Investigations & Téléphonie Mobile

Le Guide à l'usage des avocats

- Haurus -

Investigations
&
Téléphonie mobile

Le guide à l'usage des avocats

Haurus

L'ensemble des informations citées dans cet ouvrage est accessible au public. Elles sont issues des textes de loi, règlements et décrets en vigueur sur le territoire français.

Cet ouvrage a pour but d'informer un public de professionnels du droit ainsi que toute personne tenant légitimement au respect de sa vie privée.

Aucune partie de ce livre ne peut être reproduite, stockée ou transmise sous quelques formes ou par quelques moyens que ce soit, électroniques, mécaniques, photocopies, enregistrements, numérisations ou autrement sans l'autorisation écrite de l'auteur. Il est illégal de copier ce livre, de l'afficher sur un site Web ou de le distribuer par tout autre moyen sans autorisation.

Tous les noms de marques et noms de produits utilisés pour les besoins du livre et pour sa couverture sont des noms commerciaux, des marques de service, des marques commerciales et des marques déposées de leurs propriétaires respectifs. Les éditeurs et l'auteur ne sont associés à aucun produit ou fournisseur mentionné dans ce livre. Aucune des sociétés référencées dans le livre ne l'a approuvé ou n'a participé à son élaboration.

Copyright © 2021 - Haurus

Tous droits réservés.

ISBN : 9798577095246

Marque éditoriale : Independently Published

À PROPOS DE L'AUTEUR

Je suis Cédric.D, ancien fonctionnaire de police, officier de police judiciaire ayant exercé au sein de la Direction Générale de la Sécurité Intérieure (DGSI). En 2018, je suis mis en cause sous l'alias « Haurus » dans l'affaire éponyme. Au fil des enquêtes judiciaires auxquelles j'ai participé au sein du contre-terrorisme français, je me suis forgé une expérience sur la thématique de la téléphonie mobile d'investigation et l'exploitation des supports numériques.

Ce guide a pour objectif d'initier les avocats mais également tous les acteurs de la chaîne pénale aux enjeux des investigations en termes de téléphonie mobile.

« Les Whatsapp, Signal, Telegram et autres messageries cryptées sont les Bismuth de 2020 ! […] Et parmi leurs utilisateurs, il y a des magistrats, des policiers… »
Jacqueline Laffont, Avocate Pénaliste – 09 décembre 2020

« Il m'arrive de dire à un client ou à un confrère « On est au téléphone…arrêtez… » C'est déplorable. »
Henri Leclerc, Avocat Pénaliste – 03 décembre 2020

TABLE DES MATIÈRES

1. INTRODUCTION

La généralisation de l'usage du téléphone portable au début des années 2000 a profondément changé les techniques d'interceptions judiciaires. Au fur et à mesure, le téléphone mobile s'est mué en smartphone puissant, connecté et sécurisé. L'objet de communication est devenu aussi incontournable que l'ADN au sein des enquêtes judiciaires. Il est à présent un véritable élément de preuve, omniprésent dans la plupart des procédures pénales.

Autrefois réservées aux enquêtes judiciaires les plus complexes et les plus délicates, les méthodes d'investigations téléphoniques sont aujourd'hui à la portée de tous les enquêteurs. De la brigade de gendarmerie départementale au 1er échelon des services d'investigations en commissariat de police, l'identification du titulaire d'une ligne mobile ou l'obtention d'une fadette, est devenue anodine. Les lois et les techniques d'investigation se sont rapidement adaptées en conséquence pour offrir aux forces de l'ordre et aux autorités, les moyens d'entrer dans la sphère privée des citoyens et ainsi nourrir les procédures. Les fadettes, les écoutes, sont indéniablement des outils précieux dans la lutte contre la délinquance et la criminalité.

Les avocats, les magistrats, les professionnels du droit dans toute leur diversité se trouvent confrontés au quotidien à ce panel

d'investigations autour de la téléphonie, a des éléments techniques, avancés au grès des procès-verbaux. Les corrélations faites à partir des éléments recueillis, les déductions, suspicions naissantes, alimentent la preuve et se veulent souvent péremptoires. Alors même qu'elles peuvent être parfois remises en question avant d'être admises formellement comme des preuves irréfutables.

Le temps de la garde à vue, court et dense à la fois, se trouve être l'occasion pour les enquêteurs de mettre en avant des mois d'interceptions judiciaires, d'exploitations de fadettes et ainsi d'avancer pion par pion, un argumentaire fondé sur leur appréciation des données récoltées. Le temps de l'instruction se veut souvent nourri de ce recueil avec l'objectif de contester les déclarations de votre client.

Ce guide a pour but de permettre aux avocats de comprendre de quelles manières tous les éléments gravitant autour du téléphone mobile, sont recueillis et exploités. Maîtriser le lexique technique, appréhender le raisonnement des enquêteurs et ainsi assurer une défense efficiente de chaque mis en cause, lorsque la téléphonie mobile se trouve au coeur de la procédure pénale.

Lors de vos entretiens avec votre client, à l'occasion d'observations en auditions, en interrogatoires, lors d'une demande d'acte, préciser certains détails autour de la téléphonie mobile, permettra de discuter de la pertinence de la preuve. Tout comme il vous sera possible, d'analyser comment les investigations téléphoniques ont conduit à parfaitement matérialiser les faits reprochés.

Nous identifierons dans un premier temps, les informations que les enquêteurs sont en mesure de recueillir, à partir de quels outils, et de quelles manières ils les exploitent. Nous étudierons également toutes les possibilités offertes par l'étude des Fadettes, la géolocalisation et les écoutes téléphoniques. Au travers de cas

pratiques, vous pourrez appréhender les différentes informations obtenues par les enquêteurs.

Dans un second temps, nous aborderons les différentes évolutions technologiques qui ont permis l'émergence des "techniques spéciales d'enquêtes" à l'aide d'outils tels que les IMSI Catcher et les Keyloggers. Les messageries sécurisées sont également très présentes dans les investigations liées à la téléphonie mobile et nous verrons de quelle façon elles impactent le travail d'enquête.

Dans un souci de protection de vos échanges professionnels et afin de vous prémunir de tout risque de vols de données ou d'interceptions d'informations sensibles, nous aborderons les bonnes pratiques pour sécuriser votre utilisation des applications de messageries chiffrées Whatsapp, Telegram et Signal.

L'évolution des technologies de communications et votre maîtrise de leurs enjeux au sein de la procédure pénale impacteront de manière significative votre stratégie de défense.

2. LE LEXIQUE TECHNIQUE

Afin de cerner au mieux les outils et les enquêtes en matière de téléphonie mobile, plusieurs termes techniques sont à appréhender. Chacun de ces termes est un élément essentiel du fonctionnement du réseau téléphonique mobile et génère des « traces » exploitables par les enquêteurs. Ils sont mentionnés dans le langage policier au titre des « sélecteurs techniques ». Invisibles au quotidien, tous ces composants font partie intégrante de l'usage d'un téléphone mobile.

- **Les cellules (Antenne-relai / Bornes)** : Une antenne-relais est un émetteur d'ondes faisant le lien entre votre ligne mobile et le réseau téléphonique. Implantées sur tout le territoire, les antennes-relais forment ce que l'on appelle la « couverture réseau ». **En réalité, l'antenne-relais n'est que le support de « cellules » indépendantes chacune des autres.**

  Chaque cellule est dédiée à une fréquence spécifique du réseau (2G/3G/4G/5G). Chaque opérateur mobile implante sur le territoire ses antennes et ses cellules afin de réaliser un maillage qui rendra l'usage du téléphone transparent, sans perte de signal. Quand votre téléphone est allumé, il cherche en permanence à se connecter à une antenne-

relais, une cellule, pour recevoir et émettre des communications. Il s'associera à celle la plus proche et émettant le signal le plus fort.
Chaque cellule couvre un rayon qui est limité par sa puissance et qui se superpose aux rayons d'action des autres cellules de l'opérateur dans le même secteur. Les antennes-relais sont souvent appelées « borne relais ». Quand les enquêteurs parlent de « bornage », ils font référence à la géolocalisation des cellules utilisées par un téléphone mobile.

Chaque cellule est identifiable par un numéro spécifique et les enquêteurs, tout comme vous, peuvent en connaître la localisation exacte[1] et ainsi déterminer la position estimée de votre mobile. *(Voir chapitre 7 et 9)*

- **La carte SIM** : La carte SIM est une puce contenant un microcontrôleur et de la mémoire. Elle est fournie par l'opérateur téléphonique et contient deux numéros techniques importants et indispensables. Le premier est appelé numéro **« IMSI ».** Le deuxième, le numéro de « série » de la carte SIM se nomme **« ICCID »**. Pour communiquer avec votre téléphone mobile, vous disposez d'un numéro de mobile et de la carte SIM associée. Le numéro IMSI est associé à votre ligne mobile, il ne change pas. Si vous perdez votre carte, l'opérateur vous en fournit une nouvelle avec le même numéro de téléphone, le même numéro IMSI, mais avec un numéro ICCID différent.

- **Le numéro ICCID** : Il s'agit du numéro de série de la carte SIM. Chaque carte SIM dispose de son propre numéro ICCID. Il est composé de 19 chiffres. Il est visible sur le support de la carte SIM. Ce numéro permet aux enquêteurs de connaître les changements de carte SIM même s'il s'agit

[1] Site de référencement des antennes-relais en France : https://www.antennesmobiles.fr/

du même opérateur et de la même ligne mobile.

- **Le numéro IMSI** : C'est l'identifiant « technique » qui permet de vous identifier sur le réseau téléphonique. Il est unique. Il pourrait être comparé à un numéro de « client ». *(Voir chapitre 6)*

- **Le numéro IMEI** : C'est un numéro unique propre à chaque téléphone mobile. Il s'agit de son numéro de série. Il est composé de 15 chiffres. Quand nous utilisons notre téléphone, le réseau mobile enregistre son numéro IMEI. Par exemple si un mobile est volé, l'opérateur pourra faire « blacklister » (bloquer) ce numéro pour qu'il soit inutilisable s'il se connecte sur le réseau téléphonique. Le numéro IMEI est le plus souvent inscrit sur une étiquette sous la batterie.

Vous pouvez également le connaître en tapant **#06#* sur votre clavier.

Quand nous utilisons notre téléphone mobile, le réseau téléphonique retient quatre sélecteurs techniques :

- **Le numéro de la ligne mobile**
- **Le numéro IMSI**
- **Le numéro ICCID de la carte SIM**
- **Le numéro IMEI du téléphone mobile utilisé.**

- **La DATA** : Dans le domaine de la téléphonie, la DATA correspond à la connexion internet de notre smartphone et son flux. Le mot DATA renvoie à la notion de « données », dans le cas qui nous concerne, internet. Les réseaux mobiles ont rapidement évolué ces dernières années en passant de la connexion EDGE, à la 4G et pour finir la 5G. Ces différents types de connexion influent sur la rapidité de votre connexion.

Quand nous utilisons notre smartphone notamment une application ou le navigateur internet, nous émettons de la DATA. Sur une Fadette, la DATA apparaît comme une communication à part entière au même titre qu'un appel téléphonique. Nos smartphones sont aujourd'hui en permanence connectés à internet pour fonctionner et donc sollicitent en permanence une antenne-relai pour obtenir du réseau et communiquer. Si votre téléphone est simple et sans connexion internet, il n'émet pas de DATA.

Sur un smartphone connecté à un réseau wifi, la connexion internet n'apparaîtra pas comme une communication « DATA ». Elle n'apparait pas sur la Fadette.

- **L'IMSI Catcher** : Il s'agit d'un dispositif électronique sophistiqué utilisé par les forces de l'ordre et les services de renseignements pour intercepter sur le terrain les données d'un téléphone mobile. Il peut s'agir d'une valise dont la puissance dépend de la taille. Concrètement, il peut tenir dans un sac à dos comme occuper l'arrière d'un fourgon. Ce dispositif se comporte comme une antenne-relai et force les téléphones autour à se connecter dessus. Les téléphones à proximité pensent qu'il s'agit d'une antenne-relai et se connectent dessus. Quand un téléphone s'y connecte, l'IMSI catcher aspire toutes les informations du téléphone comme son numéro de ligne, le numéro IMSI, le numéro IMEI. L'IMSI Catcher évalue aussi grâce au signal, la distance à laquelle il se trouve. Il peut également intercepter les communications émises ou reçues par le téléphone. *(Voir chapitre 12)*

- **L'adresse IP** : Il s'agit d'un numéro d'identification attribué à tout terminal informatique qui se connecte au réseau internet. IP signifie « internet protocol ». L'adresse IP vous identifie sur internet quand vous vous connectez avec votre ordinateur ou votre téléphone. L'adresse IP peut être

permanente ou provisoire. Votre fournisseur d'accès internet (le FAI) attribue à votre box une adresse IP. Ainsi lorsque vous naviguerez sur un site internet, ce dernier enregistrera votre adresse IP et il sera possible en interrogeant les fournisseurs d'accès internet de connaître l'identité de l'abonné. *(Voir chapitre 16)*

- **Le chiffrement de données** : Quand vous envoyez une donnée informatique à travers le réseau internet, il est possible pour celui qui l'intercepterait d'en lire le contenu si les données ne sont pas chiffrées. Tout comme nous pourrions lire le contenu d'un ordinateur ou d'un téléphone s'il n'y avait pas de mot de passe. Depuis longtemps, il existe différentes technologies qui permettent de rendre les données « illisibles » si l'on ne dispose pas de la clé pour l'ouvrir. On parle souvent à tort de « cryptage ».

Par exemple, si vous avez un iPhone et que vous avez mis un mot de passe, les données du téléphone sont « cryptées » et sans le mot de passe pour déchiffrer le Code, impossible de lire le contenu. **Apple chiffre automatiquement les données de ses smartphones. Il faut connaître la « clé » permettant de lire le contenu chiffré.**

Il est possible également de chiffrer les communications (messages, appels, photos, vidéos) grâce à des applications. Ainsi, pour celui qui intercepte ces échanges, sans le « Code » de déchiffrage, il n'est pas possible de lire ce qu'il a récupéré.

3. LA PLATEFORME NATIONALE DES INTERCEPTIONS JUDICIAIRES (PNIJ)

Le recueil des données liées à la téléphonie mobile est aujourd'hui exclusivement dépendant de la PNIJ.

Jusqu'en 2015, quand un officier de police judiciaire souhaitait obtenir l'identité de l'utilisateur d'un numéro de téléphone ou une Fadette, il devait rédiger une réquisition avec sa requête et l'envoyer à l'opérateur par fax ou par email. Il recevait la réponse au mieux quelques heures plus tard (en fonction de l'urgence invoquée) ou dans la majorité des cas, plusieurs jours après. La réponse n'était pas instantanée et ralentissant l'avancée de l'enquête. Nous ne parlons pas ici d'enquêtes criminelles où bien entendu il était possible d'obtenir une réponse très rapidement. Les délais de réponse combinés à la lourdeur du processus rendaient l'accès aux investigations téléphoniques difficiles et peu courantes dans les enquêtes judiciaires du quotidien.

En France, les opérateurs téléphoniques ont l'obligation légale de répondre aux réquisitions des autorités[1]. Cela fait partie des conditions d'exploitations du réseau. Cependant, les réquisitions ont un coût. Quand un enquêteur envoie une réquisition à un

[1] Article D98-7 du code des postes et des communications électroniques et article L851-1 du code de la sécurité intérieure.

opérateur, ce dernier facture le prix de la « prestation » au ministère de la Justice. La plus grosse difficulté tant opérationnelle que financière résidait dans les écoutes téléphoniques, dites « interceptions de ligne ». Il n'existait aucun outil dont l'État était propriétaire et qui permettait alors de réaliser les écoutes.

Raison pour laquelle elles étaient réalisées techniquement par des entreprises extérieures (Amecs, Elektron, Midi System Azur Integration, Foretec) qui mettaient à disposition le matériel informatique, les solutions de stockage sur serveur, etc. permettant de procéder aux opérations. Les interceptions (écoutes) ont coûté à l'État la somme de 122,55 millions d'euros en 2015[2].

Ce coût s'expliquait en partie en raison du grand nombre d'acteurs impliqués dans la gestion des interceptions, mais aussi de la différence de prix des prestations mises en place. Le système était désorganisé et cette multitude de méthodes faisait courir des risques flagrants quant à la sécurité des données interceptées et à la garantie de la confidentialité. En l'absence de contrôle et de centralisation, les autorités n'avaient pas la main sur la pratique la plus attentatoire à la vie privée.

Pour répondre à ces problématiques, l'objectif était de créer une plateforme permettant de procéder aux réquisitions téléphoniques numériquement en lien direct avec les opérateurs de téléphonie et permettant dans le même temps de gérer les interceptions de communications. Un outil unique, centralisé et sécurisé.

Le projet de Plateforme Nationale des Interceptions Judiciaires (PNIJ) fut réfléchi sous la présidence Chirac dès 2005, initié sous la présidence Sarkozy et développé sous celle de François Hollande.

[2] Rapport de la Cour des comptes du 18 février 2016.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

Sa mise en place fit perdre aux anciennes sociétés prestataires des interceptions, un marché juteux, et par des blocages de placement sur écoute, elles tentèrent de protester[3].

Ce projet développé par l'entreprise Thales, groupe français spécialisé notamment dans la sécurité et la défense, se révèle être un véritable gouffre financier dont la facture finale devrait s'élever en 2024 à 385 millions d'euros[4]. L'État est maître de son outil, mais Thales en qualité de prestataire de service est chargé du développement de la plateforme. Plateforme qui doit sans cesse relever les défis imposés par les évolutions technologiques et les difficultés qu'elles représentent pour les enquêteurs, telles que la 5G.

La PNIJ est gérée intégralement par le ministère de la Justice et plus spécifiquement par l'Agence Nationale des Techniques d'Enquêtes Numériques Judiciaires (ANTENJ)[5]. Sa direction est confiée à un magistrat.

La PNIJ a été officiellement mise en service, à disposition des enquêteurs fin 2015. En quelques mois, le nombre de réquisitions téléphoniques et de placements sur écoute a explosé. La PNIJ est capable de gérer en simultané entre 10 000 et 12 000 écoutes téléphoniques. Malgré quelques déboires à son lancement au début de l'année 2016 et des difficultés d'évolution rapide, la plateforme est désormais opérationnelle et traite chaque semaine des millions de SMS, d'appels et de données DATA.

Cette plateforme est accessible aux fonctionnaires de police, gendarmes habilités (essentiellement enquêteurs dans des services de police judiciaire, en commissariat ou en unité

[3] « Grève des écoutes : la chancellerie contre-attaque » Emmanuel Fansten (Libération - novembre 2014)

[4] http://www.slate.fr/story/159046/pnij-ecoutes-judiciaires-ministere-justice-retard-facture-385-millions-euros

[5] La PNIJ est régie par les articles R. 40-42 à R. 40-56 du code de procédure pénale, instaurée par décret n° 2014-1162 du 9 octobre 2014 portant création d'un traitement automatisé de données a caractère personnel.

spécialisée) et douaniers. Elle est également accessible aux magistrats et aux greffiers.

Chaque personne habilitée à se connecter sur la plateforme est restreinte en fonction de son rôle à jouer. Les enquêteurs se connectent sur la plateforme à l'aide d'un lecteur nécessitant leur carte à puce professionnelle et un code d'accès.

Lorsqu'une enquête nécessite d'effectuer des investigations téléphoniques, l'enquêteur crée sur la plateforme un dossier numérique répondant aux références de l'affaire dont il a la charge, renseigne le cadre judiciaire dans lequel il opère (enquête préliminaire – de flagrance ou Commission rogatoire) et le nom du magistrat en charge de l'affaire. Il désigne également les autres fonctionnaires auxquels il souhaite donner accès au dossier. Ainsi dans cet espace partagé, l'enquêteur, ses collègues et le magistrat auront accès aux mêmes informations et visualiseront les mêmes données.

L'ensemble des prestations de réquisitions ou d'interceptions sont listées sous forme d'un référentiel. Le coût de chaque prestation est défini.

Exemples :

- **Prestation « MA02 » - 3.06€**

Identification d'un abonné à partir de son numéro d'appel, avec les caractéristiques techniques de la ligne ou du numéro de sa carte SIM (avec ou sans coordonnées bancaires), demande reçue sous forme papier, par fax ou sous toute forme électronique.

- **Prestation « MA21 » - 3.06€**

Historique d'attribution d'un numéro d'appel, d'un numéro de carte SIM ou d'un identifiant d'abonné (numéro IMSI).

- **Prestation « MI20 » - 16,00€**

Interception des communications de téléphonie mobile.

Il est ainsi possible d'obtenir le détail de l'ensemble des prestations réalisées et de connaître la correspondance du code de la réquisition en se référant à **l'article A43-9 du Code de Procédure Pénale**.

Prenons un cas simple. L'enquêteur ouvre un dossier sur la plateforme, car il souhaite identifier le titulaire d'un numéro de mobile. L'enquêteur choisit la demande qu'il souhaite formuler, dans le cas présent « identification de l'abonné d'une ligne mobile ». Il entame la démarche au sein du dossier lié à l'enquête pour remplir une réquisition. Il sélectionne une prestation de MA02, l'opérateur, la date à laquelle l'identification est demandée. La PNIJ informe l'enquêteur à titre purement indicatif du coût de sa demande (dans notre cas 3,06€). Il s'agit-là de sensibiliser le fonctionnaire au coût engendré par son enquête et de formuler des requêtes pertinentes.

Après avoir validé les informations, l'enquêteur est invité à signer numériquement sa réquisition en composant sur le lecteur un code personnel à plusieurs chiffres. La réquisition est alors transmise à l'opérateur téléphonique.

La PNIJ récupère la réponse en moins de trois minutes par le biais d'une mise en relation automatique des systèmes informatiques des opérateurs. Si la demande présente une certaine complexité, la réquisition est traitée « manuellement » par le service des obligations légales de l'opérateur désigné et dans ce cas la réponse sera disponible ultérieurement. Lorsque l'enquêteur est avisé que la réponse est disponible, il la consulte sur son ordinateur. La réquisition numérique à une valeur légale. La réponse également. Cette réponse est stockée sur la PNIJ.

La pratique judiciaire veut que chaque réquisition soit imprimée et jointe à la procédure. Mais partant du principe qu'elles sont numériquement stockées sur les serveurs et accessibles lors de la mise sous scellé du dossier, ce procédé n'est pas obligatoire. Néanmoins, l'enquêteur se doit d'acter en procédure les recherches engagées et nous ne pouvons qu'inciter les Conseils à

s'assurer de la fidélité des réquisitions effectuées à celles indiquées dans le scellé des données issues de la PNIJ en clôture d'enquête.

Une fois l'enquête terminée, l'enquêteur clôture le dossier et la PNIJ génère un code faisant office de scellé « numérique ». Une fois les données scellées, l'enquêteur n'a plus accès aux écoutes. Le magistrat peut à tout moment consulter toutes les réquisitions faites en son nom ainsi que les réponses obtenues. Le magistrat peut également réaliser lui-même des réquisitions et des interceptions, ce qui se pratique très peu en réalité.

Le placement sous scellé du dossier d'investigations téléphoniques se fait entièrement numériquement dans un coffre-fort sécurisé de la plateforme. Il appartient à l'avocat de solliciter une copie[6] des données placées sous scellés au magistrat qui sollicitera à son tour la Délégation aux interceptions judiciaires (DIJ). Un support lui sera alors remis.

Depuis sa mise en place, la PNIJ soulève de nombreuses questions qui subsistent encore aujourd'hui.

Le choix de faire appel à une société privée telle que Thales pose la question de la garantie de la sécurité des données de millions de citoyens. Thales a développé la plateforme, elle stocke sur ses serveurs toutes les données directement récupérées auprès des opérateurs téléphoniques et des fournisseurs d'accès internet, elle possède les clés de chiffrement des données présentes sur ses serveurs. Néanmoins, l'entreprise n'a pas accès aux contenus des informations stockées. Il aurait été plus judicieux que le stockage des données issues de la PNJI se fasse en interne sur des serveurs appartenant à l'État. L'idée qu'une entreprise spécialisée dans le domaine militaire dispose d'une telle masse de données n'est jamais rassurante.

[6] C. pr. pén., art. R. 40-51

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

Les enquêteurs ouvrent des dossiers sur la plateforme au nom des magistrats en se basant sur les autorisations délivrées par ces derniers. Néanmoins, chaque magistrat du Parquet se voit rattaché à d'innombrables dossiers ouverts sous leur « tutelle ». La PNIJ prévoit à terme que les autorisations des magistrats soient directement intégrées à la plateforme pour garantir la légalité du processus. Cela n'étant toujours pas le cas aujourd'hui, comment les magistrats peuvent-ils être en mesure de vérifier chaque jour la légitimité des dizaines de réquisitions faites sous leur autorité ?

L'ANTENJ ne peut accéder au contenu des dossiers sur la PNIJ mais néanmoins elle trace toutes les actions des utilisateurs. Les actions réalisées sur la PNIJ sont conservées pendant 5 ans. L'ensemble des données récoltées sont conservées jusqu'à l'extinction de l'action publique dans le dossier concerné.

La PNIJ souffre de ses capacités de prise en charge des nouvelles technologies telles que les messageries chiffrées qu'elle est incapable à ce jour de mettre au clair. Le ministère de la Justice fait appel à deux prestataires privés pour tenter de déchiffrer des données issues de messageries sécurisées ou de communications « PGP ».

La 5G dont le déploiement est en cours ne fait que souligner le retard persistant sur l'incapacité de la plateforme à s'adapter. La 4G comme la 5G font transiter les communications « voix » par le flux internet et les nouveaux protocoles font obstacle aux interceptions de communications. Dans ces conditions, la 5G promet d'être un frein réel à l'utilisation des IMSI Catcher[7].

La reconnaissance vocale se trouve aussi au cœur des questions subsistantes autour de la PNIJ. En effet, la plateforme offre la possibilité aux enquêteurs d'authentifier et d'analyser l'empreinte vocale d'un suspect afin de la reconnaitre dans l'ensemble des communications interceptées et ainsi faciliter le travail d'écoute. La technique actuelle ne permet pas de définir une empreinte

[7] « La 5G, un frein dans la lutte contre la criminalité »
(Le Point – juin 2019)

vocale comme étant une donnée biométrique fiable à ce jour. Quelle serait donc la force probante accordée aux interceptions judiciaires fondées sur la reconnaissance vocale ?

L'exercice du droit à la défense se révèle également entravé depuis la mise en place de la PNIJ. Auparavant, les enquêteurs procédaient à la gravure sur Cd-Rom des enregistrements issus d'interceptions de communications. Une copie de travail, accessible aux avocats, permettait à ces derniers de prendre connaissance des communications et exercer le droit à une défense effective. La PNIJ place désormais sous scellé numérique l'ensemble des enregistrements et seul le magistrat peut solliciter une copie auprès de la Délégation aux Interceptions Judiciaires (DIJ). Il semble que la remise d'une copie physique des enregistrements soit au bon vouloir de cette administration publique qui s'octroierait le droit de refuser la délivrance des enregistrements. Comment un avocat peut-il aujourd'hui défendre efficacement son client, sans accès aux enregistrements mis en avant dans une procédure ?

Au-delà des considérations évoquées, un problème plus grave encore se pose quant aux traitements des renseignements obtenus lors des interceptions de communications. En effet, la PNIJ permet aux enquêteurs de rédiger directement en ligne, les procès-verbaux de retranscriptions des écoutes réalisées et de laisser des commentaires en annotation. La PNIJ conserve donc officiellement tout ce que les enquêteurs relèvent lorsqu'ils procèdent aux écoutes. Le bon sens ainsi que les principes qui régissent la pratique pénale auraient voulu que seuls les éléments utiles à la manifestation de la vérité fassent l'objet d'une retranscription.

Ce n'est pas le cas. L'article R40-44 du Code de procédure pénale dispose que la PNIJ permet d'enregistrer des données à caractère personnel évoquées lors des communications ou dans les données interceptées. **Ainsi il est permis de consigner les opinions politiques, religieuses, les informations sur l'origine raciale ou ethnique, sur l'orientation sexuelle, de l'individu écouté, ainsi que**

celles de ses contacts. Au-delà de la possibilité offerte aux enquêteurs d'en dire bien plus sur un suspect en l'habillant autour de ses opinions qui ne regarde que lui, que deviennent ces informations ? Ont-elles vocation à être détournées et alimentent-elles les services de renseignements ?[8]

À ce jour, aucune mesure n'est mise en place pour permettre la consultation ou la suppression d'informations nominatives personnelles qui vous concerneraient, détenues au sein de la PNIJ. À l'aune des grands principes sur le respect de la vie privée des citoyens et de l'accès à leurs informations, la PNIJ apparaît comme un outil obscur et paradoxalement lui-même attentatoire au respect de la vie privée.

Dans une délibération en date du 16 janvier 2014, la CNIL consultée au sujet du décret de mise en place de la PNIJ, estimait ainsi que :

« Les risques que cette centralisation d'une masse importante de données personnelles soulève sont substantiels. »

Au-delà de sa rigidité de fonctionnement, des plaintes récurrentes des policiers et des gendarmes, la PNIJ a réussi à relever le défi de faire entrer l'investigation téléphonique mobile dans l'ère du numérique. L'évolution constante du nombre de requêtes ou d'interceptions en est le reflet.

La PNIJ est en passe de réaliser sa mutation pour devenir la PNIJ NG (nouvelle génération). Le contrat avec Thales se termine en 2024 et fort des conclusions de la Cour des comptes, le projet envisage d'internaliser le stockage des données sur différents sites de l'administration. Le premier appartient au ministère de la Justice à Nantes (Loire-Atlantique) avec le service du Casier judiciaire national (CJN). Le second dépend de l'Intérieur, il s'agit du DSIC (direction des systèmes d'information et de la communication située dans le fort de Rosny-sous-Bois en Seine-Saint-Denis.

[8] Analyse pertinente proposée par Clarisse Serre et Charles Evrard dans « Du rififi chez les grandes oreilles » (Dalloz – février 2020)

Mais le réel défi serait de proposer un outil transparent dans son usage et son contenu, un outil au service de l'investigation et de la Justice, dans le respect des intérêts de la défense.

4. MERCURE : LE LOGICIEL D'EXPLOITATION DES DONNÉES TÉLÉPHONIQUES

Aujourd'hui, la PNIJ démocratise l'accès aux données issues de la téléphonie mobile. Mais si analyser la réponse d'un opérateur pour connaître le nom de l'utilisateur d'un numéro de téléphone est simple, l'analyse d'une fadette et de ses données se révèle être autrement bien plus complexe.

Imaginez, une Fadette n'est ni plus ni moins qu'un fichier Excel (tableur) pouvant contenir parfois jusqu'à 100 000 lignes ! Comment s'y retrouver avec aisance ? Comment comptabiliser le nombre de fois où un utilisateur a contacté un numéro ? Il n'est pas envisageable de le traiter manuellement.

Ce temps-là est révolu depuis l'apparition des logiciels permettant d'analyser ces données. La gendarmerie nationale et la police utilisent chacun le leur. La gendarmerie utilise une solution logicielle développée en interne et la police utilise un logiciel sous licence. Nous allons exclusivement traiter dans cette partie du logiciel utilisé par la police nationale, à savoir le logiciel **Mercure** qui en est à sa 4e version. C'est un logiciel développé par la société Ockham solutions[1] basée à Paris.

