un lieu privé) *(Crim. 27 mai 2009)* ;
- l'utilisation par un enquêteur d'un endoscope permettant d'observer l'intérieur d'un box fermé (*Crim. 23 janvier 2013*).

N'entrent pas dans le champ d'application de cette technique d'enquête car relèvent des pouvoirs généraux d'investigation :

- la photographie de véhicules situés dans une propriété privée visible depuis la voie publique *(Crim. 15 avril 2015) ;*
- l'exploitation des enregistrements d'une vidéosurveillance installée par le propriétaire dans les parties communes de son immeuble *(Crim. 6 mars 2013)* ;
- les constatations visuelles réalisées par un enquêteur après s'être régulièrement introduit dans un parking souterrain avec l'accord d'une personne titulaire d'un droit d'accès (*Crim. 23 octobre 2013*);
- les constatations visuelles effectuées par un enquêteur au sujet de personnes se trouvant à l'intérieur d'une propriété privée close, observées à partir de points hauts situés à l'extérieur de ladite propriété (*Crim. 25 juin 2014*).

La jurisprudence a ainsi précisé les notions de :

- dispositif technique, comme étant celui permettant de capter des images qui ne sont pas accessibles, visibles à l'œil nu ;
- lieu privé, incluant les parties communes d'une copropriété ;

➔ **Le respect du principe de loyauté des preuves.** Les sonorisations ou captations d'images ne doivent pas s'inscrire dans le cadre de stratagèmes.

A ainsi été considérée comme irrégulière la sonorisation, en dehors du cadre d'audition, de deux personnes placées en garde à vue dans des cellules contiguës (*communiqué de la Cour de cassation en date du 6 mars 2015*).

En revanche, ont été considérées comme régulières la sonorisation d'un parloir de prison (*Crim, 1er mars 2006*) et la sonorisation d'une cellule occupée par deux mis en examen dans le cadre d'une information judiciaire ouverte devant le même magistrat instructeur dès lors que la détention de ces deux personnes n'a pas été provoquée mais relevait du choix du détenu et du profil similaire que présentait les deux mis en examen *(Crim. 17 mars 2015).*

## Conditions d'autorisation

Un OPJ ou un APJ ne peut procéder à une sonorisation ou une captation d'images qu'après y avoir été **autorisé par ordonnance du juge d'instruction**.

➔ **Conditions de fond**

L'acte de sonorisation ou de captation d'image doit être effectué pour les « nécessités » de l'instruction, dans le cadre d'une procédure visant au moins une qualification des articles 706-73 ou 706-73-1 du code de procédure pénale.

➔ **Conditions de forme**

L'autorisation du juge d'instruction concerne de manière alternative ou cumulative les dispositifs de sonorisation et de captation d'images.
Elle doit être délivrée, après avis du procureur de la République, par ordonnance écrite et motivée « *au regard des éléments précis et circonstanciés résultant de la procédure* » (*Crim. 6 janvier 2015*).
Elle doit comporter les éléments permettant d'identifier les véhicules ou lieux visés, la durée de la mesure ainsi que la ou les infractions motivant l'acte.

Le juge d'instruction doit délivrer une commission rogatoire spécifique aux OPJ qu'il désigne pour y procéder *(Crim. 13 février 2008).*

➔ **Durée de la mesure**

En vertu de l'article 706-98 du CPP, la durée d'autorisation est de 2 mois, renouvelable dans les mêmes conditions pour une durée totale ne pouvant excéder 2 ans.
Le point de départ de la mesure de sonorisation ou de captation d'images doit être fixé au jour de sa mise en place effective (le jour de l'installation du dispositif) et non à la date de l'autorisation du d'instruction. Le renouvellement de l'autorisation doit nécessairement intervenir avant l'expiration de la mesure précédente *(Crim 13 nov. 2008).*

➔ **Introduction dans les lieux privés**

Afin de mettre en place le dispositif technique de sonorisation et/ou de captation d'images, le juge d'instruction peut autoriser l'OPJ ou l'APJ à s'introduire dans un véhicule ou dans un local privé, y compris en dehors des heures prévues à l'article 59 du code de procédure pénale, et ce à l'insu du propriétaire, du possesseur ou de l'occupant.

S'il s'agit d'un lieu d'habitation, l'autorisation doit être délivrée par le juge des libertés et de la détention.

Cette introduction dans un lieu privé doit avoir pour seule finalité la mise en place du dispositif technique.
Toutefois, l'OPJ ou l'APJ peut dresser un procès-verbal relatant les constatations faites lors de l'installation du dispositif technique à l'intérieur du véhicule ou du local privé, dès lors qu'il se contente de transcrire ses constatations visuelles, sans procéder à aucune recherche et sans effectuer de photographies. (*Crim 23 janvier 2013*).

➔ **Lieux prohibés :**

Il ne peut être mis en place de dispositif technique de sonorisation ou de captation d'image dans les lieux suivants :

- le cabinet ou le domicile d'un avocat (56-1 du CPP) ;
- les locaux et véhicules d'une entreprise de presse, d'une entreprise de communication audiovisuelle, d'une entreprise de communication au public en ligne ou d'une agence de presse, ou encore le domicile d'un journaliste (56-2 du CPP) ;
- le cabinet d'un médecin, notaire, huissier (56-3 du CPP) ;
- les locaux d'une juridiction ou au domicile d'une personne exerçant des fonctions juridictionnelles (magistrat professionnel ou non professionnel) (56-5 du CPP) ;
- le véhicule, le bureau ou le domicile d'un député, d'un sénateur ou d'un avocat (100-7 du CPP).

## Mise en œuvre des mesures

➔ **Formalisme des opérations**

En vertu de l'article 706-100 du CPP, le juge d'instruction ou l'OPJ doit dresser un procès-verbal pour chaque opération de mise en place d'un dispositif technique de sonorisation ou de captation d'image, en mentionnant la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée. Les enregistrements ainsi réalisés doivent être placés sous scellés fermés (ce qui suppose un procès-verbal de placement sous scellés).

En vertu de l'article 706-101 du CPP, le juge d'instruction ou l'OPJ décrit ou transcrit, dans un procès-verbal qui est versé au dossier, les images ou les conversations enregistrées qui sont utiles à la manifestation de la vérité. Aucune séquence relative à la vie privée étrangère aux infractions visées dans la décision autorisant la mesure ne peut être conservée dans le dossier de la procédure *(conformément à la décision du conseil constitutionnel du 2 mars 2004).*

➔ **Conservation des scellés**

Les enquêteurs ne peuvent pas conserver, après l'exécution de leur mission, une copie des enregistrements effectués à l'occasion d'une mesure de sonorisation autorisée par un juge d'instruction (*Crim 8 juillet 2015*).

En vertu de l'article 706-102 du code de procédure pénale, les enregistrements sonores ou audiovisuels doivent être détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique. Il doit être dressé procès-verbal de cette opération de destruction.

➔ **Agents et services habilités (art.706-99 du code de procédure pénale)**

Les services, unités et organismes, visés à l'article 706-99 du code de procédure pénale, pouvant procéder aux opérations d'installation des dispositifs techniques mentionnés à l'article 706-96 sont précisés à l'article D.15-1-5 du code de procédure pénale :
- la direction centrale de la police judiciaire et ses directions interrégionales et régionales ;
- la direction générale de la sécurité intérieure ;
- les offices centraux de police judiciaire ;
- la force d'intervention de la police nationale ;
- la sous-direction de la police judiciaire de la gendarmerie nationale ;
- les sections de recherches de la gendarmerie nationale ;
- le groupe d'intervention de la gendarmerie nationale ;
- les sections d'appui judiciaire de la gendarmerie nationale ;
- les pelotons d'intervention interrégionaux de la gendarmerie nationale ;
- les groupes de pelotons d'intervention de la gendarmerie nationale ;
- le service chargé du soutien opérationnel et technique de la direction du renseignement de la préfecture de police ;

- les services et unités de la direction opérationnelle des services techniques et logistiques de la préfecture de police.

Les agents ainsi habilités sont autorisés à détenir des appareils ou dispositifs techniques permettant de procéder à la sonorisation ou la captation d'image sans le consentement des personnes concernées (*Faits prévus et réprimés par l'article 226-3 du code pénal*).