[1] https://ockham-solutions.fr/produits/mercure/mercure-v4.html

Le logiciel « Mercure » est particulièrement efficace, car il se nourrit des informations que les enquêteurs y injectent et parce qu'il propose d'innombrables possibilités de croisement des données.

Chaque service enquêteur dispose sur ses ordinateurs de ce logiciel. L'ensemble des données de téléphonies mobiles injectées dans Mercure est stocké sur des serveurs au niveau local de chaque Direction Départementale de Police. Un ou plusieurs fonctionnaires ont la charge d'administrer localement le logiciel et sa base de données.

Ainsi les données sont partagées uniquement entre enquêteurs au niveau local et non pas national. **Par exemple : les enquêteurs de la Police Judiciaire de Lille n'ont pas automatiquement accès aux données « Mercure » de la Police Judiciaire de Marseille.** C'est assez exclusif.

Toute l'efficacité de ce logiciel réside dans la possibilité de partager les données téléphoniques. En effet, le Brigadier Dumont investigue sur le +33611223344. Pour ce faire, il devra d'abord vérifier sur « Mercure », si ce numéro n'apparaît pas déjà dans une autre enquête et le cas échéant dans quel cadre ? Dans ce cas, si ce numéro apparaît dans une enquête à Lille, il n'aura pas la possibilité de le savoir autrement qu'en effectuant différentes recherches dans les bases de données de la Police Judiciaire. Cela soulève la question de l'opportunité de faire verser à son enquête les données récoltées lors de l'affaire de la PJ de Lille. Ainsi, il est possible d'exporter les données d'une base de données Mercure pour les intégrer à une autre située dans un service différent.

Partant du postulat que les Fadettes ne peuvent être obtenues que sur une période d'un an, il peut s'avérer utile d'obtenir les données antérieures à cette période et issues d'autres affaires.

Une fois le sélecteur technique (N° de mobile, N° IMEI, adresse, identité, etc..) Injecté dans Mercure, s'il apparait dans d'autres affaires du service, il sera possible de le savoir en effectuant une simple recherche.

Le logiciel Mercure se présente aux enquêteurs sous forme d'une arborescence par dossier. Un enquêteur crée un nouveau dossier auquel il attribue le nom de l'affaire ainsi que ses références. Il injecte dans l'outil le fichier contenant la Fadette en lui attribuant un nom pour se repérer plus facilement par la suite (exemple : « Ligne 33655887744 – Michel Durand »)[2]. Il peut ensuite créer des sous-dossiers par individus, etc. Chaque Fadette peut être déplacée dans le dossier de son choix. Le dossier Mercure de l'affaire est ensuite partagé avec l'ensemble des enquêteurs du service qui y auront accès sur leur compte individuel.

Par la suite, le Brigadier Dumont décide de demander une fadette sur la ligne +33611223344 pour connaître les communications sur le mois écoulé. Il va recevoir en réponse un fichier de la PNIJ sous format .XML ou un tableur Excel. L'enquêteur l'importe dans le logiciel Mercure et ce dernier va en quelques secondes l'analyser et ensuite l'expertise de l'enquêteur fera le reste. **Car le logiciel propose de nombreuses fonctionnalités, mais il ne lit pas à la place de l'enquêteur.** Ainsi le Brigadier Dumont pourra savoir quelles sont les personnes que le mis en cause appelle le plus souvent, où est-il susceptible de dormir et s'il se trouvait Rue des Arcs à Reims, le 4 octobre entre 3 et 5 h du matin, etc..

Mercure peut absorber des millions d'appels, de données de géolocalisation, des répertoires téléphoniques, des données de disques durs. Et il croise l'ensemble des données permettant par exemple :

- De savoir si deux lignes mobiles ont été localisées au même endroit dans un temps rapproché.

[2] Dans la téléphonie d'investigation, les numéros de ligne sont toujours inscrits avec le préfixe du pays (+33 pour la France), cela permet d'identifier immédiatement le pays de provenance de la ligne et également de faciliter les recherches au sein des fichiers (PNIJ, Mercure, fichiers police, procès-verbaux).

- De savoir si un individu a changé de téléphone portable en listant les numéros IMEI utilisés.

- De connaître les personnes que l'utilisateur d'un téléphone mobile contacte le plus souvent.

- De savoir si une identité utilise plusieurs lignes qui auraient été identifiées dans d'autres affaires.

- De savoir si un individu a prêté son téléphone à une autre personne qui aurait inséré sa carte SIM à l'intérieur.

- La liste des numéros en communs avec d'autres personnes.

Nous reviendrons sur ces possibilités au chapitre 8 « Cas pratiques ».

Mercure propose également d'analyser des environnements téléphoniques complets. Un simple clic génère un rapport listant les habitudes d'un utilisateur. Combien de temps appelle-t-il, combien de temps passe-t-il sur internet, appelle-t-il plutôt la nuit ou la journée, à quels endroits se situe-t-il le plus souvent et sur quels créneaux horaires...

La force de recoupement des données est aussi un atout majeur de Mercure. Il peut produire des propositions de ligne mobile à étudier de près alors quand bien même s'abriterait-elle derrière une identité fictive. Il suffit d'analyser les données de contacts, de localisations et d'identités associés.

Les données extraites de disques durs et de téléphones peuvent être aussi intégrées à Mercure. Tous les identifiants contenus, les contacts, les messages sont classés et inventoriés pour faciliter la recherche sur l'environnement d'un individu.

Mercure produit aussi d'excellents graphes où l'enquêteur visualise l'ensemble des personnes proches « téléphoniquement » et les interactions entre ces différentes personnes.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

Le stockage des données de téléphonie mobile ne fait pas l'objet d'une contrainte quant à la durée de conservation. Il n'est pas rare de constater la présence indéfinie dans le temps, de données issues de la PNIJ et qui sont conservés au sein de Mercure.

L'utilisation de Mercure doit faire l'objet d'une formation de deux jours. Sa maîtrise peut s'avérer complexe pour un profane et une longue pratique est nécessaire pour comprendre toutes les subtilités et les astuces de recherches au sein du logiciel.

Plus les enquêteurs nourrissent « Mercure », plus il produit de résultats. La seule règle pour eux est de savoir ce qu'ils recherchent, même si parfois le hasard conduit à des éléments qui changeront le cours de l'enquête.

5. L'IDENTIFICATION DE L'ABONNÉ OU DE L'UTILISATEUR D'UNE LIGNE MOBILE

La première démarche effectuée et la plus courante pour un enquêteur, c'est l'identification du titulaire et de l'utilisateur de la ligne mobile. **À qui appartient ce numéro de téléphone et qui se cache derrière ?** Néanmoins, celui qui possède l'abonnement de téléphone n'est pas nécessairement celui qui l'utilise.

Nous allons prendre un exemple : un huissier de justice se rend au commissariat après avoir reçu des menaces de mort par message et il craint le pire. Une fois la plainte prise en enquête préliminaire, la police judiciaire est saisie pour enquêter. Le Brigadier Dumont va commencer par identifier le numéro de mobile à l'origine de ses SMS menaçants.

Avant de transmettre une réquisition à un opérateur, il est important de connaître quel est l'opérateur gestionnaire de la ligne mobile. C'est à l'aide du fichier « Aerope » que l'enquêteur connaîtra l'opérateur de la ligne. Ce fichier est directement en lien avec l'Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse). Vous pouvez vous-même sur leur site, connaître l'opérateur attribué à

une ligne mobile[1].

La particularité d'Aerope, c'est d'avoir la capacité de prendre en compte la portabilité d'un numéro. Chaque opérateur se voit attribuer un « bloc » de numéro de mobile à assigner à leurs abonnés. Exemple le bloc « 062385 » est attribué à SFR. À l'origine, un numéro commençant par « 062385 » est susceptible d'appartenir à un abonné de l'opérateur SFR, mais si cet abonné a résilié son contrat pour souscrire avec le même numéro de mobile (portabilité) chez Bouygues Telecom, Aerope sera en mesure de l'indiquer aux enquêteurs et à partir de quelle date.

« Aérope » est disponible sous l'interface Cheops. Il permet l'identification de l'opérateur d'une ligne mobile mais également l'identification de masse de plusieurs lignes. L'enquêteur peut ainsi injecter un fichier sous le format Excel extrait de la PNIJ ou de Mercure afin de connaître l'opérateur d'un grand nombre de lignes mobile.

Il est primordial de connaître l'opérateur gérant le numéro de mobile afin de requérir le bon opérateur sur la PNIJ.

Le Brigadier Dumont a identifié que le numéro 0688990011 auteur des menaces contre notre huissier appartient à l'opérateur Orange. Via la PNIJ, il envoie une réquisition visant la prestation « Identification de l'abonné d'une ligne mobile » (MA02). Il reçoit la réponse en quelques instants.

La ligne 0688990011 appartient à monsieur Leroy Serge résidant à Rumigny (80). Il s'agit d'un individu ayant une dette dont notre huissier est chargé du recouvrement.

1. Renseignements obtenus lors d'une identification

Quelles informations obtient le Brigadier Dumont dans la réponse de l'opérateur Orange :

[1] https://www.arcep.fr/demarches-et- services/professionnels/base-numerotation.html

- **Nom et prénom de l'abonné** (l'abonné est celui qui a souscrit le contrat téléphonique)
- **Sa date et lieu de naissance**
- **Son adresse déclarée**
- **Ses coordonnées** (autre numéro fourni, adresse email)
- **L'utilisateur de la ligne si autre que l'abonné** (si un client prend un abonnement pour un de ses enfants, il peut déclarer à l'opérateur l'identité de celui qui utilise la ligne. C'est la différence entre le titulaire et l'utilisateur).
- **La date de souscription et le type d'abonnement** (Abonnement, carte prépayée, abonnement professionnel d'entreprise, etc.)
- **Les anciens numéros de mobile** s'il y a eu changement de numéro.
- **Le numéro ICCID de la carte SIM** (avec historique si perte ou vol de carte SIM).
- **Numéro IMSI** (avec historique).
- **Le numéro IMEI** (avec historique si changement de téléphone chez l'opérateur).
- En complément, les données de facturation si l'enquêteur a sollicité une identification avec coordonnées bancaires. **Il aura donc le moyen de paiement utilisé avec le RIB fourni ou numéro de carte bancaire.**

La liste des informations obtenues est conséquente.
Exemple de réponse obtenue (page suivante) :

Réponse identification abonné (MA02)
Opérateur : ORANGE

Informations titulaire	Nom : M SERGE LEROY			
Informations utilisateur	Nom : M SERGE LEROY			
Adresse de facturation				
40 IMPASSE DE LA VIGNE				
80680 RUMIGNY				
Abonnement	**Numéro**	**type**	**du**	**au**
Contrat opérateur	10258642302	abonne	18/02/2010	
Evenement	Actif - contrat		18/02/2010	
Evenement	Actif - MSISDN = +33688990011		18/02/2010	
Evenement	Actif - Carte SIM (activee) 8933201456049720000		18/02/2010	
Evenement	Actif		04/04/2012	
Evenement	Actif - IMEI = 357712036685025		04/04/2012	
Evenement	Actif - MSISDN = +33652857496			
Evenement			18/02/2010	
Téléphone	33688990011	icrid		
SIM	8933201456049720000	nsce		
IMEI	359945869124658,00			

2. L'identification par recherche inversée

Il est possible d'effectuer une recherche inversée à partir d'un des éléments de la liste précitée. Au lieu d'effectuer une recherche à partir du numéro de mobile, les enquêteurs peuvent obtenir la ligne utilisée par un abonné à l'aide de son adresse, de ses moyens de paiement, etc.

Dans notre exemple, le Brigadier Dumont dispose du numéro de téléphone. Si en lieu et place du numéro de téléphone, le plaignant avait fourni l'identité de l'auteur des menaces, l'enquêteur aurait pu retrouver le numéro de téléphone de celui-ci à partir de son identité.

Voici la liste des différentes requêtes inversées possibles :

- **Par identité :** à l'aide du Nom, du Prénom et de la date de naissance d'un individu, l'opérateur fournira tous les abonnés correspondants à ces critères. Les éléments peuvent être combinés différemment.

- **Par N° IMEI :** transmis aux opérateurs, si l'un d'eux dispose de ce numéro IMEI associé à la ligne dans sa base de données, il transmettra l'identité le reste des informations. (Prestation MA50)

- **Par adresse :** En demandant aux opérateurs la liste des abonnés résidant au 40, rue du Général Leclerc à Rumigny. En zone rurale, le nombre de résultats serait limité alors qu'en ville, la liste peut être longue et ne permet d'obtenir qu'une liste de suspects potentiels. (Prestation MA30 / MA31)

- **Par coordonnées (Email) :** Si un des opérateurs a enregistré l'adresse mail de M. Leroy, alors l'enquêteur obtiendra ses informations. (Prestation MA30 / MA31)

- **Par numéro IMSI ou ICCID :** Si les enquêteurs disposent de ces numéros, les opérateurs lui indiqueront quel abonné en est le propriétaire. (Prestation MA30 / MA31)

- **Par coordonnées bancaires (RIB et CB)** : L'enquêteur peut transmettre le RIB ou le n° de carte bancaire aux opérateurs et il saura lesquelles ont un abonné utilisant ce moyen de paiement et de facto, la ligne mobile associée. Cela fonctionne également avec les coupons de recharge prépayée. (Prestation MA41)

Dans la pratique, la seule véritable limite se trouve être l'imagination de l'enquêteur. L'ensemble des éléments précités peuvent être inclus simultanément dans la requête. Cependant, l'enquêteur se doit d'être pertinent dans sa réquisition au risque de faire une recherche trop imprécise ou partielle et d'obtenir en réponse une liste de résultats inexploitable.

Si le l'enquêteur souhaite en savoir davantage, il pourra en demander à l'opérateur en complément, une copie du contrat souscrit qui contiendra une copie de la pièce d'identité fournie et un justificatif de domicile.

L'exemple fourni pour illustrer la recherche de l'identité du titulaire d'une ligne mobile est valable dans le cadre d'une enquête judiciaire simple et sans difficulté particulière.

Mais comme nous l'avons évoqué, le titulaire identifié de la ligne n'est pas nécessairement celui qui l'utilise.

Le mis en cause a très bien pu souscrire l'abonnement, mais il a pu confier son téléphone et sa carte SIM à une autre personne. C'est à partir de ce moment qu'il faudra faire intervenir l'utilisation de Fadette. Cependant, d'autres complications peuvent apparaître.

3. Les cartes SIM prépayées

L'usage de carte SIM prépayée complique l'identification de l'utilisateur d'une ligne mobile. Lorsqu'une personne souscrit un forfait mensuel auprès d'un opérateur, en ligne ou en boutique, un justificatif d'identité est demandé (Carte d'identité, passeport ou titre de séjour). C'est ce que prévoit la loi, les opérateurs ont l'obligation de procéder à l'identification de leurs abonnés.

Il est possible de se rendre dans une boutique, chez un buraliste ou tout autre revendeur et d'acheter une carte SIM prépayée. Ces lignes se rechargent à l'aide de coupon disponible chez un buraliste, un revendeur ou en ligne. Ainsi, en fonction du montant et des options choisies, la carte SIM sera créditée pour une durée limitée.

À ce stade, l'identité du titulaire ne sera pas demandée[2]. Toutefois pour des raisons légales, l'opérateur fournissant la carte SIM sollicitera l'utilisateur dans un délai pouvant varier de 15 jours à un mois, afin de fournir son identité et dans le cas contraire, il procédera à la désactivation de la ligne.

Le problème se posera lorsqu'un enquêteur voudra identifier le titulaire déclaré de la ligne, l'opérateur risque de ne pas être en mesure de fournir des éléments, si l'abonné ne s'est pas identifié.

Si l'utilisateur d'un mobile change de carte SIM prépayée tous les quinze jours, cela complique nettement son identification mais ce n'est pas impossible.

Une solution existe pour pallier cela. Avec le numéro de la carte SIM (ICCID), il est possible d'identifier le point de vente et donc en théorie d'exploiter la vidéosurveillance de ce dernier et du quartier (conditionné à la présence de caméras en état de fonctionnement).

---

[2] Hormis en boutique officielle d'opérateur mobile où le conseiller sollicitera directement la présentation d'une pièce d'identité en cours de validité.

Cependant, en règle générale, les opérateurs mobiles revendent des lots de cartes SIM prépayées aux sociétés distributrices. Les lots sont ainsi répartis entre différents points de vente et il devient difficile de savoir spécifiquement dans quelle boutique un lot a été vendu.

Nous conviendrons qu'un de vos clients qui dans un dossier, changerait de carte SIM prépayée tous les quinze jours ferait naître le doute quant à sa volonté de se dissimuler aux autorités. Toutefois, des failles existent en matière d'enregistrement de l'identité déclaré du titulaire d'une ligne mobile prépayée.

Nous prenons ici l'exemple de la carte prépayée de l'opérateur SFR. L'utilisateur dispose de 15 jours pour s'identifier sur leur site en ligne. Il doit simplement indiquer son nom, prénom, date de naissance et le numéro de sa pièce d'identité sans devoir en fournir une copie ! Tentant dans ce cas d'indiquer des informations erronées... Une adresse mail est également demandée. Là encore, il est facile d'en fournir une acquise pour l'occasion.

Il n'est pas rare aussi pour un enquêteur de faire face à une ligne mobile prépayée dont l'identité fournie par l'opérateur est manifestement fausse avec par exemple :

- **Nom** : XXXyyyssjjekk
- **Prénom** : OkLyMpsQ
- **Date de naissance** : 01/01/2000
- **Adresse** : 1173 avenue de la République 75011 Paris

Comment un tel résultat est-il possible ? Dans certaines petites boutiques de réparation de téléphonie mobile, le vendeur aura pris la peine avant que vous achetiez la carte SIM prépayée, d'enregistrer lui-même l'identité du client, en y mettant de fausses informations.

Cette pratique est régulièrement constatée chez les revendeurs de carte SIM prépayée LEBARA et LYCAMOBILE.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

4. Les opérateurs virtuels

C'est l'occasion d'évoquer ici les « Opérateurs de réseau mobiles virtuels » connu sous le sigle de « MVNO[3] ».

En France, nous disposons de quatre opérateurs officiels ayant chacun leurs propres infrastructures et leurs propres fréquences téléphoniques, à savoir Orange, Bouygues Telecom, SFR et Free Mobile. Ils sont connus sous l'appellation d'« opérateurs historiques ».

Mais nous connaissons tous d'autres opérateurs tels que « La Poste Mobile », « Sosh », « NRJ Mobile », « B&You », etc.

Ces opérateurs virtuels ne possèdent pas d'infrastructure et achètent auprès des quatre opérateurs officiels, des forfaits d'utilisation de leur réseau pour ensuite les revendre sous leur propre marque. Ainsi « Lebara » utilise le réseau de Bouygues Telecom.

Ces « MVNO » étaient absent au début de la mise en place de la PNIJ. Au fil du temps, certains ont été intégrés, mais pour les autres les enquêteurs ont donc recours à la réquisition format papier pour demander à un « MVNO » de fournir les informations d'une ligne mobile.

Ce procédé n'est valable que pour identifier le titulaire de la ligne mobile, car dans le cadre d'une Fadette, le trafic de la ligne mobile transite par l'un des quatre opérateurs les enquêteurs doivent requérir ces opérateurs et non pas le « MVNO » auprès duquel l'abonnement est souscrit.

5. L'application « ON/OFF »

Pour terminer ce chapitre sur l'identification du titulaire d'une ligne mobile, nous ne pouvons faire l'impasse sur l'application « ON/OFF » (disponible sur Apple store et Google Play).

---

[3] Liste des opérateurs mobiles virtuels – Source Wikipédia https://fr.wikipedia.org/wiki/Liste_des_op%C3%A9rateurs_de_r%C3%A9seau_mobile_virtuel#France

« ON/OFF » créée par Taïg Khris, champion français de roller, est une application mobile se basant sur le « cloud number ». Elle permet d'obtenir un numéro de téléphone virtuel et tous ces numéros de mobiles sont mis à disposition en illimité par la société de téléphonie « Transatel ».

Le principe est simple. Il est possible de **disposer de plusieurs numéros de mobiles sur son téléphone en n'ayant qu'une seule et unique carte SIM**, les communications de ces numéros virtuels étant décomptées de votre forfait. L'intérêt est de pouvoir par exemple avoir sur votre téléphone, votre carte SIM avec votre ligne mobile personnelle et utiliser « ON/OFF » pour disposer d'un numéro professionnel, un numéro pour vos annonces sur Leboncoin, etc.

Lors de la souscription mensuelle ou annuelle, vous choisissez votre numéro (avec des options pour un numéro plus simple ou un numéro étranger). Dans l'application, chaque numéro est géré individuellement ainsi vous recevez les appels et les SMS dans un espace réservé à chaque numéro et bien sûr vous pouvez répondre avec ce numéro. Vous pouvez activer ou désactiver les numéros à volonté, personnaliser chaque messagerie, changer de numéro... C'est intuitif. « ON/OFF » utilise le réseau internet mobile pour fonctionner et ne fonctionne que si une carte SIM est insérée dans le mobile. Il est ainsi possible de disposer sur un smartphone d'une dizaine de numéros de mobile.

Dans l'application, vous rentrez le nom et prénom de votre choix, ainsi qu'une adresse email. Rien de plus. **Est-ce une garantie d'anonymat ? Non.**

Lorsqu'un enquêteur va vouloir identifier une ligne mobile délivrée par « ON/OFF », il va obtenir pour résultat « Ligne mobile gérée par Transatel ». La société Transatel revend des numéros de ligne en lots à l'application « ON/OFF ». L'enquêteur saura donc par déduction qu'il s'agit d'une ligne « ON/OFF ».

« ON/OFF » est une société française et elle est donc tenue de

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

répondre aux réquisitions des forces de l'ordre. Par ce biais, « ON/OFF » fournira aux enquêteurs les identifiants de connexion renseignée, l'adresse IP et également le numéro de la dernière carte SIM inséré dans le smartphone ayant utilisé son application.

Alors l'enquêteur connaîtra le numéro de la ligne « réelle » derrière le numéro « ON/OFF ». Il pourra également obtenir la liste de tous les autres numéros « ON/OFF » fournis à l'utilisateur et le détail des communications. Cependant si la carte SIM utilisée dans le smartphone n'est pas identifiable, l'enquêteur se trouvera face à une nouvelle difficulté. « ON/OFF » est également en mesure de fournir le détail du contenu des SMS mais il est raisonnable de penser que l'enquêteur effectuant cette requête aura sollicité une autorisation auprès du magistrat puisqu'il s'agit là d'une interception de communication.

****

Nous l'avons vu dans ce chapitre, identifier le titulaire d'une ligne mobile est assez aisée mais les écueils sont nombreux pour parvenir à celui qui utilise réellement le téléphone tant les astuces sont nombreuses pour celles ou ceux qui cherchent à se dissimuler. En ce qui concerne l'identification d'un utilisateur, les enquêteurs n'obtiennent pas de résultats systématiquement. **Mais il existe une multitude de techniques d'investigation qui se basent essentiellement sur un point : le facteur humain, synonyme d'erreur.**

Conseil stratégique :

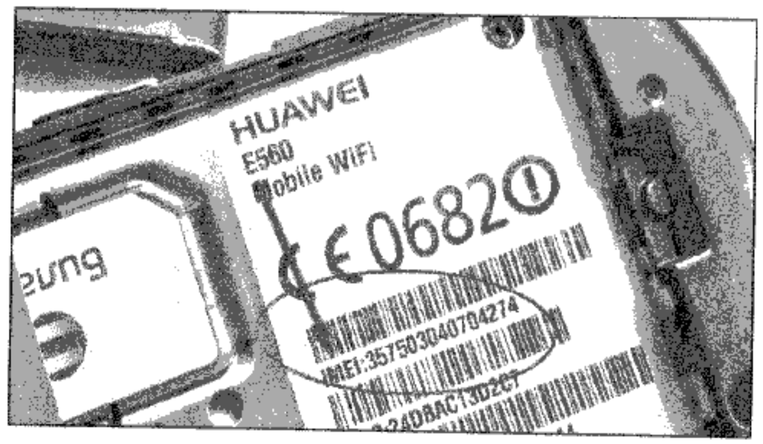
- Le titulaire ou l'abonné de la ligne mobile n'est pas nécessairement l'utilisateur. Si votre client sait qu'il est le titulaire légal de la ligne mobile évoqué, il est utile de préciser rapidement le cas échéant s'il lui arrive de prêter son téléphone mobile ou sa carte SIM.

- La majorité des questions se faisant pressante sur l'identification de l'utilisateur de la ligne, peut-être présumé que cet élément n'a pas encore été pleinement déterminé. Le doute peut-être un atout.
- Un appel « Anonyme » n'est pas anonyme. Le numéro de l'appelant apparaîtra toujours sur une Fadette et permettra une identification.
- La Fadette basée sur les contacts, la géolocalisation à proximité du lieu de domicile ou de travail, voire même les écoutes, sont autant d'éléments qui permettront d'identifier l'utilisateur d'une ligne mobile. Nier être l'utilisateur d'une ligne, c'est être certain de ne pas laisser d'éléments téléphoniques permettant de démontrer le contraire.

6. LES IDENTIFIANTS TECHNIQUES & LE RÉSEAU MOBILE

Avant d'évoquer les Fadettes, nous allons aborder ensemble quelques notions sur le fonctionnement du téléphone mobile et du réseau téléphonique. Même si nous disposons de notions sur ces identifiants, ces termes sont à prendre en compte pour appréhender les investigations dans leur ensemble. Ils sont valables que nous utilisions un téléphone mobile « basique » ou un smartphone.

Le premier identifiant à prendre en compte c'est **le numéro IMEI**. L'identifiant technique (le numéro de série unique) d'un téléphone. Il est visible sur une étiquette collée sous la batterie de téléphone :

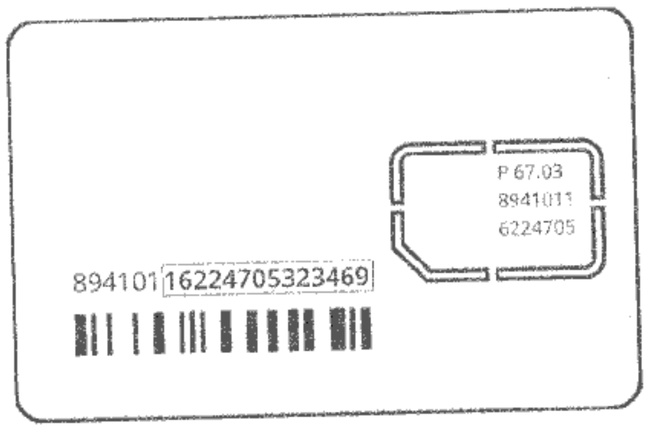


Le numéro IMEI est également disponible en tapant **#06#* sur un téléphone. Nous pouvons tout aussi bien le trouver dans les paramètres du téléphone. Par exemple pour un iPhone, suivez :

Réglages > *Général* > *Informations*.

Le numéro IMEI est composé de 15 chiffres et il est l'équivalent du numéro de série du téléphone. **Il est unique.** Vous pouvez connaître le modèle d'un téléphone à partir de son numéro IMEI sur le site www.imei.info.

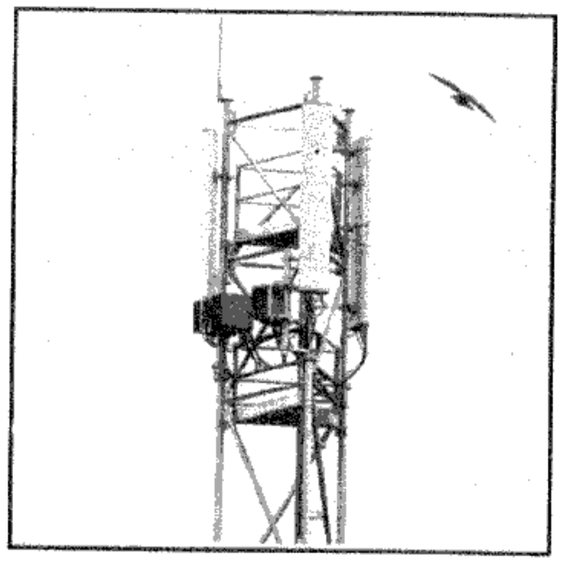
Le second élément à prendre en compte c'est le numéro **ICCID** pour *Integrated Circuit Card Identifier*. Il s'agit du numéro de série de la carte SIM et il se compose d'une suite de 19 chiffres qui permettent d'identifier le pays de provenance de la carte SIM et d'un identifiant propre à l'abonné. **Nous trouverons ce numéro sur le support de carte SIM à côté du code PUK, sur la carte SIM ou dans les informations générales du téléphone.** Il sert notamment à activer une carte SIM quand elle est envoyée à domicile. Ce numéro est propre à la carte SIM.



Le troisième numéro à prendre en compte c'est le numéro **IMSI** pour *International Mobile Subscriber Identity*. Il s'agit de l'identifiant de l'usager sur le réseau. Il est stocké sur votre la SIM et il nous identifie sur le réseau mobile. Ce numéro n'est pas connu de l'abonné utilisateur du téléphone.

Nous disposons donc des identifiants qui seront utilisés par les enquêteurs. Ce qui nous amène au pilier du réseau : l'antenne-relai. Cette antenne est composée de plusieurs cellules.

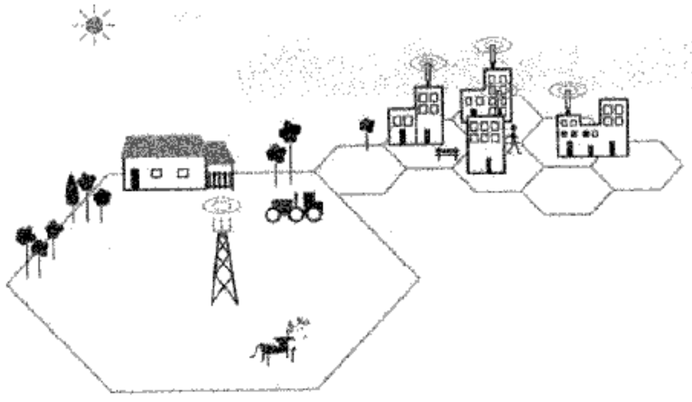
Les cellules de l'antenne-relai transforment le signal électrique en ondes électromagnétiques. Elles sont la base du réseau GSM classique et ont évolué pour apporter les fréquences 3G, 4G et 5G. Plus petites et plus puissantes au fil du temps.



Une antenne-relai est la plupart du temps associée à un opérateur, mais elle peut aussi recevoir les cellules de plusieurs opérateurs. Ainsi, chaque antenne-relai est implantée physiquement à une adresse postale précise ou à des coordonnées GPS. **L'intérêt de connaître cette position exacte est important pour les opérations de géolocalisation.**

Une cellule dispose d'une « couverture », c'est-à-dire le rayon autour d'elle sur lequel elle « diffuse » le réseau téléphonique. **En ville, comme Paris, les cellules sont nombreuses, car elles reçoivent un fort trafic de communication et leur rayon est d'environ 500 mètres. Dans une ville moyenne, la couverture porte entre 1000 à 2000 mètres. En zone rurale, la couverture peut aller de 10 à 20 km.**

Lorsqu'un enquêteur obtient la Fadette d'une ligne mobile, il obtient également la cellule déclenchée pour chaque communication. Il suffit alors d'identifier la cellule sur une carte, de connaître éventuellement sa couverture maximale et l'enquêteur aura cette information : l'individu se trouvait géolocalisé**, dans un rayon de X mètres autour de la cellule.** Ce n'est pas précis, mais c'est une information importante. Nous y reviendrons tout au long du chapitre 9 consacré à la géolocalisation.