➔ **Poursuite de la sonorisation en dehors des frontières du territoire national :**

Si la poursuite transfrontalière d'une mesure de sonorisation prévue par l'article 706-96 du code de procédure pénale n'est pas spécifiquement encadrée par les instruments conventionnels régissant l'entraide judiciaire, ni par les dispositions du code de procédure pénale, les dispositions encadrant la mise en œuvre des mesures de géolocalisation en dehors des frontières du territoire national, moins attentatoires aux libertés individuelles que les sonorisations, paraissent applicables lorsqu'est envisagée la poursuite transfrontalière d'une sonorisation de véhicule.

Ainsi, il apparaît nécessaire d'émettre une demande d'entraide pénale internationale qui sera exécutée selon la loi de l'Etat requis.

Le contrôle de la régularité d'un tel acte exécuté au regard de la loi du for est assuré par les autorités du for - c'est-à-dire les autorités étrangères.

Les actes réalisés à l'étranger étant régis par la loi de l'Etat requis, leur validité ne peut pas être appréciée au regard des dispositions de la loi française. Néanmoins, la Cour de cassation admet un contrôle minimum dont l'objet n'est pas d'examiner si les dispositions techniques de l'une ou l'autre des législations en présence ont été respectées, mais de s'assurer que *"les actes n'ont pas été accomplis en violation des droits de la défense, ni d'aucun principe général du droit"* (Crim. 4 novembre 1997, bull. n° 366).

Concernant la poursuite ou l'activation d'une géolocalisation en temps réel en dehors des frontières du territoire national, la Cour de cassation a pu estimer que les éléments recueillis ne peuvent être exploités en procédure que si la mesure de géolocalisation a été autorisée préalablement ou concomitamment par l'Etat concerné, ou que celui-ci a, postérieurement à la mesure, autorisé son exploitation, en exécution d'une demande d'entraide pénale (Crim. 9 février 2016).

# L'IMSI CATCHER

## Présentation du dispositif technique

L'IMSI-catcher est un dispositif de proximité permettant d'obtenir des données difficilement accessibles par le recours classique à de simples réquisitions téléphoniques.

Imitant le fonctionnement d'une antenne-relais, l'IMSI-catcher provoque la connexion des téléphones mobiles situés à proximité et déjoue l'utilisation désormais régulière par les mis en cause de téléphones multiples à usage unique (« téléphones de guerre »).

Ce moyen permet:

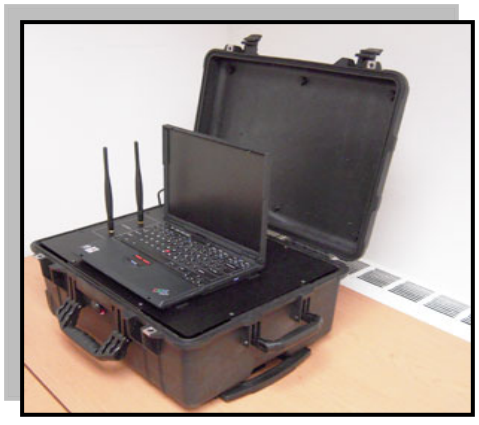
- d'identifier les équipements terminaux et de recueillir les données techniques (numéros IMSI et IMEI) ;
- de localiser efficacement les détenteurs de ces équipements lors de missions de surveillance ;
- de mettre en œuvre en urgence des interceptions judiciaires.

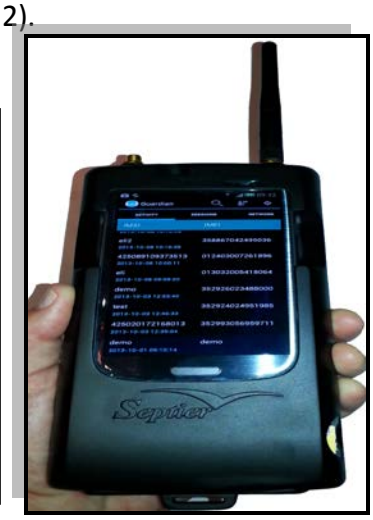
On distinguera donc le dispositif **IMSI-catcher aux fins de recueil de données techniques** du dispositif IMSI-catcher **aux fins d'interceptions de communications**.