Le réseau mobile fonctionne de la façon suivante :

Un téléphone mobile cherche en permanence la cellule de l'antenne-relai la plus proche en termes de signal et de puissance.

Si vous vous déplacez, votre téléphone passera d'une borne relais à une autre et ainsi de suite.

Lorsque vous passez une communication (Appel, SMS, Data), votre téléphone convertit la communication en signaux électromagnétiques transmis jusqu'à la cellule sur une fréquence hertzienne spécifique à l'opérateur.

Cette dernière relaie le signal à travers le réseau qui reconnait l'utilisateur grâce aux numéros IMSI et IMEI.

Le signal arrive au niveau du HLR (Home Location Register). Cet équipement de l'opérateur contient les informations des millions d'abonnés (Numéro IMEI, IMSI, données de votre forfait, etc.) et il est ainsi capable de relayer vos appels et de vous transmettre ceux que vous recevez.

Le HLR via d'autres équipements techniques, a connaissance de la cellule sur laquelle vous vous êtes connecté pour la dernière fois ou celle sur laquelle vous êtes connecté en ce moment. Il peut ainsi identifier sur quelle cellule vous envoyer la communication entrante.

7. LES FADETTES

La Fadette est un terme policier désignant la **« facture détaillée »** des communications entrantes et sortantes d'une ligne mobile (ou fixe).

Dans les chapitres précédents nous avons évoqué les différents moyens mis à dispositions des enquêteurs pour identifier le titulaire d'une ligne mobile et comment fonctionne le réseau mobile avec les différents identifiants techniques qui sont transmis.

Par la suite quand nous parlerons d'un numéro de téléphone, d'un numéro IMEI, IMSI ou ICCID, nous les appellerons **« sélecteurs techniques ».**

Alors, dans quel but requérir une Fadette ? Car il s'agit d'une grande source d'information qui en dit parfois bien plus long sur l'utilisateur de la ligne qu'un placement sous interception judiciaire de communication.

En pratique, une Fadette est très facile à obtenir, car elle est possible dans tous les cadres d'enquête (Préliminaire[1], Flagrance et commission rogatoire) sans autorisations particulière. Il s'agit d'une simple réquisition.

[1] Sous réserve de l'autorisation du Procureur de la République.

La Fadette va renseigner l'enquêteur sur ses interlocuteurs, sur l'utilisateur réel de la ligne, de son usage du téléphone et ses déplacements. Également, obtenir les Fadettes d'autres personnes visées dans l'enquête permettra de savoir quand est-ce qu'elles se sont parlé, potentiellement quand est-ce qu'elles se sont rencontrées. **Les enquêteurs sollicitent très souvent les Fadettes de l'entourage d'un individu malgré le fait que ces proches ne soient pas directement impliqués dans l'affaire.**

Les opérateurs téléphoniques conservent le détail des communications des lignes mobiles pendant un an maximum.

Exemple : Nous sommes le 1er avril 2020 et il est 15h00. Un enquêteur pourra obtenir le détail des communications d'une ligne mobile du 1er avril 2019, 15h au 1er avril 2020, 15h. Impossible de remonter au-delà d'une année.

La Fadette s'obtient en effectuant une réquisition sur la PNIJ auprès de l'opérateur concerné. Elle concerne la prestation « Détail des trafics avec localisation des équipements terminaux d'un abonné ou d'un terminal, accompagné de l'adresse du relai téléphonique (cellule) par lequel les communications ont débuté, sur une période indivisible de 31 jours. » (MT20). L'enquêteur renseigne la ligne mobile concernée et la période souhaitée.

En retour, il obtient un fichier XML ou Excel qu'il va pouvoir injecter dans le logiciel d'investigations téléphoniques Mercure pour une complète analyse.

Pour mieux comprendre ce que contient une Fadette, nous allons prendre l'exemple d'une enquête fictive portant sur un trafic de stupéfiants.

Le Brigadier Dumont enquête sur un trafic de stupéfiants. Son principal suspect se nomme Dimitri Durand. L'enquêteur a effectué des réquisitions au travers de la PNIJ et il a obtenu une réponse : Dimitri dispose d'un abonnement auprès de l'opérateur SFR.

Le Brigadier Dumont souhaite obtenir le détail des communications de Dimitri pour la journée du 1er avril 2020 avec les cellules déclenchées par le mobile. Il effectue donc une réquisition pour obtenir la Fadette géolocalisée de la ligne **33611223344** du 1er février à minuit au 1er février à 23h59.

En retour, l'enquêteur obtient pour résultat un tableau mentionnant les communications de la ligne sur la journée du 1er février :

(Voir tableau page suivante)

	Date	Heure	Abonné	Pays abonné	Correspondant	Pays correspondant	Type
1	mer 01/02/2020	13:05:25	33611223344	France	33601020304	France	VOIX
2	mer 01/02/2020	14:31:23	33611223344	France	33601020304	France	SMS
3	mer 01/02/2020	17:55:45	33611223344	France	34612345678	Espagne	SMS
4	mer 01/02/2020	20:12:30	33611223344	France			DATA

	Sens	Durée	Cellule	Infos cellule [Abonné - début]	IMEI	IMSI
1	S	00:22:14	AED1760731	Place jacques Bainville 75007 PARIS	357631050052050	270017021161295
2	E		AED1760731	Place jacques Bainville 75007 PARIS	357631050052050	270017021161295
3	S		AED1760731	Place jacques Bainville 75007 PARIS	357631050052050	270017021161295
4	S	01:32:56	AEF0192616	24 Rue St Victor 75005 PARIS	358569452578913	270017021161295

Nous avons numéroté chaque ligne de communication afin mieux nous situer dans cet exemple.

Détaillons ensemble les informations de la Fadette de la ligne n° **33611223344** de Dimitri Durand :

- **La date et l'heure** (l'horodatage) correspondent au jour et à l'heure à laquelle débute la communication.

- **L'abonné** correspond à la ligne mobile de Dimitri, objet de la Fadette. La case « pays » nous informe que le numéro de mobile est Français.

- **Le correspondant** est le numéro vers lequel est émise une communication oui qui émet une communication vers la ligne de Dimitri. Idem pour la case « pays », elle nous renseigne sur la provenance du correspondant.

- **« Type »** indique le type de communication à savoir « Voix » pour un appel, « SMS », « MMS » pour un message texte multimédia, « DATA » pour l'usage d'internet.

- **« Sens »** pour le sens de la communication. « E » pour une communication entrante donc reçue par l'abonné et « S » soit sortante, pour une communication émise par l'abonné.

- **« Cellule »** correspond à la cellule (antenne-relai) déclenchée par la communication. Ce qui indique que l'abonné se situait dans la zone couverte par cette cellule au moment du déclenchement de la communication.

- **« Infos cellules »** correspond à l'adresse physique de la cellule déclenchée. Le logiciel Mercure enregistre au fur et à mesure les adresses des cellules et ainsi peut automatiquement en fournir l'emplacement sur une carte.

- **« IMEI »** correspond au numéro IMEI du téléphone utilisé par l'abonné pour passer la communication.

- **« IMSI »** correspond à l'identifiant technique de l'abonné sur le réseau mobile.

Alors que nous apprend la Fadette de Dimitri ? Avec 4 communications, ce dernier utilise peu son téléphone sur la journée du 1er février 2020. Voici ce qu'elle nous apprend :

1. Dimitri n'effectue aucune communication entre minuit et 13h05. Soit son téléphone était éteint, soit il ne l'a pas utilisé.

2. À 13h05, il se trouve à proximité de la place Bainville dans Paris. Il appelle le **33601020304** pendant 22 minutes. L'enquêteur sait que Dimitri habite dans le 7e arrondissement de Paris à 300 mètres de cette place, donc il peut supposer qu'il se trouvait chez lui.

3. À 14h31, il reçoit un SMS du même numéro qu'il a appelé en premier lieu. Il se trouve toujours à priori chez lui.

4. À 17h55, il envoie un SMS à un numéro espagnol.

5. À 20h12, il utilise internet sur son téléphone (DATA) pendant 1h32. Il ne déclenche plus la même contrairement au reste de la journée, mais une autre située 24 rue Saint-Victor à Paris 5e. Il s'est donc déplacé entre 17h55 et 20h12, il a quitté son domicile. Il n'y a pas de correspondant, puisqu'il s'agit d'une connexion sur le Web.

Sur la ligne 4 de la Fadette, nous remarquons que lors de son usage d'internet à 20h12, le numéro IMEI enregistré par l'opérateur a changé, mais pas le numéro IMSI. Dimitri a donc inséré sa carte SIM dans un autre téléphone. Mais dans celui de qui ?

Si l'enquêteur a demandé une Fadette sur ce jour en particulier, c'est grâce à un renseignement d'un informateur « anonyme ». Ce renseignement informe l'enquêteur que Dimitri devait recevoir une livraison de stupéfiants ce jour-là et il aimerait bien savoir avec qui Dimitri a fait affaire.

L'enquêteur se demande si ce téléphone dans lequel Dimitri a inséré sa carte SIM, ne serait pas celui d'un potentiel complice. Pour savoir à qui appartient ce téléphone, l'enquêteur va donc demander une Fadette, non pas à partir du numéro de mobile (il ne dispose pas de cette information), mais à partir du numéro IMEI. **Tout comme pour la recherche du titulaire d'une ligne, il est ainsi possible d'obtenir le trafic des communications d'un autre sélecteur technique, en l'occurrence le numéro IMEI ou IMSI. C'est le principe de la « Fadette inversée ».**

Le Brigadier Dumont va donc requérir les quatre opérateurs historiques par lesquels le trafic mobile transite. Et il leur demandera si l'un d'eux a enregistré sur son réseau l'usage du numéro IMEI **358569452578913**. Le ou les opérateurs concernés lui indiqueront alors l'ensemble des communications passées sur la période demandée et le numéro de mobile ainsi utilisé.

La demande réalisée, l'opérateur Free indique à l'enquêteur qu'habituellement c'est le numéro **33601020304** qui utilise le numéro IMEI **358569452578913**. Ce numéro est le correspondant de Dimitri (ligne 1 et 2). L'enquêteur va identifier ce numéro et constater qu'il appartient à un certain Adrien Pavas.

Cette Fadette nous aura indiqué l'information suivante : **Dimitri et Adrien se sont rencontrés le 1er février à 20h12 à Paris 5e et Dimitri a emprunté le téléphone d'Adrien. Il a inséré sa carte SIM dans le téléphone de ce dernier.**

L'enquête progresse et après avoir fait des recherches auprès des caméras de vidéosurveillance de la ville, le Brigadier Dumont obtient une vidéo datée du 1er février à 20h15 où Dimitri rencontre

un individu impossible à identifier, dans la zone de couverture de la cellule au 24 Rue Saint-Victor à Paris.

L'individu embarque dans son sac un gros sachet. Nous sommes le 2 février, il est 6h du matin et l'enquêteur décide de perquisitionner l'appartement d'Adrien Pavas. Lors de cette opération, il découvre un sachet d'un kilo d'herbe de cannabis.

En garde à vue, interrogé sur ses complices, Adrien ne veut rien dire. Dimitri est lui aussi immédiatement placé en garde à vue et nie connaître Adrien. **Les enquêteurs disposent du téléphone d'Adrien et du numéro IMEI correspondant parfaitement à celui relevé de la Fadette de Dimitri. Ils ont ainsi la preuve que les deux hommes se sont rencontrés ce jour à l'heure de la vidéo surveillance.**

Devant la preuve irréfutable apportée par la téléphonie, Dimitri et Adrien admettront s'être rencontrés et avoir ainsi procédé à la transaction autour du sachet d'herbe de cannabis.

Les enquêteurs pourraient en conséquence, demander les Fadettes de Dimitri et d'Adrien sur une année complète. Ils pourraient ainsi donc matérialiser l'ensemble des rencontres des deux complices grâce aux cellules qu'ils auraient déclenchées simultanément.

La Fadette de notre exemple est volontairement succincte. En réalité, avec l'usage des smartphones, les Fadettes sur un mois ou plus, sont emplies de ligne « DATA » **(ce qui permet une meilleure géolocalisation puisqu'il y a une indication fréquente des cellules déclenchées).**

Elles comportent la plupart du temps des milliers de communications et c'est à ce moment que Mercure intervient afin de permettre aux enquêteurs de classer les contacts par fréquences, d'indiquer les numéros IMEI utilisés par la ligne, de matérialiser les déplacements sur une carte et les endroits les plus fréquentés, etc..

Il apparaît difficilement envisageable pour un avocat d'étudier l'ensemble des Fadettes d'un dossier pénal en l'absence de logiciel d'exploitation (même s'il est bien sûr possible de faire l'acquisition d'une licence d'utilisation de Mercure). Bien souvent, l'exploitation des informations se base sur le procès-verbal rédigé par l'enquêteur et sans possibilités d'un réel échange contradictoire. Il peut toutefois s'avérer intéressant de demander une copie numérique des Fadettes et par le biais de quelques manipulations de l'ouvrir sur un tableur. Ainsi les filtres et les outils de recherches sur Excel permettront dans un premier temps d'éclaircir le tout. Il est utile de vérifier les déductions des enquêteurs pour rectifier le sens donné à l'exploitation des données. Parfois dans une Fadette, quelques lignes plus haut ou plus bas, un élément litigieux qui aurait été initialement omis pourra être mis en exergue. Prenez le temps si nécessaire d'étudier les Fadettes, elles peuvent parfois révéler un élément capital.

Dans la continuité de cette enquête fictive relative à un trafic de stupéfiants, nous allons aborder les différentes recherches et réflexions possibles pour les enquêteurs.

8. EXPLOITATIONS DES FADETTES : CAS PRATIQUES

L'utilisation de Fadettes complétée d'une analyse des données par Mercure permet bien souvent de progresser rapidement au sein d'une enquête judiciaire et d'obtenir des éléments de preuves qui nécessiteront d'être exploités mais permettront la découverte d'élément de preuve essentiel.

Plus que jamais aujourd'hui, les procédures judiciaires sont abreuvées d'éléments provenant d'investigations téléphoniques et il devient difficile de nier la force probante des éléments issus de ces recherches. En qualité de Conseil, il est important de maîtriser les principaux aspects de l'analyse des données téléphoniques et notamment des Fadettes afin d'appréhender la méthode de réflexion de l'enquêteur et ses capacités d'investigations.

Nous savons à présent quels éléments techniques composent une Fadette et nous allons voir de quelle manière ils peuvent être exploités. La Fadette a pour vocation d'être injectée à Mercure pour être comparée aux autres données déjà obtenues. **Toutefois, l'enquêteur doit savoir ce qu'il cherche ou tout du moins disposer de quelques pistes de réflexion.**

Pour vous permettre de mieux cerner le fonctionnement des investigations téléphoniques et quelles sont les informations que les enquêteurs peuvent en extraire, nous allons nous appuyer sur plusieurs cas pratiques d'analyse des données. Les recherches faites par les enquêteurs sont le fruit d'une question simple. Ainsi nous allons aborder un ensemble de cas, les plus courants en matière d'enquête, en nous basant sur l'enquête fictive initiée au précédent chapitre.

L'ensemble des analyses présenté n'engage que l'auteur et son expérience en matière de téléphonie d'investigation. De multiples possibilités de requêtes sont possibles et nous abordons ici les plus fréquentes.

1. Changement de carte SIM : identifier la nouvelle ligne d'un individu

Dimitri pressent que la police est sur ces traces, il fait preuve de précaution et il jette sa carte SIM, pressentant que son numéro est identifié et sous surveillance. Ainsi, il entre dans une boutique et repart avec une carte SIM prépayée.

Hypothèse A : Dimitri change de numéro et d'opérateur, mais il a pris soin de déclarer son identité. L'enquêteur n'aura plus qu'à effectuer une réquisition auprès de tous les opérateurs avec une recherche par nom/prénom/date de naissance et il obtiendra le nouveau numéro de Dimitri.

Hypothèse B : Dimitri a jeté sa carte SIM, mais il a gardé le même téléphone. Ce même téléphone dont l'enquêteur connaît le numéro IMEI grâce à la Fadette du 1er février 2020.

L'enquêteur établit une réquisition dite « inversée » sur la base du numéro IMEI précédemment utilisé.

Rappelons-nous que lors d'une communication, le réseau enregistre le numéro IMEI du téléphone et les identifiants de la carte SIM. L'enquêteur sollicite les opérateurs afin d'obtenir la Fadette non pas à partir du numéro de mobile, mais à partir du numéro IMEI. Il obtient ainsi la liste des cartes SIM insérées dans le téléphone et le numéro associé. Il peut donc retrouver la trace de la carte SIM et le numéro que nous connaissions déjà dans un premier temps, mais surtout il peut obtenir l'identifiant de la nouvelle carte SIM de Dimitri et le numéro associé à celle-ci.

Ainsi, l'individu qui change de carte SIM sans changer de téléphone mobile sera identifiable grâce à ce dernier et son numéro IMEI.

****

Un nouveau problème s'ajoute à notre exemple et va venir compliquer la tâche du Brigadier Dumont. Dimitri a acheté une nouvelle carte SIM et un nouveau téléphone mais il a jeté l'ancien téléphone et n'a pas enregistré son identité pour l'abonnement.

Il s'agit d'un changement complet rendant impossible une recherche à partir du numéro IMEI.

Solution A : L'enquêteur dispose de la Fadette de Dimitri sur plusieurs mois. Il dispose également de la liste des 5 ou 10 contacts que Dimitri appelle le plus fréquemment. À savoir sa maman, son grand frère, son meilleur ami et sa sœur. L'enquêteur peut fortement envisager que Dimitri appellera ses proches avec sa nouvelle ligne mobile.

Le Brigadier Dumont va donc demander une Fadette des lignes mobiles des personnes que Dimitri contacte le plus régulièrement en temps normal. Et il va effectuer cette demande à compter du jour où il a cessé de constater des communications sur la ligne connue de Dimitri. Il effectue cette réquisition pour les lignes de Maman, le grand frère, le meilleur ami et la sœur.

C'est sur Mercure que le tri va s'opérer à l'aide de **l'outil « numéros communs ».** En toute logique :

- Les Fadettes du grand frère et de la sœur auront en commun la ligne de la mère et l'ancienne ligne de Dimitri.

- La mère et le grand frère auront en commun le numéro de la sœur. Etc.

Ce qu'il ressort de cette analyse, c'est que tous les quatre ont en communs l'ancien numéro de Dimitri. Ils l'ont tous contacté ou auront reçu des appels de cet ancien numéro. Et il y a de fortes probabilités pour qu'ils aient en commun le nouveau numéro de Dimitri qui les aura appelés avec.

Il suffira donc de vérifier si ces quatre personnes du cercle « familial » ont en commun un nouveau numéro inconnu de l'enquêteur et cela à la date à laquelle la ligne de Dimitri a cessé d'émettre.

Bien entendu, ce schéma est modulable. L'enquêteur en fonction du profil de Dimitri aurait pu faire la même chose à partir des Fadettes de tous les amis de Dimitri, de tous ces collègues ou de tous les joueurs de son club de tennis. Si les investigations ne fournissent aucun élément, l'enquêteur orientera sa recherche sur d'autres individus de l'environnement de Dimitri.

Solution B : L'enquêteur va parier ici sur le hasard, mais il n'est pas inutile de vérifier via une recherche inversée sur IMEI si les membres de la famille ou les amis n'ont pas inséré dans leur téléphone une nouvelle carte SIM.

À ce stade, l'élément important pour orienter l'enquêteur, c'est le changement d'habitude pour la personne ciblée ou son entourage.

Imaginons que le frère de Dimitri utilise toujours depuis un an le même numéro, le même téléphone, la même carte SIM, aucune variation perceptible. Et au détour des dernières communications de sa ligne, il aura inséré une fois, une carte SIM inconnue. C'est sur ce détail que l'enquêteur portera son attention.

Dans cette hypothèse qu'un proche aurait prêté son téléphone à Dimitri, il est important de vérifier leurs dernières communications. À ce moment, ce qu'il faut déterminer, ce sont les habitudes de ses proches et lire entre les lignes de la Fadette si un sélecteur technique a changé et permet d'aiguiller l'enquête.

Dans la continuité, si l'enquêteur sait que Dimitri a déjà utilisé par le passé d'autres téléphones, il lui faudra effectuer des Fadettes inversées sur tous les numéros IMEI précédemment utilisés par le suspect. D'où l'intérêt pour Dimitri de ne pas réutiliser d'anciens téléphones.

Dans les deux dernières solutions proposées, ce qui risque probablement de mener Dimitri aux enquêteurs, c'est son entourage familial et amical, car il les aura contactés avec la ligne qu'il semble vouloir dissimuler. Et garder le même téléphone ne ferait que faciliter le travail des enquêteurs.

Nous étudions ici une technique efficace, la recherche de trafic (Fadette inversée) à partir d'un numéro IMEI. **Elle permet de tracer systématiquement chaque carte SIM insérée dans n'importe quel mobile sur une période d'un an.**

2. Classer et identifier l'ensemble des contacts d'un individu

Le Brigadier Dumont enquête sur les potentiels complices de Dimitri et Adrien. Il n'a pas pu suivre les deux comparses assez longtemps pour identifier tous les individus gravitant autour de ce trafic.

La première chose à faire sera de lister tous les contacts téléphoniques de Dimitri et Adrien.

Pour cela, les enquêteurs auront demandé une Fadette sur une période d'un an (ou moins si le trafic a commencé il y a moins d'un an) pour les lignes de Dimitri et d'Adrien.

Prenons pour exemple la Fadette de Dimitri qui comporte un total de 6571 communications (Voix, SMS, MMS, Data) et 96 correspondants sur une période d'un an. À l'aide de Mercure, l'enquêteur va trier les correspondants par nombres de communications (occurrences). Il va à l'aide de plusieurs « filtres » masquer tout ce qu'ils appellent les numéros « techniques » ou « marketing » (N° court, N° de services clients, N° d'entreprises) pour raffiner le résultat final.

Il reste 54 numéros dits « particulier » appartenant à des personnes physiques ayant été en contact avec Dimitri. Nous affichons ici les 10 correspondants principaux par ordre décroissant :

Ordre	Occurrences	Correspondants
1	1080	33712131415
2	452	33621222324
3	387	33634333231
4	156	33698979695
5	142	33641434245
6	112	33609080706
7	91	33601020304
8	47	33665676869
9	45	33659585754
10	38	33661696764

Nous visualisons ici les 10 numéros que Dimitri a contactés le plus souvent sur une période d'un an. Les occurrences correspondent aux nombres de communications passées ou reçues avec chaque numéro.

Il y a un numéro en 7e position, déjà connue de l'enquête, le **33601020304** utilisé et appartenant à Adrien Pavas, complice de Dimitri. Ils ont échangé au total 91 communications sur l'année.

Pour identifier les autres abonnés, le Brigadier Dumont devra procéder via la PNIJ une « identification en nombre d'abonnés ». **C'est une réquisition où il est possible de faire identifier jusqu'à 300 numéros de téléphone, en une seule fois.**

La plateforme « Aerope » qui sert à connaître l'opérateur d'un numéro de mobile propose aussi toutefois une fonction d'identification de masse. L'enquêteur n'a plus qu'à charger un fichier extrait de Mercure, contenant la liste de tous les contacts de Dimitri, remplir une réquisition et l'envoyer via la PNIJ. **Il est donc possible d'identifier les titulaires de lignes en très grand nombre, presque par millier en quelques réquisitions.**

En retour sur la PNIJ, l'enquêteur reçoit un fichier contenant toutes les identifications demandées. Il n'a plus qu'à l'importer dans Mercure pour que le logiciel associe chaque numéro à une identité (avec les informations obtenues en sus).

Voici le résultat pour l'identification des 9 principaux contacts non identifiés de Dimitri :

Ordre	Occurrences	Correspondants	Titulaire
1	1080	33712131415	Jocelyne DURAND 58 Rue de l'université 75008 Paris
2	452	33621222324	Kévin DURAND 58 Rue de l'université 75008 Paris
3	387	33634333231	Samy Lavergne 12, av du cotentin 95000 Pontoise
4	156	33698979695	Mathilde DURAND 129 av du Général de Gaulle 92200 Neuilly-Sur-Seine
5	142	33641434245	Tom Lelouche 65 Allee du bois 78160 Marly Le roi
6	112	33609080706	Jennifer Abomba 78 Rue de la sentinelle 93100 Montreuil
7	91	33601020304	Adrien Pavas 44 Av de la République 75010 Paris
8	47	33665676869	Lucile Lerdameur 12 Rue Coriolis 75012 Paris
9	45	33659585754	Patrick Calvin 36 rue du Bastion 75017 Paris
10	38	33661696764	Alberto Torteli 52 Sentier du pin 66000 Perpignan

Bien entendu, le Brigadier Dumont aurait pu procéder à l'identification des 96 correspondants de Dimitri, mais il a estimé que les 10 principaux étaient suffisants.

Nous constatons ainsi que Jocelyne Durand, sa mère, est le principal contact de Dimitri, suivi de son frère Kévin, son meilleur ami Samy et sa sœur Mathilde.

Nous avons donc répondu à l'interrogation n°2 à savoir classer et identifier les contacts d'un individu. Mais les complices de Dimitri et Adrien ne sont pas encore identifiés.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

3. Comparer les numéros en communs entre plusieurs individus

À ce stade, après avoir identifié les contacts principaux de Dimitri, il est difficile de dire pour les enquêteurs qui seraient le ou les complices. Mais si complices il y a, ils doivent avoir eu des contacts avec Dimitri et Adrien.

Via la PNIJ, le Brigadier Dumont va demander la Fadette de la ligne d'Adrien Pavas sur l'année écoulée. Après l'avoir intégré à Mercure, il va procéder à la même opération de classement et d'identification des contacts qu'avec la ligne de Dimitri.

Dans son dossier sur Mercure (les Fadettes de Dimitri et d'Adrien apparaissent sur un espace partagé avec les autres enquêteurs du groupe), notre enquêteur va sélectionner la Fadette de Dimitri et choisir l'option « numéros communs ». **C'est une option qui permet de déterminer quels sont les numéros en communs entre deux ou plusieurs Fadettes.**

Ici par exemple, nous allons comparer les numéros en communs entre les Fadettes de Dimitri et d'Adrien. Résultat :

Numéros	33611223344 [Dimitri]	33601020304 [Adrien]
33611223344	0	119
33601020304	91	0
33698979695	156	589
33641434245	146	78
33661696764	38	67

En toute logique, Dimitri et Adrien ont leurs numéros respectifs en commun. Ils se sont appelés mutuellement et ainsi Dimitri a eu 91 contacts avec Adrien et ce dernier a eu 119 contacts avec Dimitri.

La ligne **33698979695** appartient à la sœur de Dimitri. C'est un numéro commun aux Fadettes de Dimitri et Adrien. Adrien qui a donc eu 589 contacts avec la sœur de Dimitri.

Les deux mis en cause ont également deux autres numéros en communs, le **33641434245** identifié à Tom Lelouche et le **3361696764** identifié à Alberto Torteli.

Nous excluons la sœur de Dimitri de la liste des suspects potentiels. Sur tous leurs correspondants, Dimitri et Adrien ont deux numéros communs et ils méritent de l'attention, car orientés sur cette piste, le Brigadier Dumont a découvert à l'aide du TAJ que Tom et Alberto avaient déjà été inquiétés dans un trafic de stupéfiants.

4. Identifier les téléphones utilisés par plusieurs individus (IMEI commun)

La recherche par numéros communs s'applique également aux autres sélecteurs techniques tels qu'IMEI ou IMSI. **Il est à ce titre tout à fait possible de savoir si Dimitri et Adrien ont utilisé les mêmes téléphones portables.** Exemple :

IMEI	33611223344 [Dimitri]	33601020304 [Adrien]
355764923425780	9	14
358569452578913	37	12745
357631050052050	6525	26

Le **N° IMEI 358569452578913** (Ligne 2) est celui du téléphone d'Adrien comme le montre le volume de communication (12745). Il apparaît dans la Fadette de **Dimitri donc ce dernier a inséré sa carte SIM dans le téléphone d'Adrien 37 fois.** Mercure permettra à l'enquêteur de visualiser en détail chacune de ces 37 communications (avec donc l'horodatage et la localisation de la cellule déclenchée).

Le **N° IMEI 357631050052050** (Ligne 3) est celui de Dimitri. *(Voir Fadette Dimitri du 1er avril 2020 - chapitre 7.)* Son numéro IMEI apparaît 26 fois dans la Fadette d'Adrien. Adrien a donc inséré sa carte SIM dans le téléphone de Dimitri à 26 reprises.

Le **N° IMEI en ligne 1** est inconnu des enquêteurs jusqu'à ce jour, mais Dimitri et Adrien ont utilisé à plusieurs reprises ce téléphone. **À charge pour l'enquêteur de déterminer pourquoi et à qui appartient ce téléphone**. Quelle est la pertinence de cette information dans l'enquête en cours ?

Ce qu'il faut retenir de cette dernière recherche, c'est que les enquêteurs seront toujours en mesure de savoir quand une ligne a été insérée dans un autre téléphone et à qui le téléphone a pu être prêté.

Vous avez ici l'exemple type des investigations téléphoniques à tiroirs, car une Fadette en amène une autre, la découverte d'un nouveau numéro IMEI relance les recherches et ainsi de suite.

5. L'analyse du profil d'un utilisateur en fonction de son profil d'usage du mobile

Il s'agit d'un procès-verbal courant appelé « Exploitation de la ligne mobile 336XXXXXXXX utilisé par le dénommé X ».

Il intègre principalement les identifications des contacts, les téléphones utilisés (IMEI), la période d'utilisation, l'analyse des localisations de la ligne, mais il se base aussi avant tout sur « l'usage » fait de la ligne et les déductions qui peuvent être faites sur les habitudes de son utilisateur.

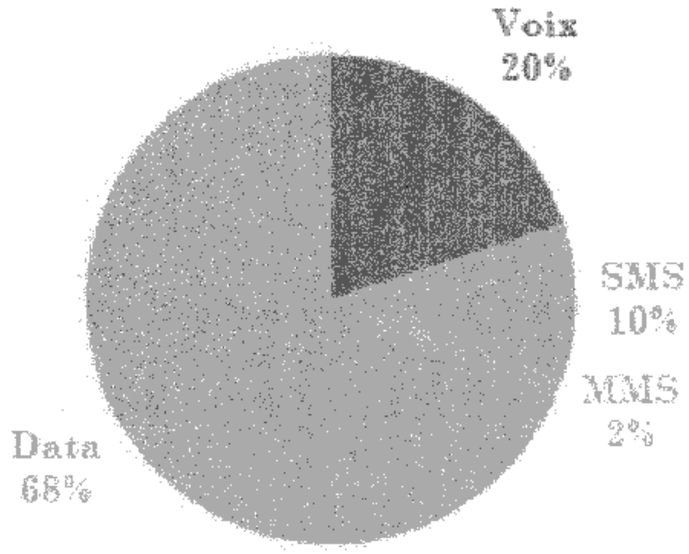
La fonction « rapport d'analyse » du logiciel Mercure permet d'établir un profil rapide et complet. Il consiste à prendre en compte les milliers de communications d'une Fadette pour analyser l'usage de communications voix, SMS, MMS, Data, la

répartition du sens des communications, les plages horaires d'utilisations et les localisations les plus fréquentes.

Pour illustrer nos propos, appuyons-nous sur une Fadette fictive comportant 20 000 communications sur une année.

La répartition des communications :

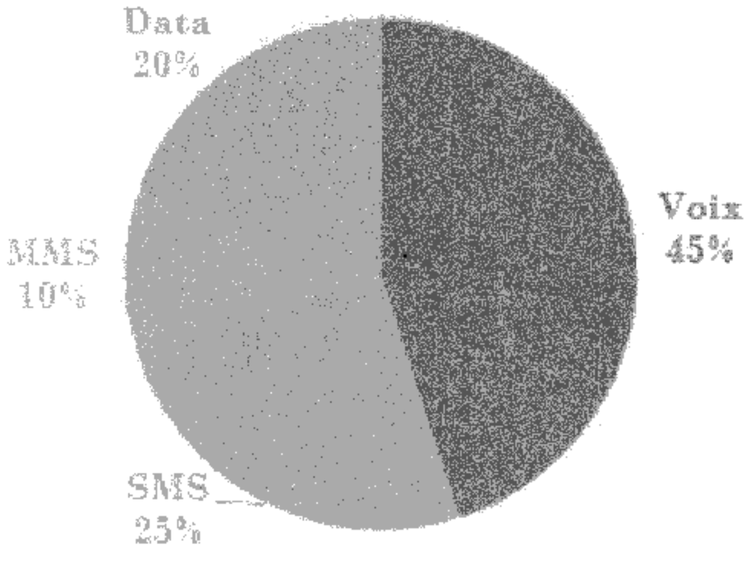
PROFIL 1



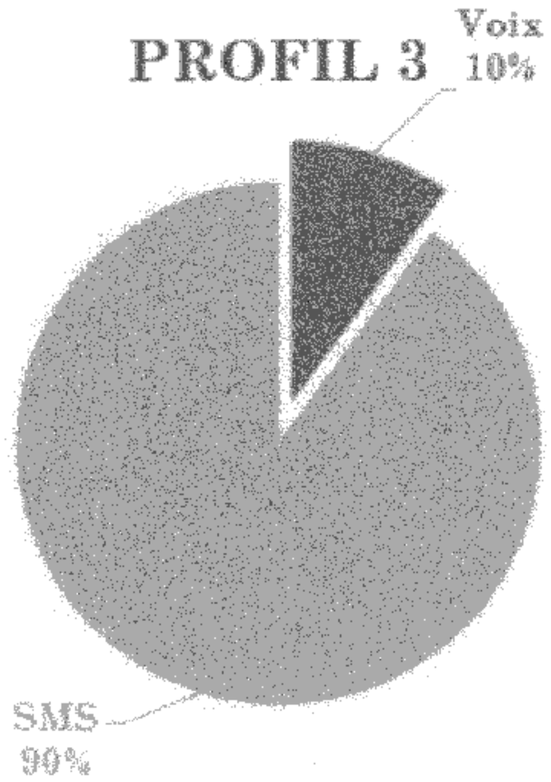
Le **profil** 1 indique que l'utilisateur à un usage majoritairement « internet » (data) à 68% au détriment des appels vocaux et des SMS.

Cela indique qu'il est soit adepte des réseaux sociaux ou **soit qu'il utilise majoritairement des applications de messageries « classique » ou chiffrées**. C'est un indicateur qui incitera l'enquêteur à analyser plus en détail ces applications ainsi qu'à prospecter sur les réseaux sociaux.

PROFIL 2



Le **profil 2** est un utilisateur dit « Normal ». Il passe beaucoup de temps au téléphone et privilégie les appels aux SMS. Il préfère communiquer directement avec ses interlocuteurs et son usage « data » est limité aux fonctions de bases d'un smartphone et ne laisse pas sous-entendre un usage « poussé ».

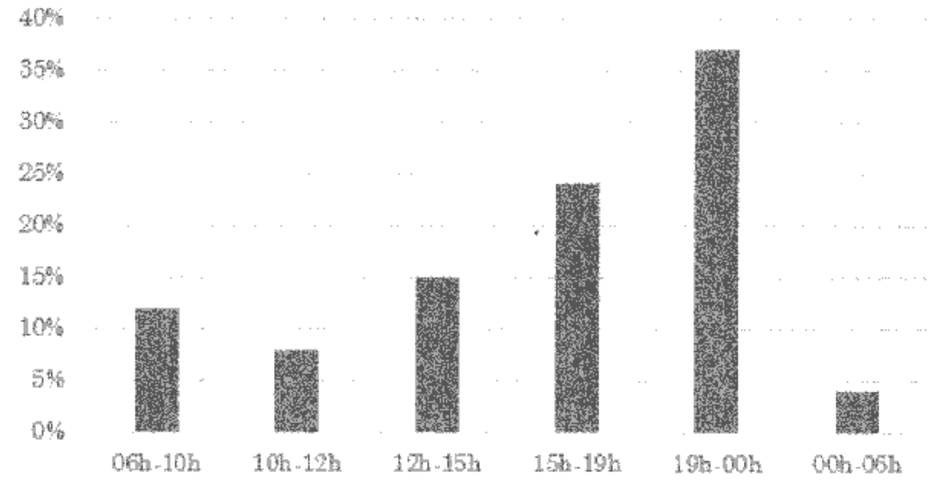


Le **profil 3** est atypique. **L'absence de Data et de MMS indique qu'il s'agit d'un téléphone basique**. Il s'agit là très probablement d'un téléphone « jetable » prépayé. L'utilisateur communique de façon directe par SMS et parfois par « voix ». Il peut s'agir d'un téléphone de « travail » si l'enquête porte sur un trafic de stupéfiants. A contrario, il peut tout simplement s'agir d'une personne souhaitant un téléphone basique.

La répartition des communications dans le rapport d'analyse reste très subjective. **Elle apporte un réel intérêt quand un profil atypique se dégage tel que dans l'exemple du profil n°3.**

Les périodes d'utilisation :

Les 20 000 communications analysées par Mercure offrent une vision complète des habitudes de l'utilisateur de la ligne. Ainsi le logiciel, classe les communications par tranche horaire ou par jour, ce qui permet d'appréhender le comportement de l'utilisateur.

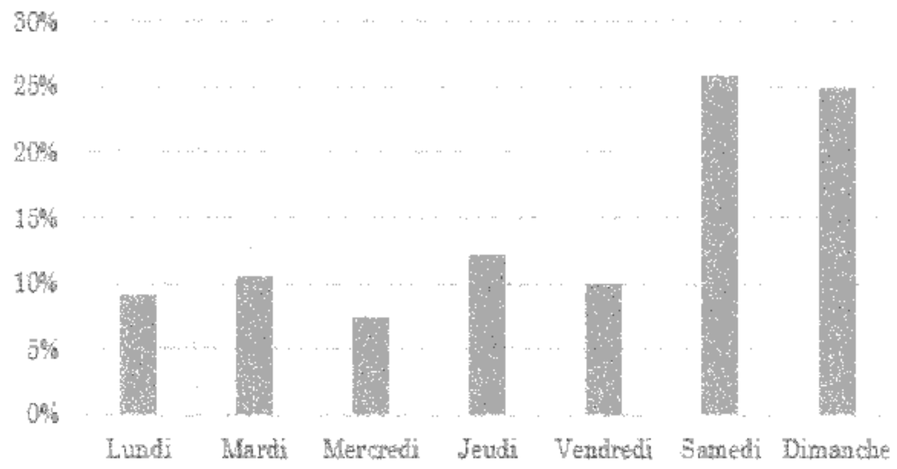


Le graphique ci-dessus met en avant de façon synthétique les tranches horaires sur lesquelles sont passées les communications de la ligne.

L'individu utilisant la ligne mobile étudiée est une personne qui travaille sur des horaires de bureau. L'essentiel de l'activité est concentré sur la tranche 19h – minuit après le travail, là où l'intéressé dispose de temps libre pour communiquer. Vient en second la tranche 12h-15h, correspondant certainement à une pause déjeuner. Pour finir, sur la tranche des horaires de nuit, l'utilisateur est très peu actif.

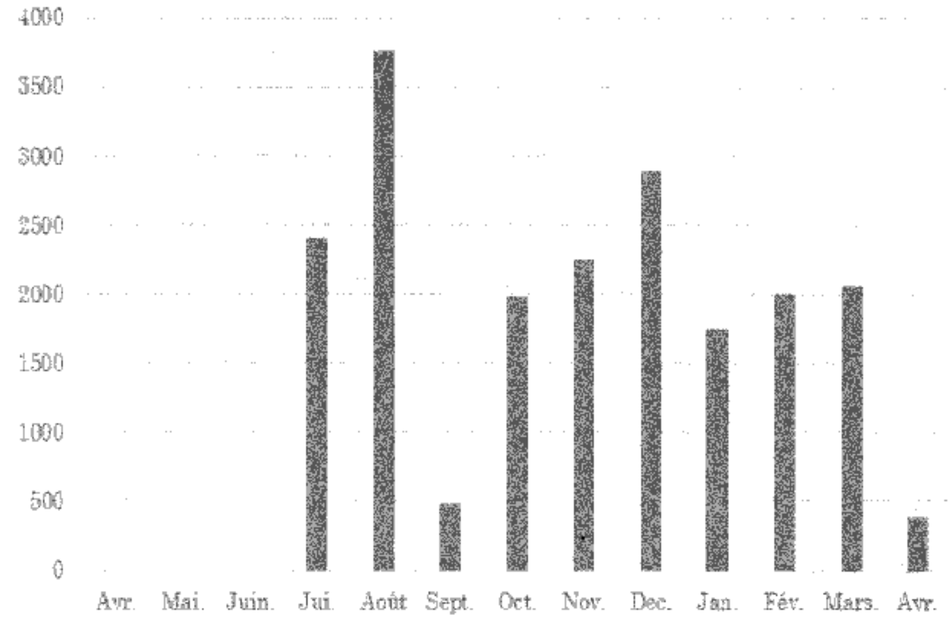
Un utilisateur de ligne mobile qui serait très peu actif le matin et très actif le soir et la nuit, c'est un autre indicateur qui permet de supposer que soit il travaille de nuit ou qu'il n'a pas d'emploi et s'adonne à d'autres activités. Là encore, il ne faut pas tirer de conclusion hâtive.

L'analyse des communications s'effectue également par jour d'utilisation :



En corrélation avec l'analyse sur tranche « horaire », l'analyse des jours d'utilisation confirme des habitudes d'un utilisateur ayant un rythme de travail hebdomadaire et ne travaillant pas le week-end où les communications sont beaucoup plus nombreuses.

Et pour finir l'analyse des « périodes d'utilisation » de la ligne, nous pouvons compléter avec une vue d'ensemble sur l'année de la Fadette :



Sur l'analyse « annuelle », on constate l'absence de communications sur les mois d'avril, mai et juin. La ligne a donc commencé à être utilisée en juillet. L'individu aurait probablement utilisé une autre ligne avant cette date. Il faudra donc vérifier la date de début d'abonnement de la ligne.

En septembre, il y a très peu de communications en comparaison du reste de l'année. Une recherche approfondie permettra de constater que l'utilisateur est parti en vacances à l'étranger durant ce mois.

Le mois d'avril de cette année est peu fourni en communication, car l'enquêteur a effectué la demande de Fadette au cours du mois.

Les localisations les plus fréquentes :

C'est un des éléments les plus intéressants du rapport d'analyse d'utilisation de la ligne.

Où est-ce que l'utilisateur se trouve le plus souvent localisé ? Chaque communication étant localisée par la cellule déclenchée, il est donc aisé d'établir un classement :

	Cellule [Adresse]
1	70 RUE DE FLANDRES 75019 PARIS-19E-ARRONDISSEMENT
2	11 R RIQUET 75019 PARIS-19E-ARRONDISSEMENT
3	55 R RIQUET METRO RIQUET 75019 PARIS-19E-ARRONDISSEMENT
4	8 R NICOLET 75018 PARIS-18E-ARRONDISSEMENT
5	52 R DES POISSONNIERS 75018 PARIS-18E-ARRONDISSEMENT

Dans cet exemple, la majorité des communications sont passées dans un périmètre couvert par les cellules se situant proches de la station de métro « Riquet » à Paris 19e.

Il apparaît donc que l'utilisateur réside dans ce secteur ou du moins s'y trouve hébergé. Pour s'assurer de cette information, il est possible de classer les localisations les plus fréquentes par tranche horaire en sélectionnant celle de soirée et de nuit :

	Cellule [Adresse]
19h-00h	70 RUE DE FLANDRES 75019 PARIS-19E-ARRONDISSEMENT
00h-06h	70 RUE DE FLANDRES 75019 PARIS-19E-ARRONDISSEMENT

Le constat est sans appel, sur une période de plusieurs mois, le soir et la nuit, l'utilisateur déclenche le plus souvent la cellule située au 70 rue des Flandres à Paris 19e. Cela conforte l'hypothèse qu'il réside sur ce secteur mais dans le cas où une personne désactive sa carte SIM le soir, il sera difficile de déterminer son secteur de résidence.

Ce type de recherches et de classement a aussi pour but de corréler des informations obtenues par le biais des différents fichiers police (TAJ, SNPC, SIV etc). Cela permet par exemple de confirmer une adresse.

6. Suivre les déplacements de l'utilisateur d'une ligne mobile

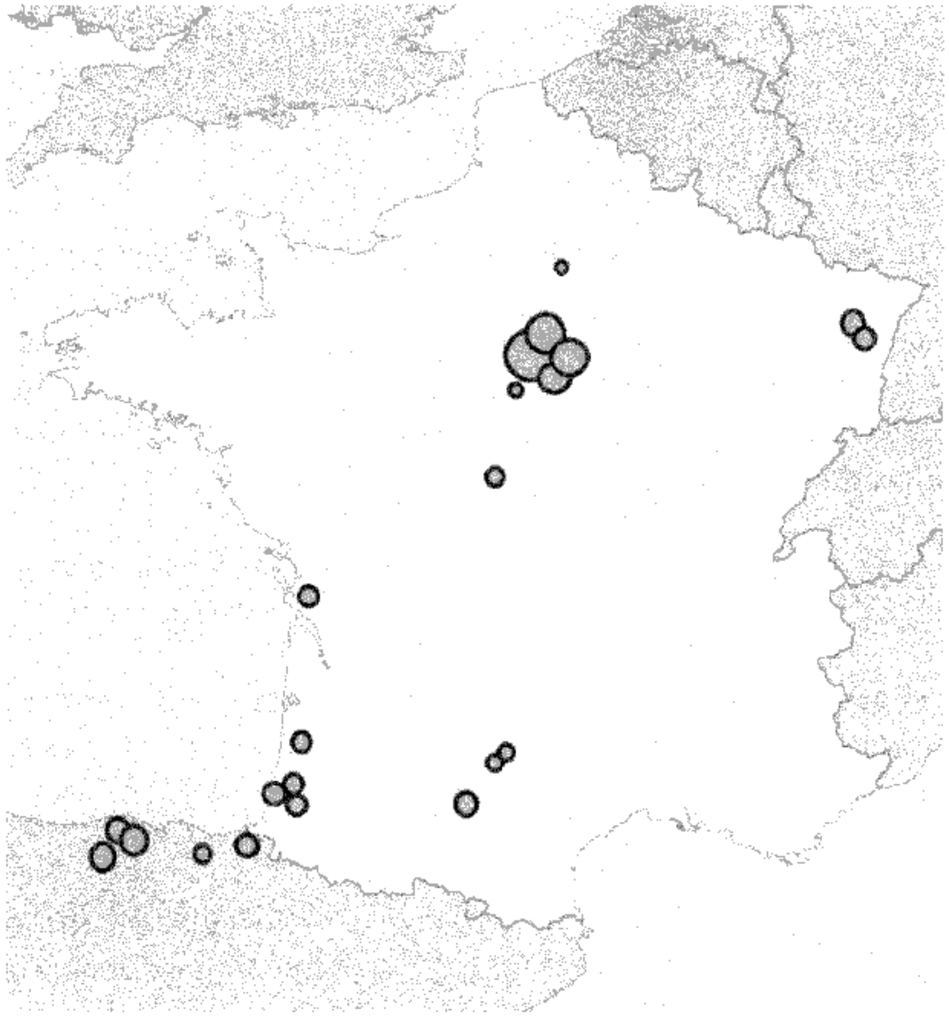
Avant même de parler de mesure de géolocalisation sur une ligne mobile, **l'analyse des cellules déclenchées par une ligne mobile permet de matérialiser sur une carte via Mercure l'ensemble de ces déplacements.**

Si la Fadette est réalisée sur la période maximale d'un an, l'enquêteur disposera des déplacements de l'utilisateur sur un an.

Si tous les éléments de l'enquête permettent d'affirmer que l'utilisateur de la ligne est bien celui qui tient en main le téléphone, les déplacements faits avec celui-ci lui seront attribués.

Le Brigadier Dumont a réussi à prouver que Dimitri est l'utilisateur réel de la ligne 33611223344. Il s'intéresse donc à ces déplacements du 1er février 2019 au 1er février 2020. Un onglet sous Mercure lui permet ainsi de visualiser les trajets effectués par Dimitri avec son téléphone.

Les secteurs qui concentrent le plus de déclenchements de cellules de la part de la ligne mobile du suspect sont matérialisés sur une carte :



La carte en fournit un aperçu. Nous savons que Dimitri réside dans le 7e arrondissement de Paris. Donc il se trouve majoritairement localisé en région Parisienne. Cependant, l'enquêteur peut observer des déplacements en province tels qu'un séjour à Strasbourg, Toulouse ou encore Bayonne.

Et un élément l'intrigue, **un séjour à Bilbao en Espagne ainsi que plusieurs localisations autour de la frontière franco-espagnole.**

Un simple clic sur les localisations signalées sur la carte permettra à l'enquêteur de connaître les dates auxquelles Dimitri s'est rendu en Espagne (ou dans les autres villes) et il pourra déterminer les dates et le nombre de séjours.

La Fadette initiale portant sur le 1er février 2020 faisait apparaître l'envoi d'un SMS par Dimitri à un numéro espagnol, le **+3412345678**. L'enquêteur pourra vérifier sur la Fadette en remontant sur l'année complète, le nombre de contacts que Dimitri a eu avec ce numéro espagnol et si ces contacts ont été effectués sur les périodes où il se rendait en Espagne.

De nombreux trafics de stupéfiants passent par l'Espagne et s'il s'avère que Dimitri s'est fourni là-bas, le Brigadier Dumont pourra comptabiliser le nombre de trajets effectués et poursuivre son enquête sur les différentes ramifications du trafic mis à jour.

L'enquêteur dispose d'un outil performant qui lui permet sur la carte en question de zoomer et dézoomer sur les points de localisation qui attire son attention. Il peut obtenir également la liste de communications correspondantes au secteur géographique choisi.

7. Identifier les rencontres entre deux individus

Plus les enquêteurs injecteront de données dans Mercure et plus ils obtiendront d'informations sur les différents mis en cause de l'enquête.

Nous avons vu plus haut comment visualiser sur une carte les déplacements d'un individu et à postériori en connaître les détails exacts.

La fonction « points de rencontre » va au-delà en permettant de visualiser les possibles rencontres entre deux (ou plusieurs) utilisateurs de ligne mobile. Pour exacte, cette fonction matérialise la présence des lignes mobiles et leur bornage à partir d'une fourchette de distance et de temps.

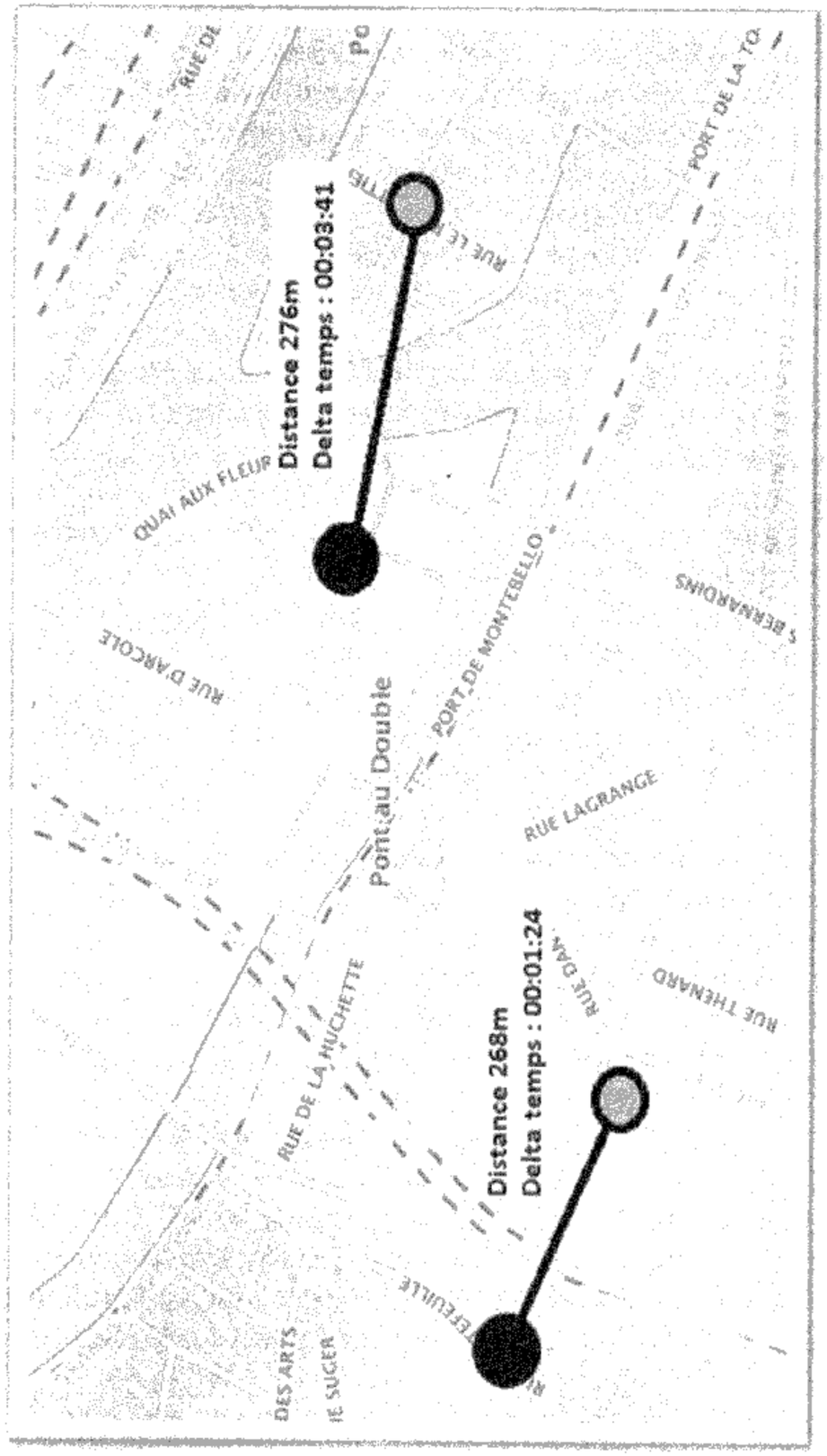
Mercure compare les différentes cellules déclenchées de deux ou plusieurs Fadettes. Ainsi, l'enquêteur prédéfini un réglage à savoir la distance maximum entre les cellules et le temps maximum entre les horodatages et leurs déclenchements.

Exemple : L'enquêteur souhaite connaître les différentes rencontres entre Dimitri et Adrien qui peuvent être déterminées par les communications effectuées avec leur ligne mobile. Pour cela, il sollicite la fonction « Point de rencontre » sous Mercure et prédéfinit un réglage avec un maximum de 300 mètres entre les cellules déclenchées et dans un laps de temps inférieur à 5 minutes.

Mercure fournira l'ensemble des communications passées par les deux individus et pour lesquelles les lignes auront été localisées à moins de 300 mètres l'une de l'autre avec un maximum de 5 minutes entre les localisations.

Le Brigadier Dumont souhaite savoir quand Dimitri et son complice Adrien se sont vus sur la journée du 8 mars 2020. Pour cela, il programme la fonction « points de rencontre » sur cette date avec le réglage distance (300m) et temps écoulé (5min).

(Voir résultat sur le plan page suivante)



Les deux premiers points observés se situent à proximité du boulevard Saint-Michel à Paris. Pour la journée du 8 mars 2020, en comparant les Fadettes de Dimitri et d'Adrien, Mercure met en avant un déclenchement de cellules proches l'une des autres. Dimitri (point gris) déclenche une cellule située à 268 mètres d'une cellule déclenchée par Adrien (point noir). Ces communications ayant déclenché les cellules ont été passées dans un intervalle de 1 minute et 24 secondes.

Pour résumer : Dimitri utilise son téléphone à 14h35 sur cellule à moins de 300 mètres de celle déclenchée par Adrien à 14h36min24sec.

L'enquêteur va donc affirmer qu'Adrien et Dimitri étaient ensemble.

Sur les seconds points situés sur l'île de la Cité, le scénario se reproduit. Deux cellules déclenchées à 276 mètres l'une de l'autre et 3min41 sec entre les deux communications. Les appels ont eu lieu à 14h48min et à 14h51min41sec. Là encore, le Brigadier Dumont avance que Dimitri et Adrien étaient ensemble et que ce n'est pas une coïncidence s'ils se trouvaient le même jour, à la même heure, dans le même secteur.

L'exemple serait encore plus parlant si les points de rencontre étaient situés en zone rurale avec une seule antenne-relai à des kilomètres à la ronde.

Il faut néanmoins se montrer prudent avant d'affirmer grâce à la téléphonie que deux ou plusieurs personnes se sont rencontrées « physiquement ». Votre client pouvait très bien s'être rendu chez son épicier favori ou chez un ami, ce jour-là, au même moment. Et ce ne serait que pure coïncidence. **Ce qui importe c'est le réglage opéré sous Mercure pour déterminer les points de rencontre.**

Plus la distance est courte et plus le temps écoulé entre les communications est court, plus il est facile d'affirmer une rencontre entre deux utilisateurs de ligne mobile. Si l'enquêteur règle sur distance 200 mètre et laps de temps 1 minute, le calibrage est précis et le résultat beaucoup plus probant.

En revanche, si l'enquêteur règle la recherche à toutes les communications ayant eu lieu sur une « distance de 5 kilomètres et laps de temps 20 minutes », c'est ce qu'il s'appelle « ratisser large. » Il obtiendra des résultats c'est certain, mais beaucoup plus contestables. Cela revient à affirmer que deux personnes se sont vues, car elles se trouvaient dans un rayon de 5km entre deux cellules (soit au plus fort 20km entre elles) dans un laps de temps de 20 minutes. **Il s'agit là d'un élément important à préciser par l'enquêteur si cela n'est pas mentionné au procès-verbal : faire préciser le critère de recherche pour les points de rencontre si votre client conteste la réalité de celles-ci.**

Pour l'enquêteur, le risque est d'effectuer un calibrage trop serré dans sa recherche et de passer à côté d'une rencontre réelle où la distance entre cellules et le laps de temps se trouvaient légèrement au-dessus des valeurs sélectionnées.

Dans le cas de Dimitri et Adrien, le Brigadier Dumont pourra demander les « points de rencontre » sur toute la période couverte par les deux Fadettes. Il obtiendra en conséquence la liste sur carte de toutes les rencontres de deux hommes selon les critères choisis.

Si l'enquêteur intègre aussi les Fadettes d'autres protagonistes, il pourra effectuer la même démarche en comparant les points de rencontre de l'ensemble des Fadettes et matérialiser les rencontres des utilisateurs, en groupe.

L'outil « points de rencontre » est simple et puissant à la fois en termes d'investigation, car il se base uniquement sur les localisations des communications.

Ce type de recherches **est régulièrement mis en avant au sein des procédures quand deux ou plusieurs personnes nient avoir pu**

un jour se rencontrer physiquement et avoir été ensemble à un moment donné au même endroit.

Néanmoins la précision de cet outil est liée aux nombres de communications d'une ligne. Si la Fadette présente peu ou pas de communication, il y aura donc peu de cellules déclenchées et par conséquent tous les rapprochements pouvant être fait avec seront restreints.

8. Obtenir les communications d'un individu utilisant une ligne étrangère

Cette démarche fait appel à des notions déjà évoquées en amont au sujet des Fadettes inversées :

Cas N° 1 : L'individu utilise sur le réseau français une carte SIM provenant d'un autre pays. L'enquêteur sollicitera les quatre opérateurs historiques pour connaître le détail des communications transitant sur leurs réseaux avec cette ligne étrangère. Et dans la continuité, il sera possible de connaître le numéro IMEI, faire une Fadette inversée, savoir si d'autres puces ont transité par le téléphone de l'individu, etc. Tout sera récupérable. **Utiliser une puce étrangère en France ne permet pas à un utilisateur de se soustraire aux investigations.**

Cas N° 2 : L'individu se trouve à l'étranger et utilise donc une carte SIM étrangère. Dans ce cas, impossible de connaître les communications qu'il passe dans le pays où il se trouve (sauf par le biais de la coopération internationale).

Néanmoins, il est possible de connaître le détail des communications qu'il a passées avec des numéros français. Sur le principe de la recherche inversée, l'enquêteur sollicitera auprès des opérateurs sur la PNIJ, la liste des numéros français ayant été en contact avec le numéro étranger visé. Intégré à Mercure ce résultat permettra de lister l'ensemble des contacts de l'individu en France.

9. Réaliser une recherche à partir du trafic détaillé d'une cellule (antenne-relai)

Sur la PNIJ, un enquêteur peut solliciter l'obtention de **toutes les communications ayant transité par une cellule**.

Une cellule enregistre que ce soit en ville ou à la campagne, un nombre incalculable de communications à chaque instant. La PNIJ limite donc la requête à une période de 4 heures. Et sur 4h de temps, le résultat se chiffre en dizaines de milliers de communications.

C'est une prestation à utiliser avec parcimonie, car elle est généralement demandée sur un évènement exceptionnel de grande ampleur, quand les enquêteurs sont dans l'incertitude et qu'ils cherchent à « geler » les données de téléphonie d'un secteur pour exploiter si besoin le résultat ultérieurement.

Une antenne-relai peut héberger plusieurs cellules, de plusieurs opérateurs et gérant plusieurs fréquences (2G, 3G ou 4G). Il faudra ainsi solliciter le trafic pour chaque cellule d'une antenne-relai et le résultat est exponentiel. Plusieurs raisons peuvent pousser les enquêteurs à solliciter une telle requête, mais nous allons prendre un exemple concret :

Les enquêteurs ne savent pas quels numéros de téléphone utilisent les mis en cause. Un crime a été commis Place de la République à Paris et en revanche ils savent que quelques heures plus tard les individus ont été aperçus dans le centre-ville de Lille.

En analysant les données issues du trafic des cellules proches des lieux des faits, il sera possible « d'isoler » les numéros et téléphones (par IMEI) s'étant trouvés à 18h à Paris 10^{e} (en choisissant les cellules les plus proches du lieu des faits) et à 22h aux alentours de leur dernière localisation à Lille.

Plusieurs personnes auront pu faire le trajet depuis la place de la République jusqu'à Lille dans ce laps de temps, mais le résultat sera beaucoup plus mince et permettra d'isoler moins d'une

dizaine de lignes « suspectes ».

L'analyse des Fadettes permettra de se concentrer sur celles dont le profil des titulaires intéresse le plus les enquêteurs. Si plusieurs personnes sont suspectées, à l'aide des fadettes obtenues sur la période d'une année, il sera également possible de voir si ces lignes se sont « rencontré » dans d'autres lieux à d'autres occasions, ce qui réduira le champ des investigations.