En pratique, les enquêteurs pourront utiliser ce dispositif pour récupérer les numéros de lignes téléphoniques ou numéros de boitiers téléphoniques de leurs objectifs, à distance, sans qu'il leur soit nécessaire d'avoir un accès direct au support physique. L'IMSI-catcher aura également vocation à permettre de localiser efficacement les détenteurs de ces équipements lors de mission de surveillance.

Trois types de matériels sont mis à la disposition des enquêteurs. Ces derniers peuvent utiliser les dispositifs suivants :

- un matériel puissant ayant vocation à être intégré dans un véhicule permettant de couvrir simultanément toutes les fréquences de tous les opérateurs ;
- un dispositif « portatif » mais encombrant doté d'une portée plus faible, susceptible d'être transporté en dehors du véhicule des enquêteurs (figure 1);
- un appareil mobile aisément transportable (« pocket ») pouvant par exemple couvrir l'intérieur d'une salle (figure 2).





## Cadre légal

Les articles 706-95-4 à 706-95-10 du code de procédure pénale introduits par la loi du 3 juin 2016 instaurent un régime juridique encadrant l'utilisation de l'IMSI-catcher dans le cadre des enquêtes relevant de la criminalité organisée, portant sur les infractions visées par les articles 706-73 et 706-73-1 du code de procédure pénale. Hors cette liste d'infractions, le recours à l'IMSI-catcher n'est pas possible.

Si le législateur a entendu restreindre le recours à l'IMSI-catcher à certaines infractions limitativement énumérées, il en favorise l'utilisation quel que soit le cadre des investigations. Il est en effet possible d'y recourir tant dans le cadre des enquêtes conduites par le procureur de la République qu'au cours d'une information judiciaire.

Aux spécificités liées à ces deux cadres juridiques distincts, s'ajoutent des particularités tenant aux finalités de l'IMSI-catcher, lequel vise soit le recueil de données techniques, soit l'interception des communications.

## Le recours à l'IMSI-catcher dans le cadre des « enquêtes parquet »

➔ **Sur autorisation du juge des libertés et de la détention saisi par requête du procureur de la République**

Le recueil des données de connexion ou des données relatives à la géolocalisation est autorisé pour une période d'un mois renouvelable une fois. Ce procédé permet d'identifier ou localiser un équipement terminal ainsi que le numéro d'abonnement de son utilisateur.

L'officier de police judiciaire dresse un procès-verbal mentionnant la date et l'heure de début et de fin de ces opérations. Seules les données utiles à la manifestation de la vérité sont jointes au procès-verbal. Les données recueillies à l'aide des IMSI-catchers sont détruites, à l'expiration du délai de prescription de l'action publique ou lorsqu'une décision définitive a été rendue au fond.

L'interception des communications par IMSI-catcher ne peut concerner que la personne ou la liaison visée par l'autorisation, laquelle est accordée pour une durée de 48 heures renouvelable une fois.

L'OPJ mentionne sur procès-verbal la date, l'heure de début et de fin de chaque interception et enregistrement. Seules les correspondances utiles à la manifestation de la vérité doivent être retranscrites. Les enregistrements sont placés sous scellés fermés avant destruction, constatée par procès-verbal, à l'expiration du délai de prescription de l'action publique.

➔ **En cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens**

Le procureur de la République peut autoriser pour 24 heures le recours à l'IMSI-catcher, tant pour recueillir les données de connexion que pour intercepter des correspondances.

Cette autorisation du procureur de la République doit comporter l'énoncé des circonstances de fait établissant l'existence du risque imminent et être confirmée par le juge des libertés et de la détention dans un délai maximal de vingt-quatre heures. A défaut, il est mis fin à l'opération, les données ou correspondances recueillies sont placées sous scellés fermés et elles ne peuvent pas être exploitées ou utilisées dans la procédure.

Dans tous les cas de figure évoqués ci-dessus, les autorisations délivrées par le juge des libertés et de la détention font l'objet d'une ordonnance écrite et motivée[1]. Cette ordonnance n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours. Le juge des libertés et de la détention qui a délivré ou confirmé une autorisation est informé dans les meilleurs délais par le procureur de la République des actes accomplis et des procès-verbaux dressés en exécution de son autorisation.