****

En conclusion de ce chapitre, vous avez pu constater que l'analyse de Fadette fournit énormément d'informations précises et qu'il est important de poser les bonnes questions pour obtenir le meilleur résultat. Le potentiel de Mercure est intéressant quand l'ensemble des fonctions est bien maîtrisé par les enquêteurs.

L'ensemble des traces laissées par l'usage d'un téléphone mobile sont autant d'indices fragilisant les déclarations d'un mis en cause. Et malgré un usage précautionneux, c'est bien souvent le facteur humain qui trahit l'utilisateur.

9. LA GÉOLOCALISATION EN TEMPS RÉEL

Les Fadettes permettent d'obtenir sur simple réquisition l'ensemble des communications d'une ligne mobile assorti de la localisation de la cellule déclenchée et ainsi tracer les itinéraires de l'utilisateur. Il n'est donc pas possible d'obtenir une information de la position en temps réel, car la Fadette est obtenue quelques minutes après la demande, il y a donc un décalage.

Pour obtenir une position régulière, il faudrait redemander une Fadette chaque fois que nécessaire. De surcroit, la localisation d'une cellule indique la présence de l'utilisateur dans une zone de couverture réseau, ce qui réduit le degré de précision.

Si la ligne mobile visée n'émet aucune communication, les enquêteurs ne disposent donc d'aucune géolocalisation. C'est ici qu'intervient donc le placement sous géolocalisation en temps réel d'une ligne mobile.

La géolocalisation d'une ligne mobile, se traduit par le suivi dynamique de ses positions, en temps réel et ceci que le téléphone émette des communications ou non. Néanmoins, la géolocalisation d'une ligne mobile fonctionne uniquement grâce aux antennes-relais. **Ce n'est en aucun cas une géolocalisation à partir du GPS du téléphone.**

1. Cadre légal et durée de la mesure de géolocalisation

La géolocalisation et son cadre légal sont définis par le Code de procédure pénale de l'article 230-32 à l'article 230-44. Ces articles définissent les règles applicables au placement sous mesure de géolocalisation pour un terminal mobile (téléphone), mais aussi la géolocalisation d'un véhicule ou de tout autre objet (à l'aide d'une balise GPS).

La géolocalisation à postériori d'une ligne mobile à l'aide du bornage des communications contenues dans les Fadettes ne constitue pas une mesure de géolocalisation en temps réel[1].

La mesure de géolocalisation ne peut être utilisée que pour les enquêtes portant sur des crimes ou délits punis d'au moins 3 ans d'emprisonnement par le Code pénal. Mais elle concerne aussi les enquêtes portant sur les recherches de la cause de la mort d'une personne ou de sa disparition, et sur les personnes en fuite.

Seul un OPJ est habilité à mettre en place la mesure. Un APJ peut également le faire, sous l'autorité de l'OPJ.

La durée :

Article 230-33 du code de procédure pénale

L'opération mentionnée à l'article 230-32 est autorisée :
1° Dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une procédure prévue aux articles 74 à 74-2, par le procureur de la République, pour une durée maximale de quinze jours consécutifs dans les cas prévus aux articles 74 à 74-2 ou lorsque l'enquête porte sur un crime ou sur une infraction mentionnée aux articles 706-73 ou 706-73-1, ou pour une durée maximale de huit jours consécutifs dans les autres cas. À l'issue de ces délais, cette opération est autorisée par le juge des libertés et de la détention à la requête du procureur de la République, pour une durée maximale d'un mois renouvelable dans les mêmes conditions de forme et de durée ;

2° Dans le cadre d'une instruction ou d'une information pour recherche des causes de la mort ou des causes de la disparition mentionnées aux articles 74, 74-1 et 80-4, par le juge d'instruction, pour une durée maximale de quatre mois renouvelables dans les mêmes conditions de forme et de durée.

La durée totale de cette opération ne peut pas excéder un an ou, s'il s'agit d'une infraction prévue aux articles 706-73 ou 706-73-1, deux ans.

La décision du procureur de la République, du juge des libertés et de la détention ou du juge d'instruction est écrite et motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

Dans le cas d'une enquête préliminaire ou une enquête de flagrance, la mesure est autorisée par le procureur de la République.

- **15 jours si l'enquête porte sur des crimes ou délits prévus aux articles 706-73 à 706-73-1 du Code procédure pénale** (Délinquance et criminalité organisées).

- **8 jours pour toutes les autres infractions** (punies de plus de 3 ans d'emprisonnement)

Passé ces délais de 15 ou 8 jours, le procureur de la République doit saisir sur requête motivée, le juge des libertés et de la détention, pour solliciter une autorisation pour la poursuite de la géolocalisation.

[1] Crim ., 22 novembre 2011, N°11-84308
Crim., 22 novembre 2016, N°16-82376

Le juge des libertés et de la détention peut autoriser sur décision motivée, la géolocalisation pour une durée d'un mois renouvelable.

La décision du juge des libertés et de la détention porte sur un numéro de mobile ou IMEI bien précis et il n'y a donc pas d'autorisation « générale ». **Si la personne visée change de mobile et de carte SIM, il faut de nouveau effectuer une demande.**

Dans le cadre d'une commission rogatoire, le juge d'instruction peut autoriser l'OPJ à procéder aux mesures de géolocalisation pour une durée maximale de **4 mois, renouvelable.**

Arrivé au terme de chaque autorisation, l'enquêteur doit solliciter le procureur de la République ou le juge d'instruction afin de renouveler l'autorisation.

Peu importe le cas, la mesure de géolocalisation ne peut excéder :

- **1 an**

ou

- **2 ans si l'enquête porte sur des infractions liées à la délinquance et criminalité organisée ou à caractère terroriste**

2. Mise en place du suivi dynamique et fonctionnement de la géolocalisation

Une fois les autorisations obtenues (du Parquet, du JLD ou du juge d'instruction), l'enquêteur doit rédiger un procès-verbal de mise en place et de début de la mesure.

À noter qu'une géolocalisation en temps réel est possible sur une ligne mobile mais également sur un numéro IMEI (par conséquent, un changement de carte SIM n'empêche pas la

géolocalisation).

À la fin de délai autorisé, l'enquêteur rédige un procès-verbal mentionnant la fin de la mesure. (S'il s'agit d'une balise pour véhicule, il doit acter le retrait du dispositif de géolocalisation.)

Toute géolocalisation qui serait réalisée en dehors des délais autorisés ou dont les opérations de mise en place, de début et de retrait qui ne seraient pas actées sont invalidées.

Une fois la géolocalisation terminée, l'enquêteur place sous scellé le support contenant le détail de l'ensemble des géolocalisations obtenues et horodatées.

Pour mettre en place une mesure de géolocalisation sur une ligne mobile, l'enquêteur sollicite dans un premier temps l'opérateur téléphonique concerné par le biais d'une réquisition afin de lui demander la mise en place d'un suivi dynamique sur le numéro autorisé. Les techniciens de l'opérateur procéderont à la réalisation de la partie « technique » sur leur réseau.

La Plateforme Nationale des Interceptions Judiciaires est prévue techniquement pour permettre la mise en place et le suivi des géolocalisations en temps réel. Néanmoins, il semble qu'à ce stade cette fonctionnalité ne soit pas opérationnelle.

La police a donc recours à une société extérieure pour réaliser la géolocalisation.

Il s'agit de la société **Deveryware** (43, rue Taitbout, 75009 Paris) qui se présente comme un acteur historique de la géolocalisation en temps réel.

L'enquêteur devra requérir en même temps que l'opérateur téléphonique, la société Deveryware pour assurer la mise en place de la mesure de géolocalisation.

DEVERYWARE
Sécurité

L'accès à la plateforme « Deveryloc » de la société Deveryware permet à l'enquêteur de suivre sur une carte la position de la ligne mobile. Et si dans une enquête, plusieurs géolocalisations sont en cours, il peut également afficher l'ensemble des lignes sur une seule carte.

Pour obtenir une position de la ligne mobile géolocalisée, Deveryware envoie un signal à travers le réseau téléphonique pour savoir sur quelle cellule le téléphone est localisé.

L'enquêteur peut à travers la plateforme régler la fréquence à laquelle il souhaite obtenir une « position ». Cela peut aller d'une position toutes les 30 secondes à plusieurs minutes, voir même plusieurs heures. **C'est un système basé sur le principe du « SMS Silencieux ». Un SMS qui ne s'affichera pas à l'écran est envoyé vers le mobile ce qui indiquera sur quelle cellule il est connecté.**

Mais attention, plus il y a de « SMS silencieux » envoyé de façon très régulière, plus la batterie du téléphone se décharge vite... Ce qui peut être un indicateur d'une géolocalisation en cours.

Deveryware facture la prestation en fonction du nombre de positions demandées sur l'ensemble de la période de géolocalisation. Plus les enquêteurs sollicitent des positions fréquentes, plus le coût de la réquisition est élevé.

La position obtenue n'est pas celle d'un GPS, mais bel et bien celle d'une cellule d'antenne-relai. Donc la position de l'utilisateur se situe dans la zone de couverture de la cellule.

Bien entendu, la technologie permet une triangulation grâce aux cellules pour obtenir une géolocalisation suffisamment précise.

À tout moment, l'enquêteur peut solliciter une position de la ligne. **Si le téléphone n'est pas connecté au réseau (éteint ou en mode avion), il n'y aura aucune géolocalisation disponible. Il est possible que la carte SIM soit désactivée, mais que l'individu utilise les messageries par le biais de la connexion WiFi du mobile.**

L'enquêteur a également accès à l'historique complet des positions. Ainsi s'il ne s'est pas connecté durant quelque temps pour voir les positions de la ligne mobile, il peut retracer sur une carte les différents trajets effectués.

La plateforme « Deveryloc » a développé un système d'alerte par notifications qui s'avère très efficace. En effet, l'enquêteur peut définir des « zones d'alerte ». Ainsi, il peut par exemple paramétrer des alertes qu'il recevra quand la ligne géolocalisée quittera une zone définie (un rayon défini autour de son domicile par exemple) ou quand il rentrera dans une zone. Il peut aussi obtenir une alerte quand le téléphone quittera le territoire ou quand il cessera d'être allumé pendant un certain temps. **Ces fonctionnalités sont utiles pour être informées rapidement d'un changement important dans l'utilisation ou dans la géolocalisation de la ligne.**

Les enquêteurs œuvrant sur un dossier sensible avec des lignes géolocalisées et qui souhaitent régulièrement s'informer des positions des cibles ne restent pas jour et nuit au bureau. Pour qu'ils puissent accéder à la plateforme Deveryware depuis n'importe quel accès internet, la société dispose d'une application mobile nommée « Deveryloc ».

Les procès-verbaux indispensables à la réalisation d'une géolocalisation en temps réel sur un téléphone mobile (à partir du numéro d'appel ou du numéro IMEI) :

- Procès-verbal actant la réception de l'autorisation écrite[2] de placement d'une ligne mobile sous mesure de géolocalisation en temps réel. (Autorisation émise par le Parquet ou le Juge d'instruction – Mesure de prolongation autorisée par le JLD le cas échéant).
  Le rapport de demande d'autorisation transmis à l'autorité judiciaire est annexé à l'autorisation reprenant les motifs exposés pour solliciter la mise en place de la mesure.

- Procès-verbaux de réquisition transmis à l'opérateur gestionnaire de la ligne visée et réquisition transmise à la société Deveryware (les dates de mise en place et de cessation de la mesure doivent être mentionnées).

- Procès-verbal de mise en place et d'effectivité de la mesure de géolocalisation. (Les articles relatifs à la géolocalisation doivent être visés en entête ainsi que le rappel de l'autorisation obtenue).

- Procès-verbal de cessation de la mesure.

- Placement sous scellé sur support numérique (ou papier si peu de données) de l'ensemble des données recueillies par le dispositif le temps de la mesure.

[2] L'autorisation écrite et motivée doit être antérieure à l'effectivité de la mesure de géolocalisation.

10. LES INTERCEPTIONS DE COMMUNICATIONS (ÉCOUTES TÉLÉPHONIQUES)

Les écoutes téléphoniques dans le cadre judiciaire représentent un atout majeur pour les enquêteurs. Elles sont très encadrées sur le plan législatif, mais elle reste néanmoins extrêmement attentatoire à la vie privée de nos concitoyens. Alors qu'elles devraient représenter la dernière mesure mise en place, les autorisations de placement d'une ligne sous interceptions de communications ont connu un bond spectaculaire ces dernières années. La PNIJ fait état à ce jour d'une moyenne de 10 000 lignes placées sur écoute en permanence.

L'évolution permanente des technologies de communications a toutefois drastiquement atténué la pertinence des écoutes téléphoniques. La VoIP, les messageries chiffrées ont limité les capacités d'interceptions. Toutefois les interceptions restent utiles, car premièrement tout le monde n'est pas familier de l'usage d'applications de messageries chiffrées et deuxièmement, l'usage des appels « classiques » laisse des éléments exploitables non négligeables pour la procédure pénale.

Il peut paraître évident qu'aujourd'hui, un mis en cause aurait tendance à ne pas s'exprimer pleinement lors d'une conversation téléphonique pouvant le mettre directement en cause sur le plan judiciaire. Mais les habitudes de vies, ses contacts, leurs degrés de proximités, des noms, des adresses, des pseudonymes, peuvent être une source importante d'indices utiles aux enquêteurs.

Les écoutes téléphoniques soulèvent au sein de la société de nombreuses interrogations, notamment parce que leur fonctionnement et leur utilisation sont méconnus.

La technique se révèle totalement transparente et invisible pour l'utilisateur. Il n'y a pas de grésillement sur une ligne écoutée, pas d'écho ou de « bip sonore ». Il s'agit là de légendes urbaines.

Bien évidemment, à l'époque où les enquêteurs se branchaient directement sur la ligne fixe pour l'intercepter et l'enregistrer sur bande magnétique, les indices étaient nombreux. Aujourd'hui, l'interception de la communication se fait à la « source ».

Une écoute téléphonique se nomme techniquement une **« interception judiciaire de communication »**, les enquêteurs parlent entre eux de « branchement d'une ligne ».

1. Cadre légal et durée des interceptions de communications :

Dans le cadre d'une enquête préliminaire ou une enquête de flagrance, l'interception de communication n'est possible uniquement que dans le cadre de la délinquance et la criminalité organisée.

Le placement sur écoute se fait sur autorisation du JLD sur requête du procureur de la République pour une durée maximale **d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée** *(article 706-95 du Code de Procédure Pénale)*.

Les interceptions de communications sont principalement réalisées dans le cadre d'une instruction et l'autorisation est

délivrée par le juge d'instruction. *(Articles 100 à 100-8 du Code procédure pénale)*.

L'autorisation d'interception n'est possible que pour les crimes et délits punis d'au moins 3 ans d'emprisonnement.

Le juge d'instruction autorise la mesure pour une durée **de 4 mois. Elle est renouvelable dans la limite d'un an. La durée est portée à 2 ans dans le cas d'infractions liées à la criminalité en bande organisée et les infractions à caractères terroristes.** *(Articles 706-73 du Code de procédure pénale.)*

Bon à savoir : Les enquêteurs disposent d'un temps d'écoute maximal d'un mois, voire deux, dans le cadre d'enquête préliminaire ou de flagrance. Ils peuvent s'ils le souhaitent « fractionner » ce temps d'écoute en plusieurs fois selon les besoins de l'enquête.

Il existe plusieurs exceptions aux interceptions de communication pour les professions spécifiques :

- Aucune interception ne peut avoir lieu sur la ligne d'un **député ou d'un sénateur** sans que le président de l'Assemblée nationale en soit informé.
- Aucune interception ne peut avoir lieu sur la ligne du **cabinet ou du domicile d'un magistrat** sans que le Premier président ou le procureur général de la Cour d'appel où il réside n'en soit informé.
- Aucune interception ne peut avoir lieu sur la ligne du **cabinet ou du domicile d'un avocat** sans que le bâtonnier en soit informé.

Les communications entre un client et son avocat sont inviolables et ne peuvent faire l'objet de retranscription que dans des cas exceptionnels. En effet, à la lumière d'indices graves et concordants laissant présumer la commission d'infraction par ce dernier, la décision de placement sur écoute de la ligne

téléphonique d'un avocat peut être ordonnée. Toutefois, il est aisé de contourner ce principe d'inviolabilité. En effet, lorsqu'un enquêteur place sous interception la ligne d'un suspect, il est susceptible d'écouter des conversations pourtant frappées du sceau du secret liant l'avocat à son client.

Cette problématique a été parfaitement illustrée par l'affaire dite « Bismuth » mettant en cause Nicolas Sarkozy et son avocat, Me Thierry Herzog dans le cadre de laquelle les conversations ont été entendues, interprétées et ont pu donner lieu à des actes d'enquête complémentaires. En application de la pratique policière des écoutes dites « filantes », les enquêteurs laissent une interception se dérouler même si elle ne présente plus d'intérêt pour l'enquête en cours. Pourtant, si elles permettent de révéler d'autres agissements frauduleux, elles seront utilisées.

Ce procès médiatique fut l'occasion de mettre en exergue l'atteinte au secret des correspondances entre un client et son avocat. Plusieurs arrêts rendus le 22 mars 2016 par la Chambre Criminelle de la Cour de Cassation valident la transcription des interceptions de communication entre Nicolas Sarkozy et son avocat, Me Thierry Herzog. Ces transcriptions issues de l'affaire dite du « financement libyen » ont pu être versées légalement dans la procédure distincte ouverte pour trafic d'influence, corruption active et recel de violation du secret professionnel.

Ces arrêts ont distingué néanmoins deux points importants :

- La protection des correspondances avocats/clients s'applique de manière générale même si l'avocat n'est pas encore régulièrement désigné et même si le client n'est pas encore formellement mis en cause dans la procédure dans laquelle les écoutes ont lieu.

- Les interceptions sur la ligne d'un mis en cause discutant avec son avocat (ou sur la ligne d'un avocat dans le respect de la procédure d'information du bâtonnier) mettant en avant la participation de l'avocat à la commission d'infractions, peuvent faire l'objet de transcription.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

En tout état de cause, toute interception de ligne qui serait réalisée en dehors de l'autorisation d'un magistrat ou en dehors des délais prescrits sera considérée comme irrégulière.

2. Mise en place et fonctionnement d'une interception de communication :

Une fois l'autorisation d'interception d'une ligne téléphonique obtenue, l'enquêteur transmet via la PNIJ, une réquisition judiciaire précisant la ligne visée et la durée, à l'opérateur téléphonique. S'il s'agit d'un MVNO (Opérateur virtuel tel que Lebara, La poste Mobile etc.), l'enquêteur adresse sa réquisition à l'opérateur historique en charge du réseau de ce MVNO. L'opérateur procède ainsi au « branchement » de la ligne visée par l'autorisation du magistrat.

(Particularité : Si la cible change régulièrement de carte SIM, mais pas de mobile, il est possible d'intercepter non pas le numéro de mobile, mais le n°IMEI ainsi, peu importe que la cible change de ligne, il sera toujours possible d'intercepter les communications transitant sur le téléphone.)

Le branchement de la ligne mobile consiste par le biais d'un ordinateur de commutation, à copier et transférer les données vers la PNIJ. Le réseau copie les données transitant par la ligne et les transfère sur le réseau de la PNIJ. Il s'agit là d'une opération totalement transparente pour l'utilisateur de la ligne.

Il nous faut évoquer une particularité liée à la 4G qui a modifié ces dernières années le protocole d'interception de communication. Les appels passés par une ligne sur le réseau 4G sont « numérisés » et transitent via le réseau internet pour arriver à destination. Il s'agit de la VoIP (Voice over Internet Protocol). Il a fallu de nombreuses mises à jour régulières pour que la PNIJ soit en

mesure de recevoir les appels passés en 4G et être capable de les lire.

3. Comment l'enquêteur accède-t-il aux informations interceptées ?

Une fois l'interception mise en place sur la ligne mobile, l'enquêteur peut accéder aux résultats de plusieurs façons :

- **Sur la PNIJ** : Sur l'écran d'accueil du dossier relatif à l'interception, l'enquêteur recevra une notification pour chaque communication interceptée. Également, en consultant l'onglet dédié à la ligne interceptée, l'enquêteur aura accès à l'ensemble des communications classées par type (voix, sms, MMS et site internet visités), par date ou par correspondant.

- **Par renvoi d'appel** : L'accès à la PNIJ ne peut se faire que sur le réseau interne du ministère et nécessite donc que l'enquêteur soit à son bureau. Pour permettre de suivre les écoutes tout en étant sur le terrain, l'enquêteur peut mettre en place un renvoi sur son téléphone portable. Une fois l'option activée, dès que la ligne interceptée reçoit une communication « voix », l'enquêteur reçoit un appel et écoute en direct la communication. Pour les SMS, l'enquêteur reçoit une notification de la PNIJ avec le contenu du SMS.

- **Sur ordinateur dédié** : L'ANTENJ (service gestionnaire de la PNIJ) met à disposition des enquêteurs des ordinateurs portables sécurisés par l'agence nationale de la sécurité des systèmes d'information (ANSSI). Ces ordinateurs disposent d'un protocole de sécurité de niveau « Secret Défense ».

  Ainsi l'enquêteur a accès à une interface simplifiée de la PNIJ depuis n'importe où du moment qu'il dispose d'un

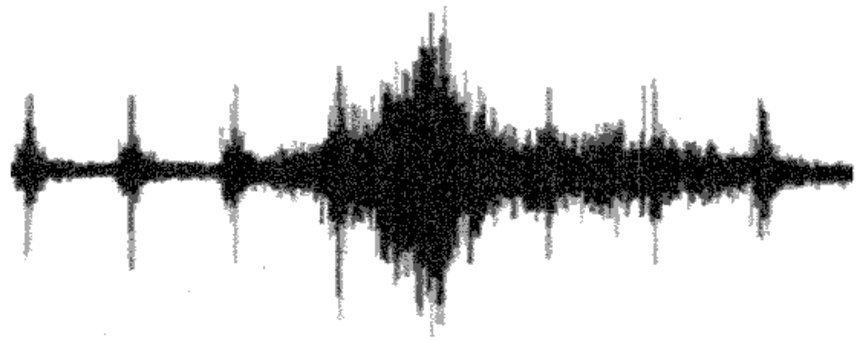
réseau WIFI. Il peut ainsi consulter les écoutes en cours. Néanmoins, il ne peut pas effectuer d'autres manipulations telles que des réquisitions.
Cet ordinateur portable est aussi utilisé par les interprètes pour leur permettre d'effectuer les traductions des écoutes à distance.

4. Quels sont les communications interceptées et le contenu visible par l'enquêteur ?

L'interception de communication sur une ligne mobile permet d'accéder à 5 types de contenus :

1. **Les appels « voix »** : Ce sont les appels téléphoniques par la voie classique effectués sur le réseau mobile (donc hors appels via messageries sécurisées). L'enquêteur visualise les appels entrants et sortants.

Chaque appel est numéroté, daté avec le numéro appelant et le numéro appelé, le numéro IMEI utilisé par la ligne interceptée, la cellule déclenchée et la durée de la communication.



L'enquêteur visualise la conversation sous forme de diagramme. À l'aide d'un curseur temporel, il peut se déplacer à son gré et ainsi cerner les passages où il n'y a pas de son et écouter les passages intéressants. Une option permet de ralentir le débit de la voix pour mieux

comprendre les paroles prononcées. Il est possible aussi d'accélérer quand la conversation est longue.

2. **Les SMS** : Les messages textes s'affichent en intégralité avec le numéro de l'expéditeur, la date et la cellule déclenchée. Un traducteur automatique intégré permet de traduire le contenu.

3. **Les MMS :** Même procédure que pour les SMS avec visualisation de la photo ou de la vidéo envoyée ou reçue.

4. **Le trafic Data (internet) :** La PNIJ affiche l'intégralité des sites internet consultés avec date et heure ainsi que l'adresse IP utilisée. Chaque application utilisée laisse une trace également sans permettre d'en voir le contenu.

L'appel est enregistré dès le début des tonalités ainsi même si l'appel n'a pas encore abouti, l'enquêteur entendra ce qui se dit ou se passe avant que l'interlocuteur ne décroche.

Le micro est actif dès le départ. Si vous êtes mis en attente ou que vous atterrissez sur un répondeur, tout est enregistré.

5. Quels types de contenus ne sont pas visualisables par les enquêteurs ?

Voici la liste des communications qui ne sont pas prises en charge par la PNIJ et auxquelles l'enquêteur n'a donc pas accès :

- Lorsque l'appel passe par une application dite « chiffrée » telle que ***WhatsApp, Telegram, Signal, Viber***, l'enquêteur peut voir qu'il y a eu un appel néanmoins il ne dispose d'aucune information et l'appel étant chiffré, la PNIJ affiche un message d'erreur l'informant que le contenu n'est pas lisible. Il ne peut rien entendre et il ne peut pas connaître l'interlocuteur.

- Les appels passés par ***Facebook Messenger, Skype et autres applications*** dites « non chiffrées » n'étaient pas non plus visibles dans la PNIJ. Néanmoins, l'évolution constante des capacités de la plateforme auront peut-être permis un accès à ce contenu ce dernier n'étant pas protégé.

- Tous les contenus « texte », images, liens internet, vidéos échangés via les applications chiffrées telles ***WhatsApp, Telegram, Signal ou Viber***, ne peuvent être lu sur la PNIJ et sont donc inaccessibles pour les enquêteurs.

- Le contenu des mails ne peut être lu.

- Si le contenu d'une application est sécurisé tels vos comptes bancaires, la PNIJ ne peut l'afficher. Globalement tout ce qui n'est pas accessible en cliquant sur le lien sans devoir s'authentifier, n'est pas visible pour l'enquêteur.

6. Comment sont retranscrites les communications ?

Dans une enquête judiciaire, plusieurs lignes mobiles peuvent être interceptées. « Ecouter » une ligne peut représenter un travail colossal en fonction du volume de communications. Ainsi si la cible interceptée utilise constamment son téléphone, il y aura de nombreuses heures d'écoutes en perspective et parfois cela sur plusieurs mois.

Les enquêteurs se répartissent le travail au sein du service et en fonction de la sensibilité du dossier, chaque ligne doit être vérifiée quotidiennement. Un retard trop conséquent dans la mise à jour ferait courir le risque de passer à côté d'informations essentielles ou tout simplement de pas s'apercevoir d'un changement de ligne mobile par l'utilisateur (aucune donnée interceptée par exemple).

La PNIJ offre de nombreuses fonctionnalités intuitives pour un travail partagé entre enquêteurs. Un système de codage couleur

permet de différencier les communications intéressantes et celles qui ne le sont pas. Il sera possible à chaque fois de marquer la communication et d'un coup d'œil savoir s'il s'agit d'un message répondeur, d'un appel qui n'a pas abouti, etc.

Un marquage par conversation permet d'indiquer aux autres enquêteurs si la conversation a été lue et si elle a été retranscrite (ou si cela est à faire).

Les enquêteurs n'ont pas l'obligation de retranscrire toutes les conversations interceptées. Par conséquent seules celles intéressant l'enquête feront l'objet d'un procès-verbal. **Les informations relatives à la manifestation de la vérité sont retranscrites, mais comme nous l'avons souligné dans le chapitre relatif à la PNIJ, les éléments relatifs à la vie privée de l'utilisateur et de ses contacts peuvent être également formalisés sur procès-verbaux. Tel que ses opinions politiques, religieuses, etc.**

En fonction du langage utilisé ou de la qualité de l'appel, retranscrire un appel de 10 minutes peut parfois prendre plus d'une heure. Un appel d'une heure peut nécessiter une après-midi de travail et devant la masse de travail à accomplir, les enquêteurs privilégieront les communications les plus pertinentes.

Cependant, un appel « long » n'est jamais retranscrit dans sa totalité, seul le passage intéressant est retranscrit sur papier. L'enquêteur indiquera dans son procès-verbal à partir de quel moment il retranscrit l'appel. Charge à lui de ne pas dénaturer le sens de la communication et brouiller le message initial en lui donnant une orientation particulière.

Exemple :

Appel d'une durée de 15min et 35 secondes débuté à 14h05min10sec.
Retranscription à 8min23sec :

[Daniel] *Comme je te disais, je ne sais pas si je serai là au rendez-vous (silence) Je ne me sens pas prêt, c'est du lourd là, c'est risqué hein ! (Rire).*
[Xh] *Arrête ! Dany ! Tu vois le fric qu'on va se faire ! Il faut que tu sois là ! Je compte sur toi pour assurer. On n'aura pas d'autres occasions. Imagine 10 kilos de chocolat, c'est notre plus gros coup !*
[Daniel M] *Ouai, je sais, je sais. Mais si les bleus sont là hein ! Non, mais.. (Inaudible bruits extérieurs).*
[Xh] *T'inquiète on gère, on gère. On a fait ça bien.*
[Daniel M] *Et sinon les enfants, ça va ?*
Arrêtons la retranscription à 10min41sec.
Le reste de la conversation n'intéressant pas l'enquête en cours.

Dans l'exemple de retranscription donné, l'enquêteur n'a pas identifié l'interlocuteur de la cible. [Xh] signifie homme inconnu. L'enquêteur choisit de ne retranscrire sur procès-verbal que les informations intéressantes en occultant le début et la fin de la conversation.

La retranscription peut se faire de deux manières différentes :

- Soit sur procès-verbal libre ou sur le logiciel (LRPN – Logiciel de rédaction des procédures de la Police Nationale).
- Soit sur l'outil de retranscription de la PNIJ qui générera un procès-verbal de retranscription.

Les SMS, MMS et consultations internet sont retranscrits complètement (elles sont effectuées par copier-coller, ce qui est moins fastidieux).

Les conversations en langues étrangères sont quant à elles soumises à un traducteur assermenté. L'interprète qui se trouve requis par les enquêteurs accède aux écoutes soit directement au sein du service soit par un accès personnel à la PNIJ. Il traduit l'intégralité des conversations et messages sur la PNIJ et indique à l'enquêteur celles qui sont les plus pertinentes.

L'enquêteur réalise une transcription sur procès-verbal qu'il fera obligatoirement signer à l'interprète accompagné de son assermentation.

******

Le cadre légal des interceptions judiciaires est en proie à de futures évolutions élargissant considérablement la possibilité d'y recourir.

La loi de programmation 2018-2022 et de réforme pour la justice avait pour objectif d'élargir l'usage des interceptions de communications en enquête préliminaire ou de flagrance aux infractions de droits communs (punies de 30 ans d'emprisonnement) sur autorisation du JLD. Les écoutes n'auraient plus été limitées au champ de la délinquance et criminalité organisée.

Dans le même esprit, la loi prévoyait la possibilité pour le procureur de la République, dans une notion « *en cas d'urgence résultant d'un risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens* », d'autoriser la mise en place d'une interception de communication pour un délai de 24 heures. Cette autorisation devant être confirmée dans un délai de 24 heures, à peine de voir les informations recueillies inexploitables.

Un rapport du Sénat relatif à cette loi, à l'époque où elle se trouvait à l'état de projet, dénonçait le caractère excessif de l'extension du cadre législatif entourant les interceptions de communications.[1]

[1] Rapport n° 11 (2018-2019) de MM. François-Noël BUFFET et Yves DÉTRAIGNE, fait au nom de la commission des lois, déposé le 3 octobre 2018.

	Cadres	Enquête de flagrance	Enquête préliminaire	Information judiciaire
Délinquance et criminalité organisée	Infractions concernées	Crimes ou délits mentionnés aux articles 706-73 et 706-73-1 du code de procédure pénale		Crimes ou délits punis d'une peine d'emprisonnement supérieure ou égale à deux ans
	Compétence	Autorisation du juge des libertés et de la détention, à la requête du procureur de la République		Juge d'instruction
	Durée de l'autorisation	1 mois, renouvelable une fois		4 mois renouvelable, deux ans au maximum
	Base légale	Article 706-95 du code de procédure pénale		Articles 100 à 100-8 du code de procédure pénale
Droit commun	Infractions concernées	ø		Crimes ou délits punis d'une peine d'emprisonnement supérieure ou égale à deux ans
	Compétence	ø		Juge d'instruction
	Durée de l'autorisation	ø		4 mois renouvelable, un an au maximum
	Base légale	ø		Articles 100 à 100-8 du code de procédure pénale

11. LES INTERCEPTIONS DE COMMUNICATIONS ADMINISTRATIVES

Dans le précédent chapitre, nous avons évoqué les interceptions de communications effectuées dans le cadre d'une procédure judiciaire mais il existe une autre possibilité offerte à l'État pour procéder à des investigations téléphoniques et des écoutes sur une ligne mobile ou fixe : **les interceptions de sécurité**.

Nous parlons ici d'écoutes dites « administratives » réalisées par les services de renseignements français (DGSI, Service central du renseignement territorial (SCRT), Direction du renseignement de la Préfecture de Police de Paris), par les services du ministère de la Défense (DGSE et Direction du renseignement militaire) et par la Direction nationale du renseignement et des enquêtes douanières.

Ces interceptions réalisées dans le cadre du renseignement concernent essentiellement de nos jours les atteintes à la sûreté de l'État, la prévention du terrorisme et la protection des intérêts économiques.

Les premières écoutes pour le compte du renseignement français furent réalisées en 1889 et jusqu'en 1960, elles échappaient à tout cadre légal. Elles étaient réalisées de manière discrétionnaire. Ainsi, en 1960, Michel Debré alors Premier

ministre, créa le Groupement interministériel de contrôle (GIC) en charge encore à l'heure actuelle, de réaliser ces interceptions.

En 1991, Michel Rocard fait voter la loi relative au secret des correspondances émises par la voie des communications électroniques. En 2006, la loi relative à la lutte contre le terrorisme vient modifier celle de 1991. En 2012, la notion d'interception de sécurité est totalement intégrée au Code de la sécurité intérieure.

1. Pour quel motif une interception de sécurité peut-elle être mise en place ?

Il existe un panel de neuf motifs invocables par les services de renseignement pour solliciter la mise en place d'une écoute administrative[1] :

- Défense de l'indépendance nationale, de l'intégrité du territoire et défense nationale.
- Défense des intérêts majeurs de la politique étrangère, de l'exécution des engagements européens et internationaux de la France, prévention de toute ingérence étrangère.
- Défense des intérêts économiques, industriels et scientifiques majeurs de la France.
- Prévention du terrorisme.
- Prévention des atteintes à la forme républicaine des institutions.
- Prévention de la reconstitution ou du maintien des groupes de combat et milices privées dissous

[1] Article L811-3 du Code de la sécurité intérieure.

- Prévention des violences collectives portant gravement atteinte à la paix publique.
- Prévention de la criminalité et de la délinquance organisée.
- Prévention de la prolifération des armes de destruction massive.

2. Qui contrôle les interceptions de sécurité et pour quelles durées sont-elles mises en place ?

Les autorisations d'écoutes administratives sont accordées par le Premier ministre, ou par une des personnes autorisées par ce dernier (habilitées secret défense). Un rapport motivé doit être transmis par le service sollicitant la demande.

La Commission nationale de contrôle des techniques de renseignement (CNCTR) a la charge d'examiner les demandes et les autorisations délivrées. Elle est composée de neuf membres, dont deux députés et deux sénateurs, deux membres du Conseil d'État, deux magistrats hors hiérarchie de la Cour de cassation et une personne qualifiée désignée par l'ARCEP.

La CNCTR contrôle l'ensemble de l'activité liée aux interceptions de communications, elle rend son avis quant aux demandes formulées et dispose d'un accès aux données interceptées.

La commission est sollicitée par les services du Premier ministre et rend son avis dans un délai de 24 heures. Lorsqu'une autorisation est délivrée malgré un avis défavorable de la commission, un rapport motivant cet avis défavorable est transmis.

L'autorisation est délivrée par le Premier ministre pour une durée de 4 mois. Renouvelable.

En cas d'urgence absolue, le Premier ministre peut délivrer une autorisation, mais doit informer la CNCTR dans un délai de 24 heures.

Un parlementaire, un magistrat, un avocat ou un journaliste ne peut être l'objet d'une demande de mise sur écoute administrative en raison de sa profession.

Seuls les éléments utiles à l'enquête administrative sont transcrits dans un rapport.

À l'issue d'un délai de 30 jours à partir du recueil des renseignements, les enregistrements sont détruits.

****

Les interceptions de sécurité sont essentiellement autorisées dans le cadre de la prévention du terrorisme et la criminalité organisée. Elle concerne uniquement la personne ciblée et l'entourage proche appelé « N+1 » par les services de renseignements. Ces services tentent depuis quelques années d'obtenir l'autorisation d'écouter les « N+2 » qui sont les personnes présentes dans les carnets d'adresses des cibles et de l'entourage. En vain.

Le cadre légal évoqué concerne également les techniques d'investigation telles que les Fadettes, la géolocalisation, la sonorisation de pièce ou de véhicule et les interceptions de données informatiques.

Les écoutes ainsi réalisées ont pour vocation d'alimenter les bases de données du renseignement et permettre d'enclencher des actions préventives telles que des perquisitions administratives ou des assignations à résidence.

Quand les écoutes administratives révèlent des infractions susceptibles de faire l'objet d'une qualification pénale, elles sont transmises au Parquet, de manière « épurée » et permettront l'ouverture d'une enquête judiciaire. Il s'agit là du processus de judiciarisation.

12. LES IMSI CATCHER & KEYLOGGER

Quand les outils traditionnels pour faire progresser une enquête à l'aide de la téléphonie mobile ne suffisent plus, les techniques spéciales d'enquêtes entrent en scène. Ce nouvel arsenal a récemment fait son apparition dans le panel à disposition des enquêteurs et a permis de repousser les limites dans le domaine de la captation de données.

Ces outils à la pointe de la technologie, en constante évolution restent néanmoins l'apanage des enquêtes judiciaires liées à la délinquance et la criminalité organisées et même s'ils se démocratisent, leur usage demeure exceptionnel. Ils sont prévus par le Code de procédure pénale au chapitre relatif aux « autres techniques spéciales d'enquête ».

1. L'IMSI Catcher

Il s'agit d'un équipement informatique permettant d'intercepter à distance les informations d'un téléphone, le trafic des communications mobiles ou de tracer les mouvements de l'appareil.

Cet outil de surveillance agit comme une fausse antenne-relai. Il force les téléphones mobiles dans son champ d'action, à s'y connecter.

Un téléphone mobile cherche en permanence la cellule la plus proche, pour se connecter à celle proposant le meilleur signal. Le téléphone capte le signal de l'IMSI Catcher et le considère comme une antenne-relai et ainsi il va lui transmettre les informations de connexion de la ligne dont le fameux numéro IMSI qui permet à une carte SIM de s'identifier sur un réseau téléphonique. L'IMSI Catcher renvoi sur le réseau téléphonique les communications qu'il a reçues. **L'opération est invisible.**

Nous l'avons vu plus haut, le numéro IMSI permet d'identifier l'abonné de la ligne mobile par le biais d'une réquisition judiciaire, mais l'IMSI Catcher enregistre également le numéro IMEI.

L'IMSI Catcher se substituant à une antenne-relai, il enregistre également l'ensemble des communications émises par le téléphone portable. Le détail est consultable, mais pas nécessairement le contenu.

L'IMSI Catcher exploite une faille du réseau 2G (EDGE). En effet, le réseau demande au téléphone de s'identifier, mais pas l'inverse. Les réseaux 3G et 4G ont comblé cette faille, néanmoins l'IMSI Catcher peut forcer un téléphone à basculer sur le réseau 2G en brouillant le signal 3G/4G.

Les applications sont multiples, mais concrètement, **l'IMSI Catcher va par exemple permettre d'identifier l'ensemble des lignes mobiles d'une maison, d'un bâtiment, d'un quartier, le tout en fonction de sa puissance.**

Si les enquêteurs le placent derrière une porte d'appartement, il sera possible de connaître les informations des téléphones en fonctionnement à l'intérieur. C'est l'idéal s'ils ne connaissent pas quelles sont les lignes de leurs cibles utilisant des cartes SIM prépayées.

L'IMSI Catcher est clairement utilisé quand les enquêteurs ignorent tout des lignes mobiles utilisées par les personnes visées.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

La puissance de l'IMSI Catcher dépend de sa taille et de l'utilisation voulue. Ainsi, un IMSI Catcher tenant discrètement dans un sac à dos sera utile pour intercepter un mobile dans un rayon de quelques mètres. Le modèle tenant à l'arrière d'un fourgon sera capable d'être déployé sur un rayon de plusieurs centaines de mètres.

La problématique réside une fois de plus dans le respect de la vie privée des citoyens. En effet, l'IMSI Catcher capte l'ensemble des téléphones mobiles à sa portée sans possibilité de ne cibler qu'une ligne en particulier, **ainsi il enregistre toutes les données, même celles d'individus non concernés par l'enquête.** Lorsque l'enquêteur souhaite écouter une ligne captée par l'IMSI Catcher, il peut le faire en se focalisant sur l'IMSI choisi. Il est possible d'écouter jusqu'à 4 lignes simultanément.

L'IMSI Catcher permet également de pister un téléphone. En fonction de la puissance reçue du téléphone suivi, il est en mesure de donner une indication sur sa position.

L'utilisation de l'IMSI Catcher dans le cadre judiciaire est légalisée par le Code de procédure pénale et a fait l'objet d'une réforme en 2019.

Il ne peut être utilisé que pour les infractions liées à la délinquance et la criminalité organisées. *(Articles 706-95-11 à 706-95-20 du Code de procédure pénale)*.

Plusieurs cas de figure pour son utilisation sont à prendre en compte en fonction de l'objectif poursuivi :

- Si l'IMSI Catcher est utilisé pour identifier le numéro IMEI ou le numéro de ligne d'un téléphone mobile, ou localiser le téléphone mobile :

- **Durée 1 mois** (renouvelable une fois) pour une **enquête préliminaire ou de flagrance**. Autorisation délivrée par le JLD sur requête du procureur de la République.

- **Durée 4 mois** (renouvelable jusqu'à 2 ans) pour **une instruction judiciaire**. Autorisation du juge d'instruction après avis du procureur de la République.

- En cas d'urgence, le juge d'instruction peut délivrer une autorisation sans recueillir l'avis préalable du procureur de la République.

↳ Si l'IMSI Catcher est utilisé pour intercepter les communications d'une personne ou de sa ligne mobile, les articles de lois relatifs aux écoutes téléphoniques s'appliquent.

L'utilisation de l'IMSI Catcher pour pratiquer les écoutes est limitée à 48 heures dans ce cas précis. Il est néanmoins plus aisé pour les enquêteurs de demander l'interception des communications du boitier IMEI identifié par le biais des articles relatifs aux écoutes téléphoniques pour obtenir un résultat moins fastidieux à mettre en place et sur une plus longue durée.

Certaines dispositions des articles relatifs à l'IMSI Catcher sont amenées à être revues prochainement, car déclarées non conformes par le Conseil constitutionnel.

L'utilisation, la détention, la fabrication, la vente d'un IMSI Catcher par un particulier est punie par le Code pénal de 5 ans d'emprisonnement et de 300 000 euros d'amende.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

Seuls les opérateurs habilités ont la possibilité de vendre ce dispositif aux services autorisés et le prix moyen d'un IMSI Catcher est de 100 000 euros.

Certaines entreprises proposent à la vente des téléphones « cryptés » dits « PGP » dont le protocole de sécurité empêche l'IMSI Catcher d'exploiter la faille du réseau 2G et alerte l'utilisateur d'une tentative d'intrusion.

Le 3 octobre 2018, le rapport n°11 émanant du Sénat au sujet de la loi de programmation 2018-2022 et de réforme pour la justice, **relevait que le ministère de l'Intérieur ne disposait que de 11 IMSI Catcher.**

2. Le Keylogger

En anglais, « keylogger » signifie enregistreur de frappe. Il entre dans le panel d'outil offert pour l'interception de données émises depuis un terminal mobile. **Et c'est très certainement, l'arme ultime pour espionner les communications d'un individu, car il offre un accès direct à tout ce qui se passe sur l'écran utilisé.**

Le keylogger est un logiciel espion capable de transmettre aux enquêteurs tout ce qu'il se passe sur un équipement informatique et en temps réel. Ainsi, il peut sous format vidéo enregistrer l'utilisation de votre écran, il enregistre les frappes du clavier, le son, l'objectif photo frontal ou arrière, les applications ouvertes (sécurisées ou non) avec leurs contenus, les positions GPS. Absolument tout.

Le keylogger s'utilise sur un ordinateur, sur une tablette, mais nous évoquerons ici son utilisation sur un smartphone.

Le keylogger est à proprement parler, un logiciel espion dont l'utilisation est invisible par le détenteur du smartphone. Il est installé de plusieurs manières :

- Par l'envoi d'un mail ou d'un message contenant un lien ou une pièce jointe piégés.

- Par l'installation d'une application ou d'une mise à jour piégée.

- Par installation directe par un tiers ayant accès au téléphone quelques instants.

Chaque keylogger est programmé de manière unique pour pouvoir être installé sur la version du système d'exploitation du smartphone. Le logiciel est majoritairement introduit en exploitant une faille du système d'exploitation « Androïd » de Google. Plus la version du système d'exploitation est ancienne, plus l'opération se révèle être simple. Toutefois chaque mise à jour majeure du système d'exploitation du téléphone oblige les techniciens à la mise à jour du keylogger utilisé.

Dans le cas des téléphones d'Apple, la démarche est beaucoup plus compliquée, car le système IOS est très sécurisé et ne laisse que peu d'opportunités. S'il s'agit d'un iPhone datant de quelques années, c'est possible, mais pour les toutes dernières générations, sans possibilités de « craquer » le code du système d'exploitation, il est impossible d'utiliser un keylogger.

Le keylogger transmet les données obtenues lorsque le smartphone se connecte à un réseau Wifi. Le technicien peut aussi récupérer les données en temps réel en passant par le réseau mobile, mais c'est prendre ici le risque de vider rapidement la batterie et de dépasser le forfait DATA de la cible (deux éléments qui ne manqueront pas de lui mettre un doute sur la fiabilité de son smartphone).

Il vaut mieux dans ce cas que les enquêteurs se contentent d'obtenir le son et les frappes du clavier et réserver les enregistrements de l'écran pour lorsque le téléphone sera connecté à un réseau Wifi.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

La technique du keylogger était jusque-là réservée aux services de renseignement, mais depuis peu la possibilité d'un usage judiciaire a fait son apparition. Le Code de procédure pénale prévoit son usage.

Extrait de l'article 706-102-1 du Code de procédure pénale : *« Il peut être recouru à 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, tel qu'elles sont stockées dans un système informatique, telle 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. »*

L'utilisation du keylogger se fait dans les mêmes conditions d'autorisations et de durées que pour l'IMSI Catcher et il vise uniquement les infractions liées à la criminalité organisée et les infractions à caractère terroriste.

Le cas du keylogger est assez particulier, car il nécessite beaucoup de conditions spécifiques pour être mis en place et seuls quelques services spécialisés de la police nationale ou de la gendarmerie sont en mesure de le faire. L'évolution des sécurités de nos smartphones sont le frein majeur à un outil très clairement en mesure de contrecarrer l'utilisation de messagerie chiffrée.

La conception et la mise en œuvre de la technique du keylogger sont prises en charge par le Service Techniques National des Captations Judiciaires (STNCJ) placé sous l'autorité du Directeur de la DGSI.

Chaque logiciel espion doit être certifié par l'Agence Nationale de la Sécurité des Systèmes d'Informations. L'intérêt étant alors d'assurer l'intégrité du keylogger et ne de pas laisser supposer qu'il puisse modifier, altérer ou ajouter les éléments de preuves contenus dans le smartphone visé.

Chaque logiciel espion ainsi mis à disposition des enquêteurs dispose d'une durée de vie très courte. Les services de renseignements sont également peu enclins à partager leurs techniques avec les enquêteurs judiciaires au risque de voir exposer au grand jour dans les procédures ad hoc, les spécificités techniques de leur keylogger.

Depuis 2011, la loi offre la possibilité de faire usage du keylogger. En 2015, ce dispositif n'a été utilisé qu'à cinq reprises.

13. LES MESSAGERIES SÉCURISÉES

Les messageries sécurisées dites « chifrées » telles que Whatsapp, Telegram ou Signal offre depuis longtemps une alternative aux moyens de communication traditionnels que sont les appels vocaux et les SMS. Elles sont aujourd'hui très présentes dans l'usage des smartphones. Au-delà de l'aspect pratique par leurs fonctionnalités beaucoup plus en adéquation avec notre temps, elles représentent un atout majeur pour la sécurité et la protection de vos communications. En tant qu'avocat, de nombreuses informations sensibles et confidentielles transitent sur votre mobile. Les messageries chiffrées apportent une garantie non négligeable à la protection de vos données.

Les messageries chiffrées ont également bouleversé les capacités d'investigations en termes de téléphonie mobile et se sont avérées être des freins importants à la récupération de données et d'échanges entre individus. Néanmoins, comme nous l'avons vu précédemment, là où la technique protège, l'erreur humaine se révèle être une faille exploitable.

Depuis toujours, utiliser un téléphone mobile, un smartphone, c'est obligatoirement laisser des traces indélébiles. Tant que l'objet est connecté au réseau mobile, nul ne peut s'y soustraire.

L'alternative se trouve dans les applications chiffrées dites « messageries instantanées sécurisées » dont l'usage s'est démocratisé ces dernières années. Elles offrent toutes la possibilité de protéger vos communications par le biais du chiffrement, mais le niveau de protection n'est pas égal d'une application à une autre. Ainsi nous nous attarderons sur trois des messageries les plus connues à ce jour que sont WhatsApp, Telegram et Signal. *(Applications disponibles sur Apple Store et Google Play).*

Avant d'évoquer ces applications, revenons sur les chapitres précédents et faisons un constat simple. Il est possible d'intercepter à distance toutes les communications **sauf les échanges (Appels, texte, vidéos et images) qui passent par les messageries sécurisées.**

Hormis l'usage d'un keylogger, rien ne permet à ce jour de briser à distance la protection offerte par ces applications.

Utiliser un smartphone avec les appels et SMS « classiques » c'est laisser l'accès à l'intégralité des contacts. S'il y a une écoute mise en place, c'est permettre l'accès au contenu des échanges et également des déplacements.

L'utilisateur d'un téléphone mobile qui n'utilise jamais les SMS, les appels vocaux ou la navigation internet ne laisse qu'une seule donnée : La localisation des cellules déclenchées.

À chaque première utilisation, Whatsapp, Telegram et Signal solliciteront la présence d'une carte SIM et donc d'un numéro de mobile. Néanmoins par la suite, si la carte SIM est enlevée, elles fonctionneront toujours si ces applications ont accès à internet. Cela peut passer par l'usage exclusif du Wifi sur le téléphone ou d'un partage de connexion avec un autre smartphone. Les réseaux wifi publics sont nombreux de nos jours et facilement accessibles. C'est un niveau de précaution qui limite l'usage et les déplacements, néanmoins cela limite le risque d'émettre des

communications non sécurisées avec la carte SIM.

Car n'utiliser que les applications sécurisées et ne jamais utiliser le réseau de votre carte SIM, c'est une gymnastique, mais cela n'empêchera jamais un interlocuteur qui a connaissance du numéro de la ligne de commettre innocemment une erreur et d'appeler ou d'envoyer un SMS hors applications chiffrées.

Le keylogger représente aussi une menace redoutable mais amoindrie par le fait de disposer d'un iPhone récent, mis à jour et utilisant un mot de passe fort (avec majuscules, minuscules, chiffres et caractères spéciaux).

1. Comment fonctionne une messagerie instantanée sécurisée ?

Les messageries dites « cryptées » utilisent la méthode du chiffrement de bout en bout des communications. **Ce qui n'est pas le cas de Facebook Messenger, Snapchat, Instagram, Twitter, etc.**

Concrètement, les messageries sécurisées utilisent un algorithme de chiffrement qui rend **illisible** le message. Le message est chiffré directement dans l'application sur votre téléphone avant d'être envoyé. Le message part, totalement illisible pour quelqu'un qui l'intercepterait. Ainsi seul le destinataire dispose de la clé pour le déchiffrer.

Le chiffrement repose sur plusieurs technologies souvent issues du domaine militaire. Nul ne peut lire le message sans disposer du Code pour l'ouvrir.

La clé de chiffrement s'applique dès la création de la conversation avec le correspondant et la clé change à chaque nouvelle conversation. En théorie, les applications sécurisées affirment ne pas connaître la clé pour déchiffrer les communications bien qu'elles soient les créatrices du protocole de leurs propres messageries.

Vous pourriez nous dire pourquoi, chiffrer, rendre illisibles ses communications quand nous n'avons rien à cacher. Et bien pour la même raison que vous mettez votre courrier dans une enveloppe ou que vous ne vous promenez pas avec votre numéro de carte bancaire écrit sur un t-shirt.

Le chiffrement sous-entend que la conversation soit envoyée directement à un correspondant pour être lue. Mais pour le confort d'utilisation et un usage fluide de l'application, les messageries sécurisées utilisent des serveurs, des espaces de stockage de données informatiques. Le message se trouve ainsi stocké dessus. Cela permet par exemple de mettre en « attente » un message qui n'est pas remis, car le destinataire ne s'est pas connecté ou bien de retrouver ses conversations ainsi sauvegardées si le téléphone est perdu. C'est à ce niveau que pourrait se situer la faille si les serveurs étaient mal protégés et que le contenu était accessible.

Une autre différence existe entre ces applications, à savoir la conservation des métadonnées. Les métadonnées sont les informations relatives à la discussion sécurisée (Date, heure, numéros des correspondants). **WhatsApp conserve ces données durant un laps de temps, là où Telegram et Signal ne conservent rien.**

2. <u>Comment les enquêteurs peuvent-ils accéder au contenu des messageries sécurisées</u> ?

Le chiffrement rendant illisibles **à distance** les conversations et leurs contenus, impossible pour les enquêteurs d'en savoir plus. Il faudrait pour cela connaître ou briser la clé de chiffrement de chaque conversation. Sachant qu'elle change à chaque nouvel échange, vu l'énorme force de calcul qu'il faudrait déployer pour déchiffrer chaque clé, ce n'est clairement pas la bonne solution. Alors, comment procèdent-ils ?

La 1re solution est la plus simple. Obtenir en main propre le téléphone pour en lire le contenu. Si les messages ne sont pas supprimés et que certaines fonctions de protection d'accès ne sont pas activées, alors les échanges sont facilement accessibles. Dans l'hypothèse où le téléphone serait entre de mauvaises mains, voici plusieurs choses à savoir :

- Nous pouvons ne pas donner le code de déverrouillage de notre smartphone. Ainsi il n'y a pas d'accès aux applications et il n'y a pas de lecture directe des échanges. **Néanmoins, la technologie permet de contourner le code d'accès d'un téléphone.** L'accès sera beaucoup plus difficile si le mot de passe est complexe (codes composés de chiffres, majuscules, minuscules et caractères spéciaux).

- Si nous ne donnons pas notre code de déverrouillage, les enquêteurs disposent d'outils pour « aspirer » le contenu de notre smartphone et obtenir une bonne partie des données. La protection réside dans le chiffrement des données du téléphone. Concrètement, **il est possible de rendre illisibles les données du téléphone pour celui qui ne disposerait pas du code. Cela dépend directement du système d'exploitation utilisé :**

  - <u>**Sur Android (Google)**</u> : Le contenu n'est pas chiffré de base. Pour cela il faut se rendre dans *Paramètres > Paramètres supplémentaires > Confidentialité > Chiffrement et identifiants > Chiffrer un appareil en utilisant le mot de passe de l'écran de verrouillage > Activer*.
    Quand le téléphone sera éteint, les données seront chiffrées et le téléphone vous demandera votre code pour déchiffrer le contenu à l'allumage. Sans le code, le contenu est illisible. En revanche, si le téléphone est allumé, même s'il y a un code de verrouillage, le contenu n'est pas nécessairement

automatiquement chiffré.

- **Sur IOS (Apple – iPhone)** : L'iPhone propose un niveau de protection plus élevé. Le contenu de l'iPhone est chiffré en permanence. **Sans le code de déverrouillage, impossible de lire le contenu d'aucune manière que ce soit. Cela s'applique à tous les équipements d'informatique d'Apple qui ne présentent aucune faiblesse aux tentatives d'extraction de données sans détenir le code.**

La faille d'iCloud. iCloud est un service de sauvegarde de données pour les mobiles d'Apple. Il permet de copier le contenu du téléphone sur le serveur d'Apple pour y accéder à distance ou restaurer les données sur un nouveau smartphone en cas de perte. **Cette « copie » n'est pas sécurisée.** La sauvegarde copiée sur un ordinateur est complète et totalement accessible. Le contenu n'est pas protégé et en cas d'accès à l'ordinateur, il sera possible de lire cette copie intégralement.

- Il est possible d'appliquer un code de verrouillage pour chaque application et plus particulièrement sur les applications de messageries chiffrées. Néanmoins comme nous allons le voir, refuser de fournir ce code est susceptible de constituer un délit.

Le refus de fournir les codes de déverrouillage est un délit réprimé par le Code pénal[1] :

« 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

[1] Article 434-15-2 du Code pénal.

autorités délivrées en application des titres II et III du livre Ier du Code de procédure pénale. La peine est de trois d'emprisonnement et de 270 000 € d'amende.

La peine est portée à cinq ans d'emprisonnement et à 450.000 € d'amende si 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 est portée à cinq ans d'emprisonnement et à 450.000 € d'amende. »

La Cour de cassation dans un arrêt n°1804 du 13 octobre 2020 vient confirmer que le code de déverrouillage d'un téléphone constitue un moyen de cryptologie.

La 2e solution, plus difficile à mettre en oeuvre consiste pour les enquêteurs à tenter d'accéder au compte de messagerie sécurisée à distance.

Si les conversations sur WhatsApp, Telegram ou Signal sont sauvegardées, il est alors possible de les retrouver en réinstallant l'application sur un autre téléphone. Il suffira alors d'entrer les identifiants. Pour nous authentifier, l'application nous enverra un SMS sur le numéro de mobile déclaré avec un code d'identification à entrer pour restaurer notre compte et nos conversations.

Si notre ligne est sur écoute, un enquêteur pourrait tenter d'accéder à l'application en se faisant envoyer un code d'identification et le récupérer via la PNIJ. Mais clairement, nous serions tout de même surpris de voir sur notre smartphone un SMS contenant un code de validation de notre messagerie, alors que ne l'avons pas sollicité**. L'enquêteur prendrait le risque d'alerter la personne visée par la mesure.**

Dans le cadre d'une garde à vue où le mis en cause refuse de divulguer ses codes de déverrouillage, l'enquêteur souhaitera accéder aux contenus des messageries sécurisées. Pour cela, il peut insérer la carte SIM dans un autre smartphone (ou utiliser sur

ordinateur un logiciel spécialisé) et se faire envoyer le code de vérification pour récupérer tout le contenu des conversations sauvegardées. Plusieurs logiciels sont à disposition pour copier l'intégralité des données du compte de la messagerie visée. **Si l'enquêteur dispose du téléphone, mais pas de la carte SIM, il pourra réquisitionner l'opérateur pour obtenir une copie de la carte SIM.**

Plusieurs actions sont en mesure de bloquer toutes récupérations de conversation.

- **Désactiver la sauvegarde de donnée ou utiliser les conversations éphémères.**
- **Instaurer la double authentification**

Dans les trois prochains chapitres, nous allons aborder les spécificités propres à WhatsApp, Telegram et Signal, car il faut garder à l'esprit que malgré le chiffrement de bout en bout, elles ne sont pas infaillibles et que les niveaux de protection sont différents.

Imaginez simplement que nos communications circulent dans une voiture. Avec Facebook Messenger, Snapchat ou Instagram, elles roulent dans une décapotable sur l'autoroute. Avec Whatsapp, c'est une voiture fermée à clé. Avec Telegram et Signal, elles roulent dans un véhicule blindé dans un tunnel.

14. WHATSAPP

WhatsApp est une application mobile de messagerie instantanée sécurisée.

Cette application disponible gratuitement sur Apple Store et Google Play a été créée en 2009. En 2014, l'application devient la propriété de Facebook. En avril 2016, WhatsApp applique le chiffrement de bout en bout à l'ensemble des communications échangées par sa plateforme. L'application compte aujourd'hui 1,5 milliard d'utilisateurs actifs par mois à travers le monde.

C'est la messagerie instantanée qui rencontre le plus gros succès et qui est la plus connue du grand public.

WhatsApp permet de discuter avec un correspondant ou d'avoir des conversations de groupe. Vous pouvez passer des appels VoIP,

envoyer des messages écrits ou vocaux, envoyer des images, des vidéos, passer des appels vidéo, envoyer des fichiers. Tout est chiffré.

Dans le cadre de vos échanges professionnels et afin de prévenir le risque d'atteinte à leur confidentialité, nous allons aborder les différents types de sécurité et particularités de l'application :

1. Le profil et les contacts

Votre profil accessible depuis les paramètres, permet de changer votre photo de profil et votre « humeur » sur l'onglet « actu ».

Il est préférable de ne pas mettre de photo de profil et de laisser le champ « actu » vide.

WhatsApp accède au répertoire de votre téléphone et ainsi vous propose la liste de vos contacts qui utilisent l'application et à qui vous pourrez envoyer un message. Si vous êtes dans le répertoire d'une autre personne, cette dernière verra que vous utilisez WhatsApp si elle l'utilise aussi.

En cliquant sur un contact, vous pourrez consulter son numéro de téléphone et également le bloquer. Ainsi il ne pourra pas vous envoyer de message ni voir votre présence.