## Le recours à l'IMSI-catcher dans le cadre des informations judiciaires

Les autorisations délivrées par le juge d'instruction font l'objet d'une ordonnance écrite et motivée. L'ordonnance du juge des libertés et de la détention ou du magistrat instructeur doit notamment préciser tout élément de contexte, relever les éléments d'identification des personnes visées ou déterminer des lieux susceptibles d'être fréquentés par les individus ciblés.
L'ordonnance n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

➔ **Le recueil des données de connexion ou de données relatives à la géolocalisation** d'un équipement terminal ou d'un numéro d'abonnement, est autorisé par le magistrat instructeur pour une période de deux mois renouvelable dans la limite de 6 mois.

L'officier de police judiciaire dresse un procès-verbal mentionnant la date et l'heure de début et de fin de ces opérations. Seules les données utiles à la manifestation de la vérité sont jointes au procès-verbal. Les données recueillies à l'aide des IMSI-catchers sont détruites, à l'expiration du délai de prescription de l'action publique ou lorsqu'une décision définitive a été rendue au fond.

➔ **L'interception des correspondances par IMSI-catcher** sont autorisées par le magistrat instructeur pour une durée de 48 heures renouvelable une fois. Ces opérations ne concernent que la personne ou la liaison visée par l'autorisation.

L'OPJ mentionne sur procès-verbal la date, l'heure de début et de fin de chaque interception et enregistrement. Seules les correspondances utiles à la manifestation de la vérité doivent être retranscrites. Les enregistrements sont placés sous scellés fermés avant destruction, constatée par procès-verbal, à l'expiration du délai de prescription de l'action publique.

## L'utilisation du dispositif par un agent qualifié

Au terme de l'article 706-95-8 du code de procédure pénale, le procureur de la République, le juge d'instruction ou l'officier de police judiciaire peut requérir tout agent qualifié d'un service, d'une unité ou d'un organisme placé sous l'autorité du ministre de l'intérieur et dont la liste est fixée par décret.

**Décret n° 2016-1159 du 26 août 2016 pris pour l'application de l'article 706-95-8 du code de procédure pénale.**

Les services, unités et organismes mentionnés à l'article 706-95-8, dont les agents peuvent être requis en vue de procéder à l'utilisation de l'appareil ou du dispositif technique mentionné aux articles 706-95-4 et 706-95-5, sont les suivants :

«-la direction centrale de la police judiciaire et ses directions interrégionales et régionales ;
«-la direction générale de la sécurité intérieure ;
«-la force d'intervention de la police nationale ;

[1] ~~et~~[1] L'ordonnance du juge des libertés et de la détention ou du magistrat instructeur doit notamment préciser tout élément de contexte, relever les éléments d'identification des personnes visées ou déterminer des lieux susceptibles d'être fréquentés par les individus ciblés.

«-le groupe d'intervention de la gendarmerie nationale ;
«-le groupe d'observation et de surveillance de la région de gendarmerie d'Ile-de-France ;
«-le groupe d'observation et de surveillance de la région de gendarmerie de Provence-Alpes-Côte d'Azur ;
«-le service chargé du soutien opérationnel et technique de la direction du renseignement de la préfecture de police ;
«-les services et unités de la direction opérationnelle des services techniques et logistiques de la préfecture de police.

FICHE TECHNIQUE

# L'ENQUETE SOUS PSEUDONYME

## Cadre légal

**Textes applicables** :

- articles 706-2-2, 706-35-1, 706-47-3 et 706-87-1 du code de procédure pénale ;
- article 59 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ;
- articles 67 bis-1 A et 67 bis-1 3° du code des douanes.

Circulaires et dépêches :

- circulaire DACG-DGPN-DGGN du 22 mars 2010 relative aux investigations sous pseudonyme sur Internet et au rôle du centre national d'analyse des images de pédopornographie ;
- circulaire DACG du 10 septembre 2013 relative aux investigations sous pseudonyme par voie d'échanges électroniques en matière de provocation et d'apologie des actes de terrorisme ;
- circulaire DACG du 5 décembre 2014 de présentation de la loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme - Renforcement de la coordination de la lutte antiterroriste ;
- circulaire DACG du 16 décembre 2014 de présentation des dispositions de l'ordonnance n°2013-1183 du 19 décembre 2013 relative à l'harmonisation des sanctions pénales et financières relatives aux produits de santé et à l'adaptation des prérogatives des autorités et des agents chargés de constater les manquements, et des textes pris pour son application ;
- dépêche du 21 décembre 2015 de présentation de l'arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme.

La loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance puis la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) ont introduit dans le code de procédure pénale des dispositions (articles 706-25-2[1], 706-35-1 et 706-47-3) autorisant les enquêteurs à procéder à des investigations sous pseudonyme sur internet pour des infractions limitativement énumérées (cyberpatrouilles).

L'ordonnance n°2013-1183 du 19 décembre 2013 relative à l'harmonisation des sanctions pénales et financière relatives aux produits de santé et à l'adaptation des prérogatives des autorités et des agents chargés de constater les manquements a étendu le recours aux « cyberpatrouilles » dans le cadre de certaines infractions prévues par le code de la santé publique et le code de la consommation (article 706-2-2 CPP).

[1] Cet article a été abrogé par la loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

La loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme, a **généralisé ce dispositif à l'ensemble des crimes et délits relevant de la criminalité organisée et prévus aux articles 706-72 et 706-73 du CPP, lorsqu'ils ont été commis par un moyen de communication informatique**, en insérant dans le code de procédure pénale un nouvel article 706-87-1.

La loi n°2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne a créé un nouvel article 706-73-1 du CPP, auquel renvoie l'article 706-87-1. Cet article modifié par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale dresse une liste d'infractions pour lesquelles les règles procédurales applicables aux infractions relevant de la criminalité organisée (à l'exception de celles relatives à la garde à vue), dont l'enquête sous pseudonyme, sont applicables.

La loi n° 2016-731 du 3 juin 2016 précité a par ailleurs étendu la liste des infractions pour la constatation desquelles les agents des douanes peuvent recourir à l'enquête sous pseudonyme (article 67 bis-1 A du code des douanes).

## Champ d'application

### 1. Les infractions susceptibles d'être constatées par les cyberpatrouilleurs

Seules peuvent être constatées par les cyberpatrouilleurs, lorsqu'elles sont commises par un moyen de communication électronique les infractions en matière :

- de **traite des êtres humains**[2] et de **proxénétisme**[3] **lorsqu'elles ne relèvent pas de la criminalité organisée** et de **recours à la prostitution d'un mineur ou d'une personne vulnérable** [4] (article 706-35-1 CPP);
- d'**atteintes aux mineurs** mentionnées aux articles 227-18 à 227-24 du code pénal [5] (article 706-47-3 CPP) ;
- d'infractions relevant de la **criminalité organisée** - en ce compris les **délits d'apologie et de provocation au terrorisme prévus par l'article 421-2-5 du code pénal** - mentionnées aux articles 706-72, 706-73 et 706-73-1 du code de procédure pénales (article 706-87-1 CPP) ;
- de **produits de santé** [6] (article 706-2-2 CPP) ;

[2] Articles 225-4-1, 225-4-8 et 225-4-9 du code pénal.
[3] Articles 225-5 et 225-6 du code pénal.
[4] Article 225-12-1 et 225-12-2 du code pénal.
[5] Provocations envers un mineur à commettre une infraction relative aux produits stupéfiants ou à la consommation habituelle et excessive de boissons alcooliques ; provocation envers un mineur à commettre un crime ou un délit ; corruption de mineur ; infractions relatives à la pédopornographie ; fabrication, transport, diffusion de message à caractère violent, pornographique, incitant au terrorisme, portant gravement atteinte à la dignité humaine ou incitant des mineurs à se livrer à des jeux les mettant physiquement en danger.
[6] Articles L. 5421-2 (infractions liées aux médicaments, spécialités pharmaceutiques, générateurs, trousses ou précurseurs non autorisés) L. 5421-3 (infractions liées aux médicaments homéopathiques ou aux médicaments traditionnels à base de plante non enregistrés), L. 5421-13 (infractions liées aux médicaments falsifiés), L. 5426-1 (infractions liées aux préparations de thérapie génique et préparations de thérapie cellulaire xénogénique), L. 5432-1 (infractions, dans le cadre d'une activité réglementée, liées aux médicaments, plantes, substances ou préparations classées comme vénéneuses), L. 5432-2 (infractions, dans le cadre d'une activité réglementée, liées aux médicaments, plantes, substances ou préparations classées comme psychotropes), L. 5438-4 (infractions liées aux matières premières à usage pharmaceutique falsifiées), L. 5439-1 (infractions liées aux micro-organismes et toxines ou produits