2. Paramètres conseillés pour une sécurité optimale

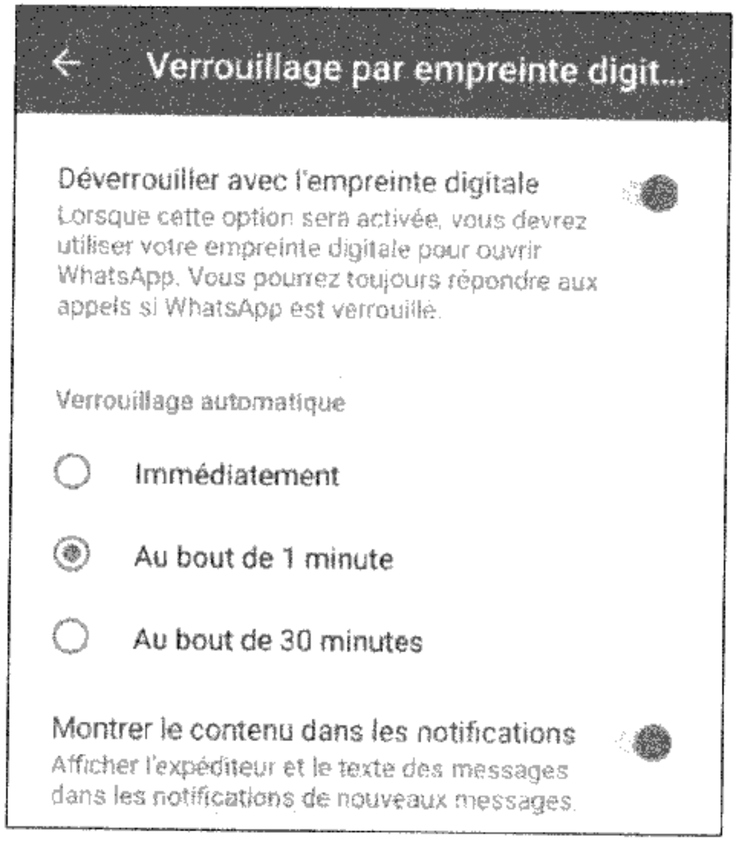
➢ Le déverrouillage par empreinte digitale ou Face ID :

WhatsApp ne propose pas la possibilité de sécuriser l'accès à l'application avec un mot de passe. Mais il est possible de sécuriser vos messages en appliquant le **déverrouillage par empreinte digitale** (ou Face ID sur iPhone) pour les smartphones équipés.

Ainsi il sera impossible d'accéder au contenu sans l'empreinte digitale et donc sans votre accord.

Pour l'activer : ***Paramètres > Compte > Confidentialité > Verrouillage par empreinte digitale***

Accédez à l'option, activez le déverrouillage par empreinte digitale et réglez sur 1 minute.



Sur cette même page, vous pouvez également désactiver « Montrer le contenu dans les notifications ». Ainsi sur la page d'accueil de votre smartphone, vous aurez une notification de message WhatsApp, mais le contenu du message ne s'affichera pas et ne sera donc pas lisible à votre insu.

Pour les utilisateurs de smartphone Android, si vous ne disposez pas de lecteur d'empreinte digitale, il existe dans l'onglet sécurité du téléphone la possibilité de verrouiller par code les applications de votre choix.

- **La vérification en deux étapes :**

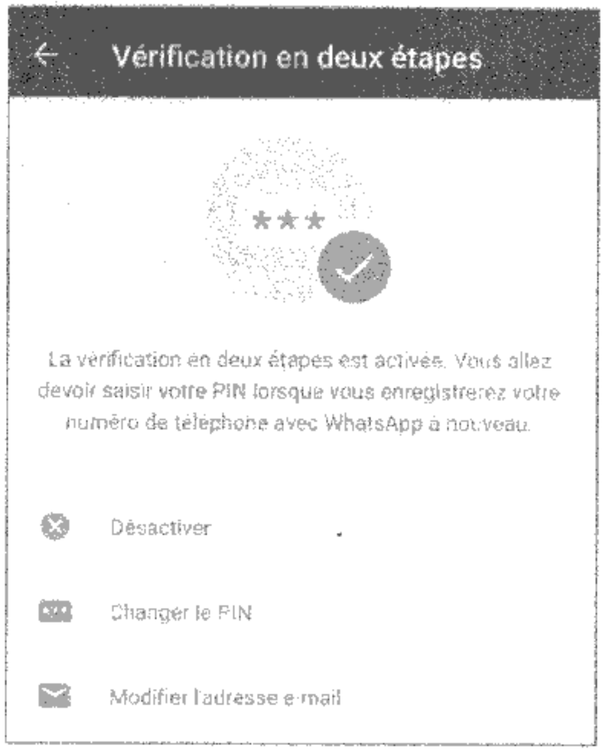
Cette option est celle que vous devez absolument mettre en place pour éviter un accès non désiré à votre compte par une tierce personne (en cas de vol par exemple).

WhatsApp va vous demander de définir un code à 6 chiffres. Si vous installez WhatsApp sur un autre téléphone, vous devrez entrer le code de vérification reçu par SMS, mais également ce code de double authentification connu seulement de vous.

Comme nous l'avons évoqué, le code de vérification reçu par SMS peut être intercepté à votre insu pour ensuite installer l'application et accéder à vos messages. **Mais sans le code de double authentification connu de vous seul, il sera totalement impossible d'usurper votre compte à distance.**

Par mesure de sécurité et pour mémoriser ce code, WhatsApp vous demandera régulièrement de le rentrer à l'ouverture de l'application.

Ne choisissez pas un code facile à deviner tel que votre date de naissance, celle d'un proche ou votre anniversaire de mariage.



Accès : ***Paramètres > Compte > Vérification en deux étapes.***

- **La sauvegarde des conversations**

Le réel point fort de Whatsapp, c'est la possibilité de sauvegarder vos discussions pour pouvoir les retrouver si vous perdez votre smartphone ou si vous installez l'application sur un autre support.

Mais ces sauvegardes ne sont pas chiffrées ! Elles sont donc accessibles et non sécurisées.

Elles sont sauvegardées à intervalle régulier sur votre compte Google Drive (pour Android) ou sur iCloud (pour iPhone). Et une copie est également faite dans la mémoire de votre smartphone. Tout est copié, le journal d'appels, les messages, les images le texte, etc. **Cette sauvegarde est l'ennemie de votre confidentialité.** Même s'il y a un aspect pratique à pouvoir récupérer des conversations en cas de perte du compte WhatsApp, la sauvegarde sera facilement accessible.

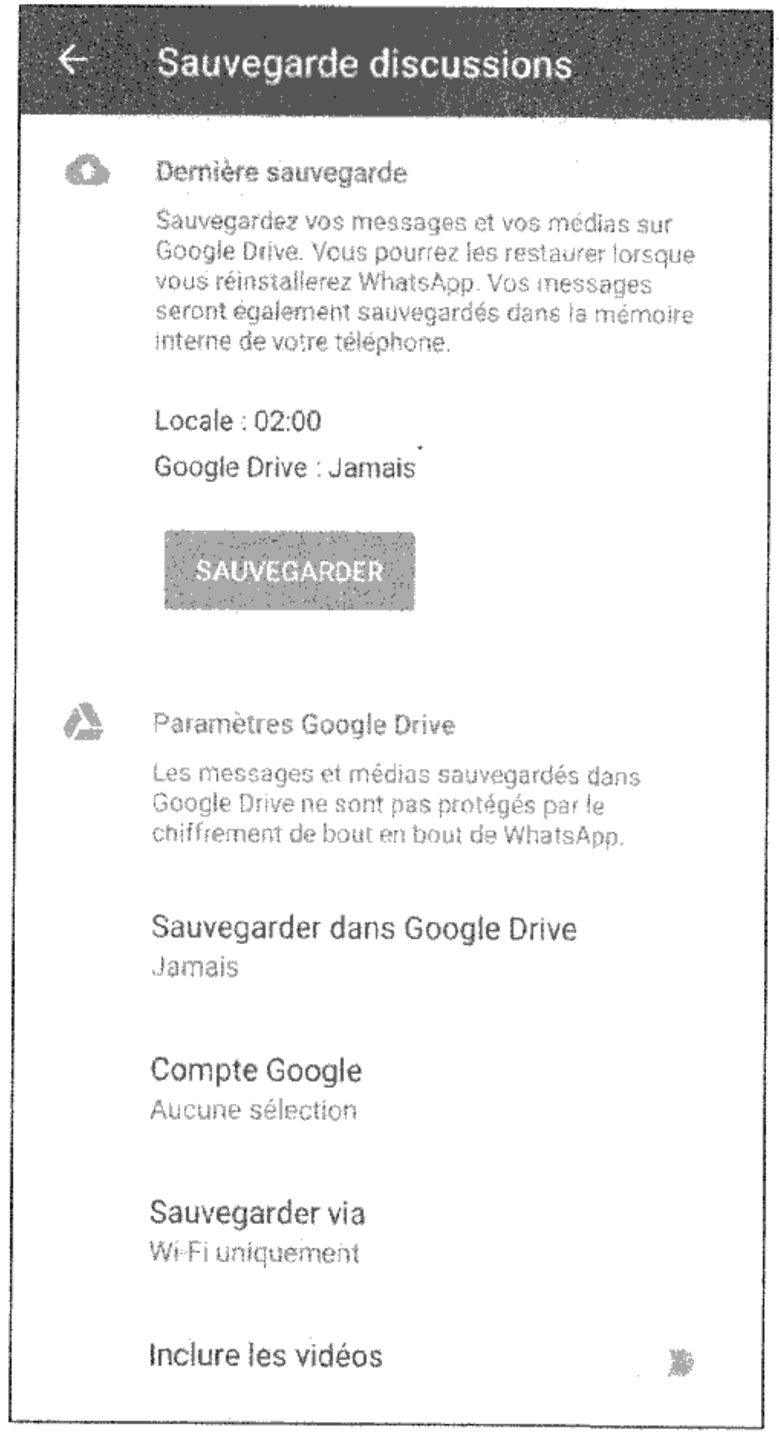
Dans de nombreuses affaires, les suspects n'ont pas fourni les codes d'accès au téléphone ou permis le déverrouillage de WhatsApp. Mais à la suite d'investigations informatiques, les messages ainsi sauvegardés sur le smartphone ont été récupérés même ceux qui avaient été effacés grâce aux techniques de récupération de données effacées. La sauvegarde Google Drive ou iCloud est également facilement accessible.

Conclusion, sauf nécessité, n'activez pas la sauvegarde des conversations sur WhatsApp.

Pour accéder aux paramètres de sauvegarde : *Paramètres > Discussions > Sauvegarde discussions*

Ne renseignez aucun compte Google Drive ou iCloud et sélectionnez « jamais » pour l'option de sauvegarde.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats



3. Les messages temporaires

Depuis novembre 2020, Whatsapp a lancé une nouvelle fonctionnalité appelée "Messages temporaires".

En pratique les messages échangés avec le contact ou le groupe sélectionné **s'autodétruisent automatiquement au bout de 7 jours.**

La mise en place des messages temporaires fonctionne de la façon suivante:

1. Ouvrez la discussion WhatsApp,
2. Appuyez sur le nom du contact ou du groupe,
3. Appuyez sur Messages temporaires,
4. Si cela vous est demandé, appuyez sur Continuer.
5. Sélectionnez Activés (sur Android) ou Oui (sur iPhone)

Conseils utiles:

- Supprimez régulièrement les discussions inutiles ainsi que l'historique dans l'onglet « appels ».

- Lorsque vous supprimez une discussion, n'hésitez pas à cocher l'option « supprimer les images et vidéos pour mon correspondant ». Ce qui permet de ne laisser aucune trace des deux côtés.

- Désactivez l'option de téléchargement automatique des images et des vidéos qui vous sont transmises. Ces fichiers sont automatiquement enregistrés dans votre smartphone et contiennent de nombreuses données.

- WhatsApp est une société américaine et obéit au droit américain. Ainsi elle collabore avec les autorités dans le cadre de commission rogatoire internationale uniquement.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

WhatsApp fournit aux autorités les informations d'identifications et de connexion au compte et peut selon les cas fournir les messages échangés. Néanmoins, les messages sont supprimés des serveurs après un certain délai sauf si les autorités ont effectué une demande pour « geler » les données du compte. Ce « gel des données » est limité à 90 jours.

15. TELEGRAM

Telegram est une application mobile de messagerie instantanée sécurisée. Elle est disponible sur Google Play et Apple Store.

L'application a vu le jour en 2013 à l'initiative de Nikolaï et Pavel Dourov, fondateurs du réseau social russe « VKontakte ». Après la prise de contrôle par le gouvernement russe du réseau « VKontakte », les deux frères décident de créer une messagerie chiffrée pour permettre de communiquer sans être espionnés par les services secrets russes.

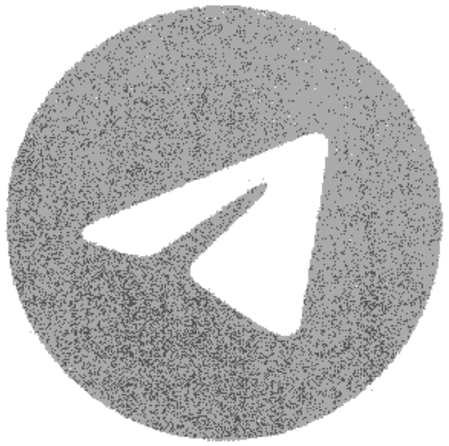
Les fondateurs de Telegram ont refusé de fournir au gouvernement russe les clés de déchiffrement du code de l'application. Une décision de justice fut prise dans le but d'interdire Telegram en Russie. Nikolaï et Pavel Dourov n'ont jamais voulu satisfaire les autorités en permettant le déchiffrage des messages et ils n'étaient pas en mesure de le faire, le chiffrement s'effectuant directement sur le téléphone de l'utilisateur. L'application est toujours utilisable en Russie à ce jour et plusieurs pays tentent d'interdire son accès, l'Inde l'a quant à elle bloqué sur son territoire.

Nikolaï et Pavel Dourov ont fini par installer le siège de leur société aux Émirats arabes unis (Dubaï).

Les messages sur Telegram sont chiffrés sur l'appareil de l'utilisateur et transitent par les serveurs de l'application. Le protocole de chiffrement de Telegram n'est pas en libre accès ce qui suscite une certaine méfiance de la part des spécialistes du chiffrement qui ne peuvent ainsi vérifier sa solidité et dénoncent son opacité.

Les échanges les plus sécurisés sur Telegram sont ceux utilisant la fonction « échange secret » (secret chat). En décembre 2014, Pavel Dourov offrait 300 000 dollars à qui serait capable de briser le chiffrement des secrets chats.

Début 2018, Telegram dépassait les 200 millions d'utilisateurs à travers le monde. L'application fut médiatisée en France en raison de son usage par les djihadistes. Elle est aussi très prisée du milieu politique français ou du Président de la République comme le révèle l'affaire « Benalla » en 2019[1].



Telegram offre une très large gamme de services permettant au travers des discussions d'échanger des images, vidéos, fichiers en tout genre, sans limites de taille. L'application chiffre également les appels audios et les appels vidéo.

[1] https://www.europe1.fr/politique/benalla-affirme-avoir-echange-regulierement-avec-macron-depuis-lete-3829970

Elle permet les discussions de groupe et les « chaînes ». Les chaînes sur Telegram sont des canaux de discussions qu'un ou plusieurs administrateurs alimentent en message. Elles peuvent regrouper plusieurs milliers d'abonnés.

Nous déconseillons l'usage des discussions de groupe, car elles ne disposent pas du chiffrement de bout en bout. Idem pour les chaînes dont le contenu s'affiche automatiquement au sein de l'application et se retrouve ainsi sur votre smartphone.

La plupart des images, vidéos ou fichiers transitant sur les différentes chaînes consultées,, sont automatiquement téléchargées sur la mémoire du smartphone si l'option n'est pas désactivée. Avoir une image ou une vidéo téléchargée sur son smartphone à l'issue du suivi d'une chaîne Telegram ne doit pas laisser nécessairement sous-entendre qu'elle a été consultée.

Seul l'échange secret offre un niveau de chiffrement et des options de sécurité optimales pour votre confidentialité, ainsi nous évoquerons exclusivement l'usage du « secret chat ».

1. Pseudonyme et contacts

L'application Telegram s'active à l'aide de votre ligne mobile et il vous sera demandé d'entrer un code d'activation reçu par SMS ou par appel vocal.

Choisissez un nom d'utilisateur, ainsi, si une personne souhaite vous trouver sur Telegram, elle pourra le faire à l'aide de ce nom sans avoir à connaître votre numéro de téléphone.

Telegram se synchronise avec votre répertoire pour vous proposer vos contacts utilisant également l'application. De votre côté, vous verrez également ceux qui parmi vos contacts utilisent Telegram.

2. Paramètres conseillés pour une sécurité optimale :

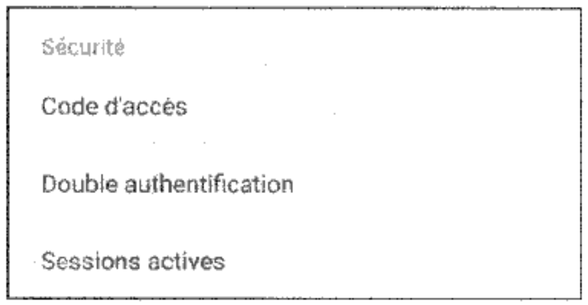
➢ Code d'accès et verrouillage de l'application

Nous vous conseillons de verrouiller l'accès à l'application à l'aide d'un code d'accès. Vous pouvez également activer le déverrouillage de l'application à l'aide de votre empreinte digitale.

Pour l'activer, accédez au menu de l'application en cliquant sur l'onglet en haut à droite de l'accueil :

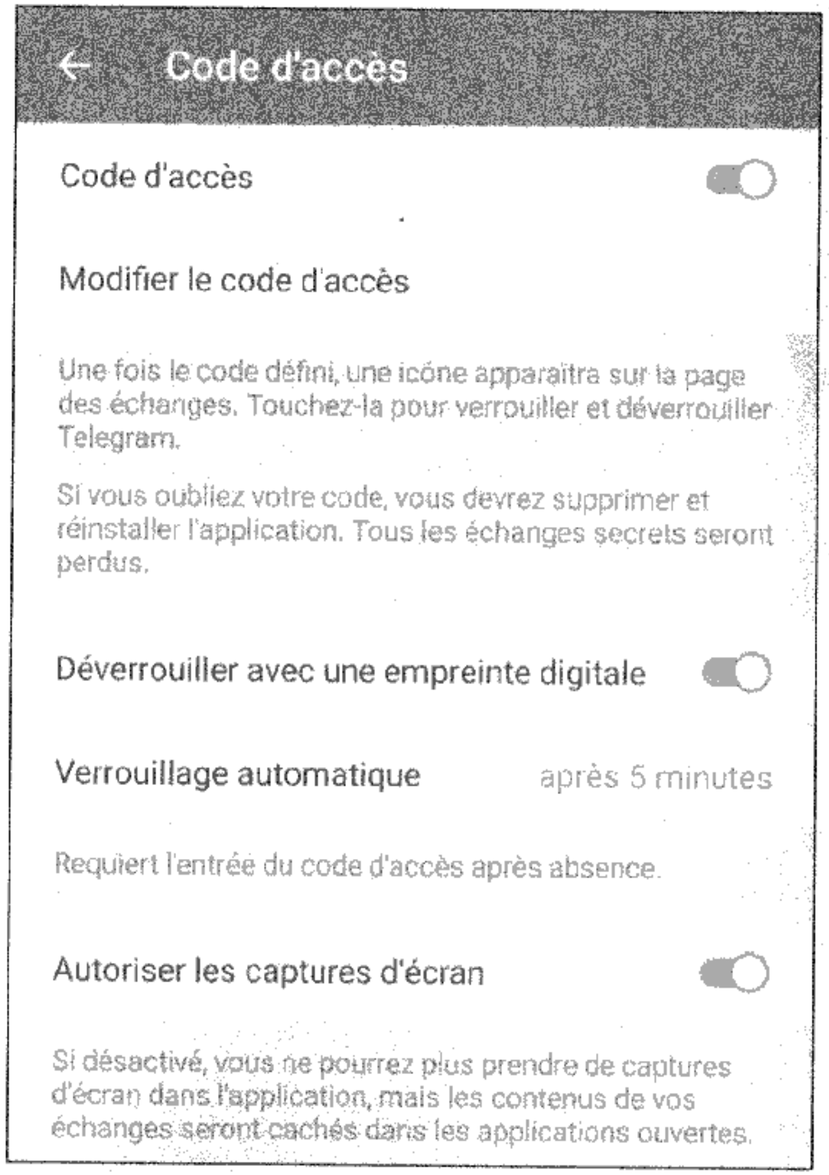
(le cadenas situé en haut à gauche permet de verrouiller l'application lorsque vous la fermerez.)

Une fois sur le menu, suivez le chemin suivant :
Paramètres > Confidentialité et Sécurité



Accédez à l'onglet « code d'accès ».

Activez le code d'accès. Il vous sera demandé à chaque ouverture de l'application. Choisissez le verrouillage automatique. Ainsi après une période d'inutilisation de Telegram, **l'accès se verrouillera automatiquement garantissant l'impossibilité d'accéder aux messages à votre insu.**

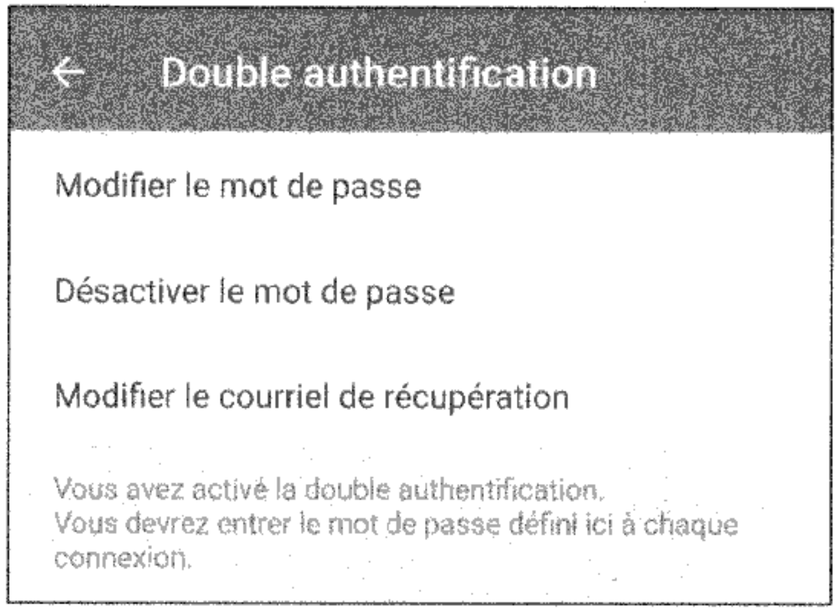


➢ La double authentification

Si vous souhaitez accéder à Telegram sur un autre smartphone ou si vous réinstallez l'application, vous pourrez le faire à l'aide d'un code de vérification envoyé par SMS. Pour éviter une intrusion sur votre compte par une tierce personne qui tenterait d'intercepter vos messages, **activez la double authentification**. Ce code vous sera demandé à chaque fois que vous réinstallerez l'application.

Il est connu de vous seul et augmente très fortement la sécurité d'accès à votre compte Telegram.

Pour l'activer : *Paramètres > Confidentialité et Sécurité > Double Authentification*



➢ La suppression automatique du compte

Cette option est disponible dans l'onglet « Confidentialité et sécurité ». Il permet de régler la suppression automatique du compte. Le réglage minimal (conseillé) est **de 3 mois**. Si pendant 3 mois, vous ne vous connectez pas à votre compte Telegram, il est automatiquement supprimé ainsi que son contenu.

➢ Sessions actives

Dans l'onglet « Confidentialité et sécurité », cet onglet permet de visualiser sur quel appareil votre compte Telegram est actif. **Si vous n'utilisez Telegram que sur votre smartphone, une seule connexion active doit apparaître.**

Vérifiez régulièrement que seule la session de votre téléphone est active. Si ce n'est pas le cas, déconnectez les autres sessions.

➢ Numéro de téléphone

L'onglet « Numéro de téléphone » se situe sur la page « Confidentialité et sécurité ».

Cette option permet de limiter la possibilité de vous trouver sur Telegram à l'aide de votre numéro de mobile.

Le réglage sur « mes contacts » à « Qui peut voir mon numéro de téléphone ? » permettra à ceux qui ont déjà votre numéro dans leur répertoire de le voir s'afficher sur Telegram.

Le réglage sur « Personne » et « mes contacts » ne donneront l'accès à votre numéro uniquement si vous avez ces contacts dans votre propre répertoire.

Utilisez cette option si vous souhaitez limiter la possibilité de voir votre numéro de téléphone et dans ce cas ne fournissez que votre nom d'utilisateur pour être contacté sur Telegram.

- **La sauvegarde des données**

Telegram sauvegarde automatiquement vos discussions qui seront stockées sur leurs serveurs. Ainsi si vous perdez votre téléphone ou l'accès au compte, vous retrouverez l'intégralité de vos échanges. Idem lorsque vous accédez à votre compte sur un autre appareil ou sur la version de Telegram en ligne. Seuls les échanges secrets ne sont pas sauvegardés.

L'application Telegram ne laisse aucune trace de vos messages dans la mémoire du téléphone, ils sont inaccessibles sans accès autorisé de votre part.

En revanche, les images, vidéos et fichiers téléchargés (automatiquement la plupart du temps) laisseront une trace exploitable et très facile à récupérer même si l'accès est verrouillé.

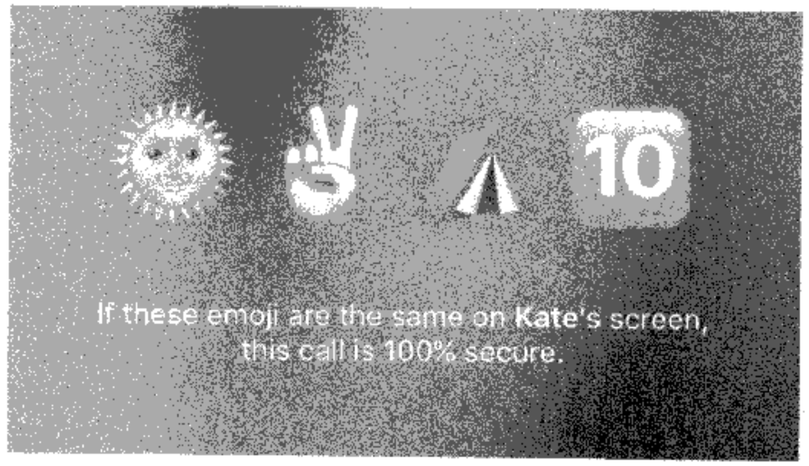
Pour une meilleure confidentialité, désactivez le téléchargement automatique des « médias ».

- **Les appels audios**

Vous pouvez passer un appel audio avec l'un de vos contacts Telegram. Les conversations sont entièrement chiffrées **et impossibles à intercepter dans le cadre d'une écoute judiciaire ou administrative.**

Telegram propose de vérifier que l'appel est bien chiffré et qu'aucune intrusion n'est en cours.

Lorsque vous passez un appel, une série de 4 symboles s'affichera en haut de l'appel en cours.



Si votre interlocuteur Telegram voit s'afficher sur son écran la même série de symboles, **alors l'appel est entièrement sécurisé.**

Dans le journal d'appel de Telegram, vous pouvez supprimer l'historique. L'application vous proposera également de supprimer l'historique de l'appel pour votre correspondant. Cela permet d'effacer l'historique même sur le téléphone de votre contact.

Cette option est également disponible pour les discussions et les groupes. Tous vos messages seront supprimés partout où ils se trouvent. N'hésitez pas à cliquer sur l'option lorsqu'elle vous est proposée à la suppression d'une discussion.

3. **<u>Les échanges secrets (Secret Chat)</u>** :

Pour garantir un chiffrement optimal et discuter en toute sécurité, nous vous conseillons d'utiliser les discussions initiées par le biais de l'échange secret.

Les échanges secrets garantissent un chiffrement de bout en bout et aucun des échanges ne transite par les serveurs de Telegram. Le chiffrement a lieu à l'envoi au sein de votre smartphone et arrive directement sur le smartphone de votre correspondant.

Les avantages :

- ***L'autodestruction des messages.*** En haut à droite de la discussion, vous pouvez définir le délai dans lequel s'autodétruiront les messages sur votre téléphone et celui de votre contact.

  Vous pouvez régler le délai de « 1 seconde » à « 1 semaine ». Une fois le message lu par votre contact, **le message sera automatiquement supprimé selon le délai choisi.**

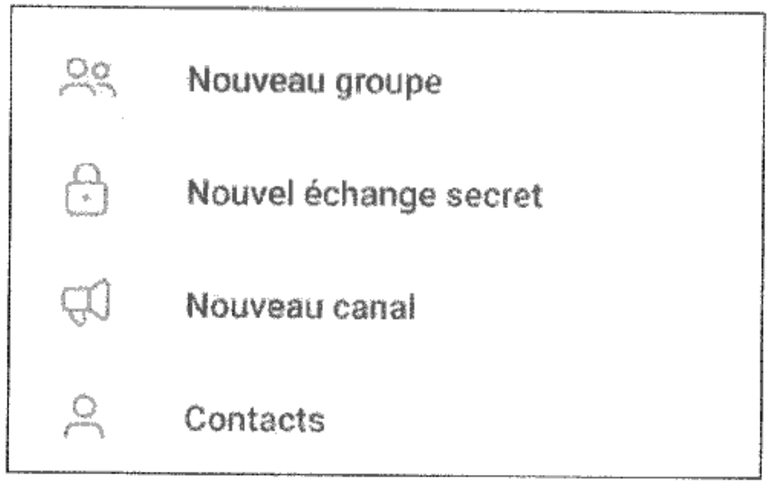
  C'est la garantie de ne pas oublier d'effacer vos messages et que les messages soient supprimés pour tout le monde.

- ***Pas de capture d'écran.*** L'échange secret interdit à vous et à votre contact d'effectuer une capture d'écran. Si votre contact essaie de faire une capture, vous recevrez une notification.
  Néanmoins, rien n'empêche votre contact de prendre son écran de téléphone en photo.

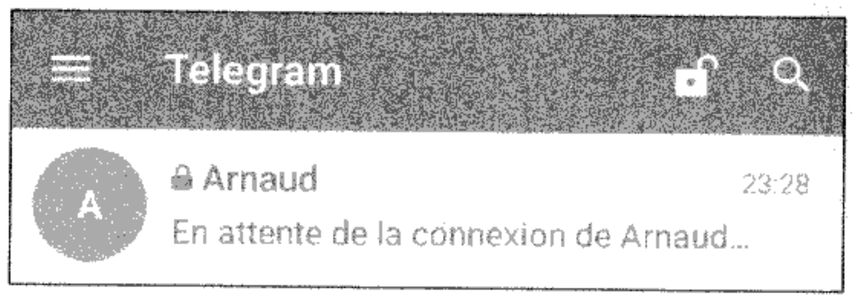
- ***Suppression de la discussion.*** Quand vous supprimez la discussion, tout son contenu s'efface également sur le téléphone de votre contact.

- ***Pas de sauvegarde et pas de trace.*** L'échange secret est visible uniquement sur le téléphone où vous l'initiez. Il n'est pas possible de retrouver un échange secret si votre compte Telegram est utilisé sur un autre appareil. **De même, les échanges secrets ne laissent aucune trace sur le smartphone.**

Pour lancer un échange secret :
Menu principal > Nouvel échange secret.



Choisissez le contact et la discussion se lance une fois que l'application a réussi à se mettre en lien avec votre contact.



Le cadenas vert indique que la discussion est intégralement chiffrée et sécurisée.

4. **<u>Conseils utiles</u> :**

- Supprimez régulièrement les discussions inutiles ainsi que l'historique dans l'onglet « appels ».

- Évitez de télécharger les vidéos ou photos envoyées dans les discussions. Ces photos sont enregistrées dans votre smartphone et contiennent de nombreuses données à dispositions des hackers.

- Telegram n'est pas en mesure de fournir de renseignements sur les échanges secrets. De surcroit, Telegram ne dispose pas de service des obligations légales. **L'entreprise ne collabore ni avec les forces de police ni avec les gouvernements.**

- Les groupes et les chaînes Telegram représentent un canal d'informations fluide, en temps réel. Si vous n'avez pas paramétré la visibilité de votre numéro de téléphone, celui-ci sera visible des membres de la conversation et il sera possible de vous identifier.

- **Nous vous déconseillons d'utiliser la version Telegram Desktop (sur ordinateur), car en cas de vol, les traces de vos échanges seront multiples et facilement accessibles.**

16. SIGNAL

Signal est une application mobile de messagerie instantanée sécurisée. Elle est disponible sur Google Play et Apple Store.

Signal a vu le jour dans sa première version le 29 juillet 2014 à l'initiative de l'organisation Open Whisper Systems. Les bases de Signal ont été posées par l'unification de Redphone et Textsecure, deux messageries chiffrées lancées en 2010. En 2011, Textsecure fût racheté par Twitter, mais son créateur Moxie Marlinspike quitta la plateforme en juillet 2012 pour continuer le développement de Textsecure et Redphone sous la forme d'un projet collaboratif open source au sein de sa nouvelle entité l'Open Whisper Systems.

Toutes les messageries chiffrées développées par l'Open Whisper Systems forment aujourd'hui le « Signal Protocol ».

Le 21 février 2018, Moxie Marlinspike et Brian Acton, co-fondateur de WhatsApp, ont annoncé la création de la Signal Foundation, un organisme à but non lucratif dont la mission est de "soutenir, accélérer et élargir la mission de Signal de rendre la communication privée accessible et ubiquiste."

Signal a la particularité d'être une messagerie chiffrée totalement transparente, son logiciel étant gratuit et open source (accessible à tout le monde). L'application est financée par des

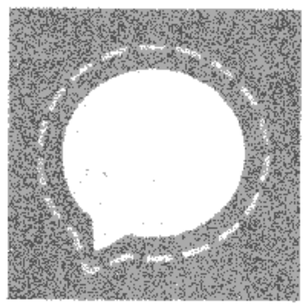
subventions et des dons. C'est ce qui fait sa force aujourd'hui, car cela permet aux experts en cybersécurité de vérifier régulièrement la fiabilité du chiffrement de l'application et elle est en évolution constante pour assurer la sécurité des utilisateurs.

Signal garanti le chiffrement de bout en bout des messages. Ainsi ni Signal ni aucune autre personne à travers le monde ne sera en mesure de lire le contenu de vos échanges.

Dans une interview[1] sur France Inter le 16 septembre 2019, **Edward Snowden affirmait aux journalistes n'utiliser exclusivement que l'application Signal**. Le lanceur d'alerte connu pour avoir révélé les programmes de surveillance de masse américains et britanniques recommande de ne pas utiliser WhatsApp ou Telegram, mais d'utiliser uniquement Signal pour les communications.

En 2020, la Mozilla Fundation délivré la note de 5/5 à l'application et l'évoque comme l'application de messagerie la plus sûre au monde.

Signal est en constante évolution et l'application propose désormais la possibilité de ne plus être identifié à l'aide d'un numéro de mobile afin de garantir son anonymat. La mise en place du protocole « Signal PIN'S » est une réelle avancée vers l'avenir des messageries chiffrées qui n'utiliseront plus le numéro de mobile comme identifiant.



[1] https://www.franceinter.fr/emissions/l-invite-de-8h20-le-grand-entretien/l-invite-de-8h20-le-grand-entretien-16-septembre-2019

Les paramètres de sécurité et de confidentialité de base sur l'application Signal sont excellents et clairement prévus pour un usage sécurisé à tout instant.

Cependant attention aux réglages. Signal propose également de se substituer aux applications de votre smartphone pour envoyer des SMS ou émettre des appels, vers vos contacts ne disposant pas de l'application. Ces SMS et appels ne sont pas chiffrés. Nous vous indiquerons comment désactiver cette option pour utiliser uniquement des messages chiffrés avec vos contacts utilisant eux aussi Signal.

1. La création du compte Signal et du profil.

Une fois l'application installée, vous procéderez à l'activation de votre compte. Contrairement à WhatsApp ou à Telegram, **Signal n'exige pas que le numéro utilisé pour la création soit le même que celui de la carte SIM présente dans votre téléphone.**

Vous pouvez utiliser un autre numéro pour recevoir le code par SMS ou appel. Il faut juste être en mesure de recevoir le code.

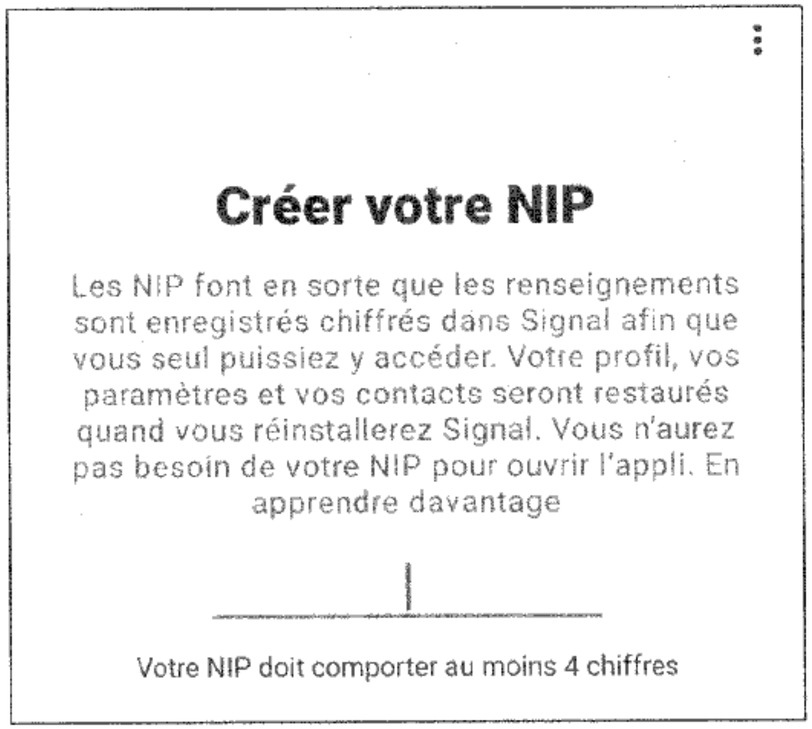
En termes d'anonymat, cela permet d'activer un compte Signal à l'aide d'une puce prépayée sur un autre mobile.

Vos contacts devront avoir connaissance de ce numéro pour pouvoir vous envoyer des messages sur Signal.

Lors de votre première ouverture de Signal, il vous sera offert la possibilité de restaurer une sauvegarde à l'aide de votre code « NIP » qui est une sécurité de double authentification. Ceci bloque toute tentative d'accéder à votre compte sur un autre appareil.

Si vous ne vous souvenez plus de votre code « NIP », il sera possible d'accéder à votre compte Signal à l'aide de votre numéro de mobile mais il sera totalement vierge et sans messages.

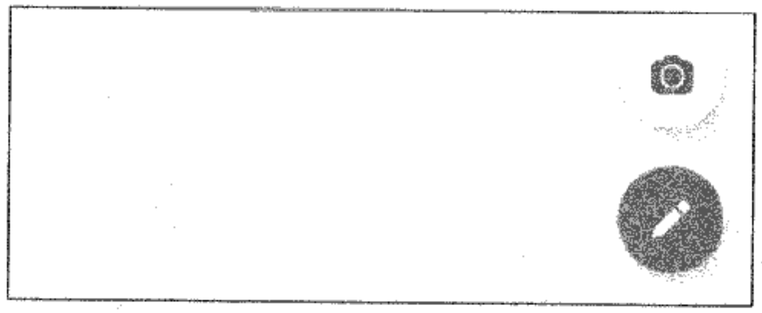
Dans tous les cas, Signal vous proposera soit d'entrer votre « NIP », soit d'en créer un nouveau lié à votre numéro de mobile.



2. **<u>La confidentialité des messages</u>**.

Signal vous permet d'envoyer des messages chiffrés à un groupe de personne ou à un seul correspondant. Contrairement à Telegram, toutes les conversations et les appels (audios et vidéos) **sont totalement chiffrés dès le départ** ainsi il n'existe pas « d'échanges secrets ».

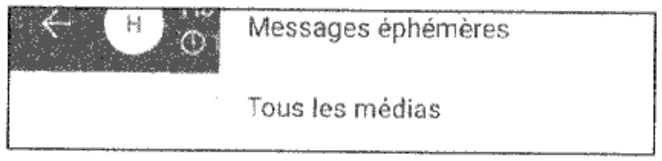
Pour créer une conversation, il vous suffit de cliquer sur l'icône en forme de crayon en bas à droite de l'accueil de l'application et de choisir votre correspondant Signal.



- **Les messages éphémères**

Signal propose l'option d'autodestruction des messages pour toutes les conversations. Une fois les messages lus, ils s'effaceront automatiquement au bout du laps de temps choisi.

Pour régler l'autodestruction, cliquez sur les paramètres de la conversation située en haut à droite et réglez l'option « messages éphémères ». Vous pouvez régler l'autodestruction de 5 secondes à une semaine.



Une fois le réglage d'autodestruction effectué, il s'appliquera automatiquement à chaque fois que vous engagez une conversation avec le même contact.

➢ **Le numéro de sécurité**

Signal propose de vous assurer de la sécurité de l'échange. Ainsi vous avez accès au sein de la conversation, au niveau de la fiche de votre contact, au numéro de sécurité de la conversation.

Comparez ce numéro avec celui affiché sur l'écran de votre correspondant. Les deux numéros de sécurité doivent être identiques. Si tel est bien le cas et qu'aucun problème n'est à signaler, indiquer cet échange comme « vérifié ». Par la suite si votre contact change de numéro de sécurité, vous serez averti.

Le numéro sera différent si votre contact change de téléphone ou qu'il réinstalle Signal. **Si le numéro change souvent, c'est le signe que quelque chose ne va pas et que votre contact n'est pas fiable.**

3. **<u>Paramètres conseillés pour une sécurité optimale :</u>**

Pour accéder aux paramètres de l'application, cliquez sur les trois points en haut à droite de la page d'accueil.

➢ Textes et messages multimédias

L'onglet « Textos et messages multimédias » situé dans les paramètres de l'application concerne la possibilité d'envoyer des SMS ou passer des appels, non chiffrés, avec tous les contacts de votre répertoire, pour ceux n'utilisant pas Signal.

Nous vous conseillons de vérifier si cette option est bien désactivée et de ne pas la mettre en place, pour ne pas risquer d'envoyer de SMS non sécurisé.

Voici le paramétrage préconisé :

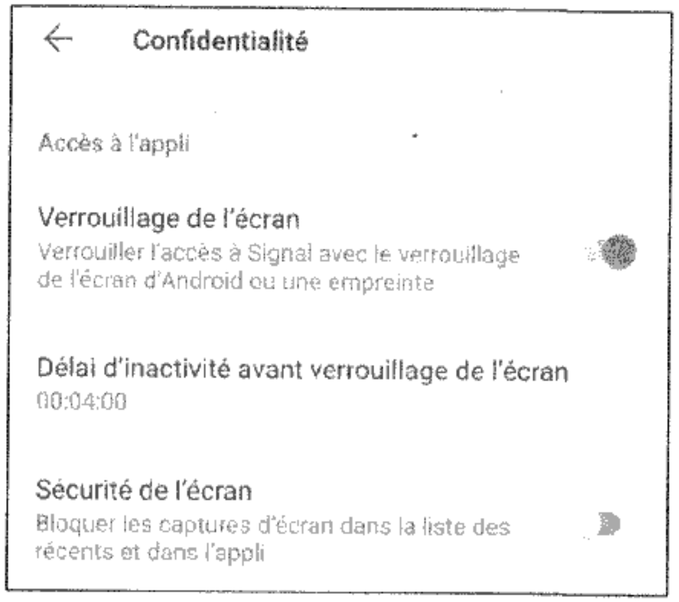
➢ Accès à l'application

Dans l'onglet confidentialité des paramètres, plusieurs options sont à prendre en compte pour protéger votre compte et vos échanges :

- **Le verrouillage de l'écran** par code ou par empreinte afin d'empêcher l'accès à vos messages si votre téléphone est déverrouillé et entre les mains d'un tiers.

- **Le délai d'inactivité avant verrouillage de l'écran**. À régler afin que l'application Signal se verrouille automatiquement au bout d'un certain temps.

- **Sécurité de l'écran**. Indispensable, cette option vous empêche de faire des captures d'écran dans l'application et bloque cette possibilité pour vos contacts lors des discussions.

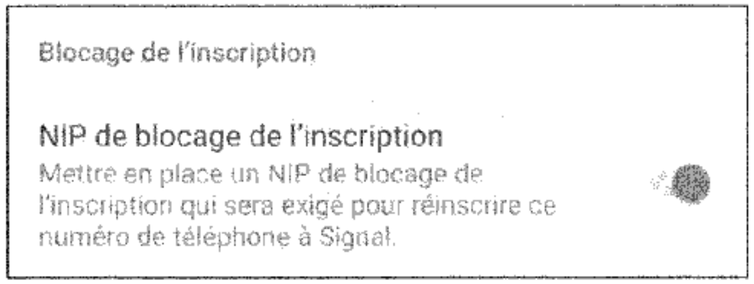


➢ Blocage de l'inscription (Double authentification)

Si vous souhaitez accéder à Signal sur un autre smartphone ou si vous réinstallez l'application, vous pourrez le faire à l'aide d'un code de vérification envoyé par SMS. Pour éviter une intrusion sur votre compte par une tierce personne qui tenterait d'intercepter vos messages, **activez la double authentification**.

Signal vous demandera de renseigner ce code à 8 chiffres (Appelé numéro « NIP ») défini par vous-même à chaque fois que vous réinstallerez l'application.

Signal vous demandera régulièrement d'entrer votre numéro NIP.



Il est connu de vous seul et augmente très fortement la sécurité d'accès à votre compte Signal.

- **La sauvegarde des messages**

Signal ne sauvegarde aucun message, ni sur le smartphone, ni sur leur serveur. Seules les discussions non effacées sont présentes dans l'application, mais sont totalement irrécupérables sans accès à l'application.

Si vous réinstallez votre compte sur un votre smartphone ou sur un autre, vous n'aurez aucun historique de vos messages. C'est un réglage par défaut.

Nous vous déconseillons de sauvegarder vos messages, néanmoins un onglet dans « Conversations et médias » permet de l'activer.

Une procédure complexe pour sauvegarder vos messages Signal est à suivre et consultable sur ce lien :

https://support.signal.org/hc/fr/articles/360007059752-Sauvegarder-et-restaurer-des-messages

4. Quelques conseils :

Signal se révèle être l'application de messagerie chiffrée **la plus complète et sécurisée à l'heure actuelle.** Ses options par défaut sont programmées pour assurer la meilleure confidentialité à ses utilisateurs. La transparence de son développement et la qualité du chiffrement sont unanimement reconnues par les professionnels de la cybersécurité.

Cependant :

- **Supprimez régulièrement les discussions inutiles.** Les historiques d'appels s'affichent directement dans une discussion et ne s'autodétruisent pas. Veillez à supprimer les messages indiquant « Vous avez appelé ».

- **Évitez de télécharger les vidéos ou photos envoyés dans les discussions.** Ces médias sont enregistrés dans votre smartphone et contiennent de nombreuses données.

Signal n'enregistre aucune donnée sur ses utilisateurs et n'est pas en mesure de fournir le contenu des messages aux autorités. Il n'existe pas d'informations relatives à la collaboration de Signal avec les autorités gouvernementales.

17. LES ADRESSES IP & VPN

Utiliser un smartphone, c'est se connecter à internet au travers d'un navigateur mobile ou des multiples applications, c'est s'identifier sur de nombreux sites internet de la vie quotidienne.

Toutes ces connexions laissent une trace exploitable par les enquêteurs et qui permet d'identifier un individu avec la même précision qu'un numéro de mobile. Il s'agit de l'adresse IP.

L'adresse IP signifie « Internet Protocol » et se trouve à la base du fonctionnement d'internet. Chaque matériel informatique utilisant internet (Routeur, serveur, ordinateur, smartphone, box internet, etc.) se voit attribuer une adresse IP par le fournisseur d'accès internet.

L'adresse IP permet aux ordinateurs de s'identifier sur le réseau et de communiquer entre eux. Lorsque vous visitez un site internet, vous écrivez dans la barre d'adresse le nom : www.lesite.fr. En réalité, l'adresse du site conduit votre navigateur vers l'adresse IP où se trouve stocké le site en question.

Une adresse IP est publique. Vous pouvez connaître la vôtre en cherchant sur un moteur de recherche « mon adresse IP ».

Deux types d'adresses IP existent :

- L'IPv4 (ancien format)
  184.160.133.241

- L'IPv6 (nouveau format)
  5800:10C3:E3C3:F1AA:48E3:D923:D494:AAFF.

Vous pouvez vous-même consulter sur internet, à quel fournisseur d'accès appartient une adresse IP et où elle est localisée dans le pays.

Exemple : L'adresse 184.160.133.241 est localisée au Canada dans la ville de Saint-Rémi (Québec)

1. Où se trouve enregistrée mon adresse IP ?

La plupart des sites sur lesquels nous nous connectons enregistrent dans leurs bases, la date, l'heure et l'adresse IP que nous utilisons. Ainsi lorsque vous vous connectez à votre boite mail, le site sera en mesure de fournir avec quelle adresse IP un utilisateur s'est connecté à son compte.

Exemple : Vous déposez une annonce sur le site d'annonces www.leboncoin.fr. Les autorités s'intéressent à l'annonce que vous avez déposée et souhaitent vous identifier. Ils vont demander à l'aide d'une réquisition, à l'entreprise gestionnaire du site « Leboncoin » de fournir les informations inscrites par celui qui a déposé l'annonce et également l'adresse IP utilisée avec la date et l'heure et le nombre de connexions.

L'adresse IP est attribuée à chaque accès internet par le fournisseur d'accès. Il peut donc s'agir soit de l'opérateur de votre abonnement mobile ou du fournisseur d'accès internet de votre box (fibre ou ADSL).

Il y a deux cas de figure concernant l'adresse IP sur un smartphone :

- Si nous utilisons la connexion internet sur notre smartphone grâce à votre forfait Data, l'adresse IP est celle que fournit notre opérateur téléphonique.

- Si vous êtes connecté à un réseau Wifi pour utiliser internet sur votre smartphone, **l'adresse IP sera celle du fournisseur d'accès internet de la box diffusant le réseau Wifi.** Tous les équipements (ordinateurs, téléphone, tablette) connectés à ce réseau Wifi auront la même adresse IP.

2. L'adresse IP dans les enquêtes judiciaires ou administratives

Notre adresse IP est unique et identifiable. Si nous utilisons internet grâce à notre abonnement mobile (3G / 4G), l'adresse IP est fournie par notre opérateur mobile. Si nous utilisons internet via le wifi de la box de votre domicile, l'adresse IP est fournie par le fournisseur d'accès internet de votre box.

Les enquêteurs peuvent identifier le titulaire d'une adresse IP française, de la même manière qu'ils identifient le titulaire de l'abonnement d'une ligne mobile. Pour cela, ils transmettent une réquisition via la PNIJ à l'opérateur concerné pour demander l'identification du titulaire d'une adresse IP.

En retour, l'opérateur fournira le nom et les informations du titulaire de l'abonnement qui utilise l'adresse IP de connexion.

Les opérateurs mobiles et fournisseurs d'accès internet sont tenus de conserver pendant un an toutes les adresses IP attribuées à un abonné mobile ou une box internet.

Dans le cas où l'adresse IP qu'ils souhaitent identifier est celle de notre connexion DATA via le réseau mobile sur smartphone, cela

revient à identifier le titulaire de la ligne mobile utilisée sur le téléphone en question.

En revanche, si nous utilisons une connexion Wifi, l'adresse IP renverra au titulaire de la box. **Concrètement si nous nous connectons sur la box internet de notre frère ou de notre voisin, les enquêteurs obtiendront pour résultat leurs noms**, puisque l'adresse IP renvoie à leur abonnement fibre ou ADSL.

Si nous utilisons un réseau Wifi public (Wifi d'une gare, d'un café, d'un hôtel) en libre accès, l'adresse IP que nous laisserons sur les sites internet sera identifiable, mais renverra au nom de l'établissement ayant fourni l'accès Wifi. **Ce sera en quelque sorte une connexion « anonyme ».**

3. Comment les enquêteurs identifient-ils un individu grâce à l'adresse IP ?

Que vous consultiez votre compte « Gmail », que vous commandiez un livre avec votre compte Amazon, ou que vous postiez un message sur Facebook, tous ces sites enregistrent votre adresse IP utilisée (avec date et heure). Nous sommes donc identifiables si l'adresse IP renvoie à notre propre abonnement mobile ou notre box internet à la maison.

Exemple : Les enquêteurs souhaitent identifier le titulaire du compte Facebook « Anemonedu75 ». Pour cela, ils vont demander à Facebook de leur fournir l'historique de connexion de ce compte avec les adresses IP utilisées.

Ils obtiendront en retour le listing de toutes les connexions du compte « Anemonedu75 » avec toutes les adresses IP utilisées.

Les enquêteurs constateront par exemple que le compte utilise toujours plusieurs adresses IP qui renvoient après identification à des Wifi publics dans la même ville. Le titulaire du compte

Facebook ne sera pas identifié.

Mais si « Anemonedu75 » s'est connecté une fois avec le Wifi de chez lui, l'adresse IP apparaîtra dans le listing de connexions (appelés Logs de connexion) et les enquêteurs pourront remonter jusqu'à lui.

Au même titre qu'une écoute téléphonique, il est possible pour les enquêteurs de placer une adresse IP ou un accès internet ciblé, sur interception. Ils obtiennent en retour, tous les sites internet consultés sur la connexion internet.

4. L'adresse MAC

Contester la réalité de l'utilisation d'une adresse IP est possible par exemple par la pluralité d'utilisateurs d'un réseau et une multitude de supports numériques au domicile. Mais un autre élément rentre en ligne de compte : **l'adresse MAC** *(Media Acces Control).*

Il s'agit d'un identifiant **unique** numérique associé à chaque périphérique telle une carte réseau WIFI. C'est l'équivalent d'une plaque d'immatriculation. Elle ne change jamais même si plusieurs techniques permettant de la modifier existent.

Exemple d'une adresse MAC : 00:1B:44:11:3A:B7

Cette adresse MAC revêt une grande importance dans les enquêtes judiciaires. Lors de la connexion à internet, ce dernier enregistre non seulement l'adresse IP mais également (pas systématiquement) l'adresse MAC du périphérique informatique utilisé.

C'est en soi une preuve. Si dans un dossier, un client ne reconnait pas s'être connecté à un site ou un réseau social, si l'adresse MAC de son ordinateur ou de son téléphone correspond à celle enregistrée lors de la connexion, cela représente une charge supplémentaire.

A contrario, à décharge, faire vérifier l'adresse MAC de connexion à un site, pour la comparer aux supports numériques de l'affaire, peut conduire à discriminer l'utilisateur des appareils si l'adresse MAC utilisée ne correspond pas.

L'adresse IP et l'adresse MAC se trouvent être des traces numériques redoutables pour identifier un individu. Cependant, l'expansion de l'utilisation de VPN représente un frein majeur à l'identification via l'adresse IP.

5. Le VPN

VPN signifie « Virtual Private Network » pour « réseau virtuel privé ».

Le VPN est un programme installé sur votre ordinateur ou votre smartphone qui permet de masquer votre véritable adresse IP. En temps normal, votre fournisseur d'accès internet fait le lien directement à travers le réseau entre vous et le site internet que vous consultez.

Lorsque vous utilisez un VPN, c'est le réseau du VPN qui établit le lien entre votre ordinateur et le site internet consulté.

Pour résumer :

- **Sans VPN**, vous êtes connecté directement au site internet qui connaît ainsi votre véritable adresse IP.

- **Avec un VPN**, celui-ci fait office d'intermédiaire. Vous passez par le serveur du VPN pour consulter le site qui lui obtient en retour l'adresse IP de votre VPN et non pas votre adresse IP personnelle.

Les VPN disposent de serveurs partout dans le monde. Une adresse IP permet d'identifier le pays et la ville dans laquelle se trouve son utilisateur. Mais comme vous utilisez l'adresse IP du

VPN, le site internet est dupé et pense que vous êtes connecté dans un autre pays !

Les VPN sont utilisés par exemple pour déjouer la censure mise en place dans certains pays qui restreignent internet et l'accès à certains sites.

Le VPN crée un « tunnel » directement entre vous et le site que vous consultez. **Ce tunnel vous protège des intrusions et vos données sont protégées, la plupart des fournisseurs de VPN chiffrant la connexion.** Toutes les informations que vous transmettez (documents sensibles, coordonnées bancaires) sont chiffrées sur le même principe que les messageries sécurisées, dès le départ sur votre ordinateur ou téléphone et ne peuvent être interceptés.

En ce qui concerne l'historique de vos consultations internet, votre fournisseur d'accès internet est en mesure de fournir aux autorités tous les sites que vous visitez.

Avec un VPN, les sites que vous visitez sont masqués et le fournisseur d'accès internet n'a donc aucun historique. Seul le VPN peut avoir connaissance de vos connexions, d'où l'intérêt de choisir un VPN dit « no logs », qui ne conserve aucun historique, qui n'enregistre pas ce que vous faites sur internet.

Sur le plan procédural, utilisez un VPN est souvent assimilé à une volonté de se dissimuler. Mais c'est un raccourci rapide, car au-delà de l'accessibilité grandissante des VPN, ces derniers permettent de se protéger en partie des tentatives de phishing ou d'hacking. Faire usage d'un VPN sur les supports numériques d'un cabinet d'avocats, c'est augmenter considérablement le degré de protection des données sensibles.

Pour résumer, un VPN offre l'avantage de :

- Masquer notre adresse IP et donc notre identité, peu importe sur quel réseau nous sommes connectés.
- Empêcher un tiers non autorisé de connaître la liste de nos consultations internet. (Sauf si bien entendu elles sont enregistrées physiquement sur l'historique de navigation de smartphone).
- Limiter fortement le risque d'être victime d'un hacker et de fuite de vos données.
- Contourner la censure de certains pays.

Il existe des VPN gratuits et des VPN payants. Les VPN payants offrent l'avantage de ne pas limiter la vitesse de votre connexion internet et offrent un grand choix de serveurs à travers le monde.

Veillez à choisir un service VPN qui chiffre vos données et qui n'enregistre pas vos connexions (no logs) telles que « NordVPN » *(dont le siège se trouve au Panama et qui limite sa collaboration avec les autorités gouvernementales.)*

Les VPN sont également disponibles sur smartphone et offrent une protection en permanence.

De nombreuses personnes pensent à tort qu'utiliser un VPN est une garantie d'anonymat sur internet. C'est une fausse idée pour deux raisons. La première c'est que de nombreux VPN enregistrent les données de connexion (d'où l'importance de bien choisir son VPN). La deuxième c'est une fois de plus l'erreur humaine qui est à l'origine de l'identification. Il suffira d'une connexion, en ayant oublié d'activer le VPN, pour laisser une trace identifiable et exploitable.

Le VPN est un véritable atout pour assurer la confidentialité et se protéger des tentatives de vol de données.

CONCLUSION

Seules la pratique et la consultation des procès-verbaux techniques, d'exploitations, la consultation des scellés en cours et en fin de procédure, vous permettront d'associer l'ensemble des éléments que nous avons évoqués et en tirer le profit nécessaire pour la défense des intérêts de votre client.

C'est un travail fastidieux et parfois difficile à mettre en œuvre, d'exploiter sans la capacité technique d'un service enquêteur, l'ensemble des données récoltées lors d'une procédure. Mais alors qu'un procès-verbal reflètera un raisonnement tronqué, qu'une écoute aura été mal ou partiellement retranscrite, alors la preuve ne revêtira plus son caractère formel.

Légalité des procédures, vérifications des délais, des durées, du placement sous scellé, ce sont autant d'éléments à contrôler. Demander des actes d'investigations pour préciser et compléter des déclarations, minorer l'importance d'un élément technique, sur la base de ce guide vous pourrez défricher le terrain de la téléphonie mobile d'investigation.

Il suffira parfois de demander à connaître la couverture d'une borne relai, de matérialiser des points de rencontres de plusieurs lignes mobiles, de faire vérifier les différents boitiers téléphoniques

utilisés par une ligne, pour amorcer un virage stratégique dans votre défense.

L'évolution des techniques d'investigation en matière de téléphonie mobile est constante. Les projets mis en place par l'État sont nombreux et ces chantiers verront le jour dans quelques années. Plus que jamais, il est crucial d'être bien informé tant la frontière entre nécessités de l'enquête et l'atteinte au respect de la vie privée est poreuse.

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

ANNEXE

L'ensemble des prestations proposées par la Plateforme Nationale des Interceptions Judiciaires à disposition des forces de l'ordre sont publiques. Elles sont listées à l'article A43-9 du Code de Procédure pénale et permettent de visualiser l'ensemble des possibilités offertes en termes d'investigation.

Article A43-9
(Extrait partiel – Source www.legifrance.gouv.fr)
Modifié par Arrêté du 4 février 2020

I. Conformément aux dispositions de l'article R. 213-2, les réquisitions adressées dans les conditions prévues au présent code ayant pour objet les interceptions de communications de téléphonie donnent lieu à remboursement aux opérateurs de communications électroniques, sur facture et justificatifs, en appliquant à ces demandes, pour chacune des prestations demandées, le montant hors taxe des tarifs fixés dans le tableau annexé au présent arrêté.

II. Conformément aux dispositions de l'article R. 213-1, les réquisitions adressées dans les conditions prévues au présent code ayant pour objet la production et la fourniture des données mentionnées à l'article R. 10-13 du code des postes et des communications électroniques donnent lieu à remboursement aux

opérateurs de communications électroniques, sur facture et justificatifs, en appliquant à ces réquisitions, pour chacune des prestations demandées, le montant hors taxe des tarifs fixés dans les tableaux annexés au présent article.

III. - Pour les prestations ne figurant pas dans les tableaux annexés, le montant du remboursement est déterminé en accord avec l'opérateur ou sur devis.

****

La liste de toutes les prestations est consultable à l'adresse suivante :

https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000041553495/2020-10-02

Investigations & Téléphonie mobile : Le guide à l'usage des avocats

A Sédar,

Ma force et mon inspiration

Le téléphone mobile est aujourd'hui au coeur des enquêtes judiciaires. Les investigations téléphoniques sont omniprésentes au sein de la procédure pénale et sont devenues incontournables dans la lutte contre la délinquance et la criminalité organisée. L'arsenal législatif s'est adapté en conséquence et les avocats y sont confrontés chaque jour.

Ce guide unique a pour objectif d'informer les avocats, mais aussi les professionnels du droit sur les techniques d'investigations déployées par les enquêteurs et les services de renseignements. Au travers des dossiers qui vous sont confiés, la téléphonie apparaît désormais comme l'élément de preuve incontournable.

De l'identification de l'utilisateur d'une ligne mobile aux interceptions de communications, nous vous initions aux différents outils à disposition des enquêteurs et aux différentes techniques mises en place. Enfin, pour garantir la confidentialité de vos échanges, nous vous informerons sur les bonnes pratiques d'utilisation des messageries sécurisées.

Cédric.D alias "Haurus" est un ancien fonctionnaire de police de la DGSI. Il vous livre ici son expérience en matière de téléphonie d'investigation. PNIJ, Fadettes, écoutes, Imsi Catcher, Keylogger, Whatsapp, Telegram, Signal n'auront plus de secrets pour vous.

18,90 € TTC

ACAB

Dépôt légal : Janvier 2021