- de **sites de jeux d'argent** [7] (article 59 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne) ;
- d'importation, d'exportation ou de détention illicite de **produits stupéfiants, de tabac manufacturé, d'armes ou de leurs éléments, de munitions ou d'explosifs et de marchandises contrefaisantes**, dans le cadre du code des douanes et uniquement en vue de l'acquisition de l'un de ces produits (coup d'achat) (article 67 bis-1 3° du code des douanes) ;
- de **contrebande, importation ou exportation sans déclaration de marchandises prohibées ou fortement taxées**[8], de **blanchiment douanier**[9], d'**infractions à la législation et à la réglementation des relations financières avec l'étranger**[10] (article 67 bis-1 A du code des douanes).

## 2. Les actes pouvant être réalisés par les cyberpatrouilleurs

Agissant dans le cadre d'une enquête ou sur commission rogatoire, les enquêteurs peuvent réaliser les actes suivants :

1° Participer sous un pseudonyme aux **échanges électroniques** ;

2° Etre **en contact par le moyen mentionné au 1° avec les personnes susceptibles d'être les auteurs** de ces infractions ;

3° **Extraire, acquérir ou conserver** par ce moyen les éléments de preuve et les données sur les personnes susceptibles d'être les auteurs de ces infractions ;

4° Extraire, transmettre **en réponse à une demande expresse**, acquérir ou conserver des contenus illicites, dans des conditions fixées par décret[11] (sauf en matière de produits de santé - article 706-2-2 CPP - et pour les investigations réalisées dans le cadre de l'article 67 bis-1 A du code des douanes).

Ces actes ne peuvent, à peine de nullité, constituer une **incitation à la commission d'une infraction**.

Les pseudonymes utilisés par les cyberpatrouilleurs sont préalablement déclarés au service interministériel d'assistance technique (SIAT) de la direction centrale de la police judiciaire qui en assure la centralisation.

Dans le cas où les cyberpatrouilleurs sont amenés pour les nécessités de l'enquête, à **acquérir des contenus illicites**, ils adressent au SIAT les demandes **de moyen de paiement**. Ce service examine leur recevabilité et fournit le cas échéant un support de paiement.

---

en contenant), L. 5451-1 (non-respect des décisions de l'agence nationale de sécurité du médicament et des produits de santé), L. 5461-3 (infractions liées aux dispositifs médicaux) et L. 5462-3 (infractions liées aux dispositifs médicaux de diagnostic in vitro) du code de la santé publique et article L. 213-1 du code de la consommation lorsque l'infraction porte sur un des produits mentionnés à l'article L. 5311-1 du code de la santé publique (tromperie sur les produits à finalité sanitaire destinés à l'homme ou les produits à finalité cosmétique).

[7] Offre en ligne de paris ou de jeux d'argent et de hasard illégaux, et publicité pour ces sites (article 56 et 57 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne).

[8] Article 414 du code des douanes.

[9] Article 415 du code des douanes.

[10] Article 459 du code des douanes.

[11] Ce décret n'a pas encore été adopté ; les facultés offertes par les articles 706-35-1, 706-47-3 et 706-87-1 du CPP et 67 bis 1 du code des douanes aux enquêteurs sous pseudonyme ne sont donc pas encore applicables.

## 3. La désignation des cyberpatrouilleurs

L'arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme fixe les conditions d'habilitation des officiers de police judiciaire (OPJ) et agents de police judiciaire (APJ) à procéder à des enquêtes sous pseudonyme.

Ces conditions uniformisées, jusqu'alors fixées par différents arrêtés pris pour l'application de chaque disposition législative, sont désormais **applicables quelles que soient les infractions considérées**[12].

Pour être autorisés à procéder aux actes définis par les articles 706-2-2, 706-35-1, 706-47-3 et 706-87-1 du code de procédure pénale, les OPJ et APJ doivent être cumulativement :

- affectés à l'un des services ou unités limitativement énumérés,
- spécialement habilités à cette fin.

➔ **Les catégories de services ou d'unités susceptibles de procéder à des enquêtes sous pseudonyme**

Les catégories de services de police et d'unités de gendarmerie susceptibles de procéder à des enquêtes sous pseudonyme sont les suivantes :

1. Services et unités relevant de la direction centrale de la police judiciaire :
   - la sous-direction antiterroriste ;
   - la sous-direction de la lutte contre la criminalité organisée et la délinquance organisée ;
   - la sous-direction de la lutte contre la cybercriminalité ;
   - les directions régionales et interrégionales de la police judiciaire.

2. Services et unités relevant de la direction centrale de la sécurité publique :
   - les directions départementales de la sécurité publique ;
   - les sûretés départementales ;
   - les circonscriptions de sécurité publique.

3. Services et unités relevant de la police aux frontières :
   - l'office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre au sein de la sous-direction de l'immigration irrégulière et des services territoriaux ;
   - l'unité de coordination opérationnelle de la lutte contre le trafic et l'exploitation des migrants ;

[12] Néanmoins, en l'absence de procédure spécifique d'habilitation par l'autorité judiciaire, les OPJ et APJ désignés par le ministre de l'intérieur et les agents des douanes désignés par le ministre chargés des douanes, autorisés à réaliser des enquêtes sous pseudonyme relatives aux **jeux d'argent et de hasard en ligne** prévues par l'article 59 de la de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne demeurent régis par l'arrêté d'application du 19 juillet 2010 portant désignation des officiers et agents de police judiciaire autorisés à constater les infractions commises à l'occasion de paris ou de jeux d'argent ou de hasard en ligne.
Il en est de même des agents des douanes agissant dans le cadre des articles 67 bis-1 A et 67 bis-1 du code des douanes, qui sont habilités par le ministre chargé des douanes dans des conditions qui leur sont propres, qui doivent être déterminées par décret.

- les brigades mobiles de recherche ;
- la brigade des chemins de fer.

4. Services et unités relevant de l'inspection générale de la police nationale :
- la division nationale des enquêtes ;
- les délégations de l'inspection générale de la police nationale à Paris, Lille, Lyon, Marseille, Bordeaux, Rennes, Metz et Fort-de-France ;
- le bureau de l'inspection générale de la police nationale à Nice.

5. La direction générale de la sécurité intérieure.

6. Services et unités relevant de la préfecture de police :
- à la direction du renseignement : la sous-direction chargée de la lutte contre l'immigration irrégulière et le travail illégal des étrangers ;
- à la direction régionale de la police judiciaire : la sous-direction des brigades centrales, la sous-direction des affaires économiques et financières et la sous-direction des services territoriaux ;
- à la direction de la sécurité de proximité de l'agglomération parisienne : la sûreté régionale des transports au sein de la sous-direction régionale de la police des transports et les sûretés territoriales au sein des directions territoriales de sécurité de proximité.

7. Services et unités relevant de la direction générale de la gendarmerie nationale :
- la sous-direction de la police judiciaire ;
- le service technique de recherches judiciaires et de documentation ;
- les sections de recherches de la gendarmerie départementale et des gendarmeries spécialisées ;
- les sections d'appui judiciaire ;
- les brigades départementales de renseignements et d'investigations judiciaires ;
- les brigades de renseignements et d'investigations judiciaires de la gendarmerie d'outre-mer et des gendarmeries spécialisées ;
- les brigades de recherches de la gendarmerie départementale et des gendarmeries spécialisées.

8. Services et unités relevant de l'inspection générale de la gendarmerie nationale :
- le bureau des enquêtes judiciaires.

Ces services ou unités peuvent organiser d'initiative des cyberpatrouilles. Ils peuvent également intervenir au profit des autres services et unités de police judiciaire ou être saisis par un magistrat, en vue d'appuyer une enquête en cours, lorsque des actes d'investigation sous pseudonyme sur Internet sont nécessaires.

### ➔ L'habilitation des cyberpatrouilleurs

Peuvent prétendre à être habilités par l'autorité judiciaire les OPJ et APJ bénéficiaires d'une formation spécifique et d'un agrément de leur autorité hiérarchique.