RAPPORT

LA PROCEDURE PENALE FACE AUX EVOLUTIONS DE LA CYBERCRIMINALITE ET DU TRAITEMENT DE LA PREUVE NUMERIQUE :

PROPOSITIONS POUR UNE EFFICACITE JURIDIQUE RENFORCEE

24 janvier 2018

Cyberlex
Association loi 1901
https://www.cyberlex.org/

Centre expert contre la cybercriminalité français
Association loi 1901
https://www.cecyf.fr/

LA PROCEDURE PENALE FACE AUX EVOLUTIONS DE LA CYBERCRIMINALITE ET DU TRAITEMENT DE LA PREUVE NUMERIQUE : PROPOSITIONS POUR UNE EFFICACITE JURIDIQUE RENFORCEE

La présente contribution est le fruit de la réflexion collective de membres de l'association Cyberlex, Association du droit et des nouvelles technologies, et du CECyF, Centre Expert contre la Cybercriminalité Français, lancée à l'initiative d'Éric FREYSSINET et de Corinne THIERACHE afin de concrétiser le partenariat avec la complémentarité des compétences de ces deux organisations, inauguré en juin 2014.

Un premier rapport de ce groupe de travail consacré au Code pénal a été discuté au cours de l'année 2016 et rendu public en janvier 2017 à l'occasion du FIC 2017. Les travaux de l'année 2017 ont porté sur le Code de procédure pénale confronté aux évolutions de la cybercriminalité et des techniques ou méthodes de recueil de la preuve numérique.

PRESENTATION DE CYBERLEX

Cyberlex réunit, depuis 1996, des juristes d'entreprise, des avocats, des professeurs de droit, des magistrats ainsi que des professionnels du marché d'Internet et des technologies numériques.

Cyberlex ne représente pas une opinion mais des opinions, à l'image de la diversité de ses membres, excluant tout lobbying. L'ambition de Cyberlex est de contribuer à mieux comprendre le monde des nouvelles technologies et l'évolution des usages, appréhender les différents aspects du droit et ainsi participer à sa meilleure lisibilité.

PRESENTATION DU CECYF

Le CECyF est une association créée en 2014 regroupant des services de l'Etat chargés de la lutte contre la cybercriminalité, des établissements d'enseignement et de recherche ainsi que des entreprises de toutes tailles.

Ils ont réuni leurs forces pour mener des actions de prévention, de formation et de recherche et développement contre la cybercriminalité. Le CECyF est le résultat du projet européen 2CENTRE qui vise à développer un réseau de telles initiatives à travers l'Europe. L'association est aussi membre du projet européen SENTER qui perpétue 2CENTRE et de l'association européenne ECTEG de développement de formations contre la cybercriminalité.

METHODOLOGIE ADOPTEE

Un groupe de travail composé de membres de Cyberlex et du CECyF, disposant de compétences juridiques et techniques nécessaires à la compréhension des enjeux sociétaux, juridiques et économiques de la cybercriminalité, a donc été mis en place sous la direction de Corinne THIERACHE, Ancienne présidente et membre de Cyberlex, et d'Éric FREYSSINET, Secrétaire général du CECyF, afin de coordonner les différents travaux (ci-après le Groupe de travail Cyberlex – CECyF).

Les réflexions qui ont alimenté ces travaux et les recommandations qui en ont découlé reprises dans le présent rapport sont proposées par les membres du Groupe de travail Cyberlex – CECyF en toute indépendance et n'engagent que ces derniers. Elles ne sauraient donc engager leurs employeurs.

Plusieurs réunions mensuelles de réflexion ont été tenues par le Groupe de travail Cyberlex – CECyF entre juillet 2017 et janvier 2018, ainsi composé (dans l'ordre alphabétique) :

Membres de Cyberlex contributeurs :

- Carole BUI, Avocat
- Matthieu CAMUS, Expert sécurité des données et vie privée
- Jean-Sébastien MARIEZ, Avocat
- Myriam QUEMENER, Magistrat, docteur en droit
- Corinne THIÉRACHE, Avocat associé

Membres du CECyF contributeurs :

- Philippe BAUDOIN, Officier de gendarmerie
- Éric FREYSSINET, Officier de gendarmerie (également membre de Cyberlex)
- Catherine HORNAIN, Inspectrice de la concurrence, de la consommation et de la répression des fraudes
- Alexandre HUGLA, Juriste
- Marc WATIN-AUGOUARD, Général d'armée de gendarmerie (2S)

POURQUOI UN NOUVEAU RAPPORT SUR LA CYBERCRIMINALITE ?

Le précédent rapport du Groupe de travail dirigé par Marc Robert dit « Rapport Robert » rendu le 16 février 2014 traitait déjà de manière exhaustive d'un certain nombre de problématiques spécifiques liées au Code de procédure pénale. Toutefois, le temps s'est écoulé depuis, soit presque quatre années, au cours desquelles nous avons pu constater une accélération de l'adoption de nouveaux textes en la matière sous la pression de la menace réelle du terrorisme et de la cybercriminalité mettant en lumière de nouveaux besoins en termes de clarification textuelle.

Ceci est d'autant plus important que le Code de procédure pénale :

- ⇨ constitue un outil indispensable pour accompagner et encadrer le travail des praticiens (magistrats, enquêteurs, avocats) et contribuer à clarifier leurs interactions avec les différents acteurs de l'enquête numérique (opérateurs, hébergeurs, experts…),
- ⇨ énonce des règles qui sont de plus en plus souvent invoquées pour recueillir la description et l'encadrement de nouvelles méthodes d'enquête,
- ⇨ et enfin assure la sécurisation des procédures sur le plan juridique, lesquelles peuvent être facilement fragilisées en l'absence de tout respect rigoureux des textes en vigueur.

OBJECTIFS POURSUIVIS PAR CYBERLEX ET LE CECYF

Il s'agit ici de contribuer à la clarification des procédures pénales applicables à la lutte contre la cybercriminalité. Il ne s'agit pas de faire des modifications massives des dispositions du Code de procédure pénale mais plutôt des propositions permettant de remédier à des lacunes ou à des incohérences. Le but est de proposer des pistes de réflexion au législateur pour des évolutions futures. Celles-ci devront être accompagnées par une hausse des ressources affectées à ce contentieux par essence souvent complexe, transversal et international.

Table des matières

1 Evolution de la compétence judiciaire 6
1.1 Compétence territoriale 6
1.2 Juridictions spécialisées 8
1.2.1 Les JIRS ne peuvent se saisir de toute infraction et leur champ de compétence infractionnel est limité. 9
2 Enquêtes sous pseudonyme 10
2.1 Description du dispositif actuel 10
2.1.1 Les investigations sous pseudonyme sur Internet : définition et différentiation 10
2.1.2 Spécificités de l'enquête sous pseudonyme 11
2.1.3 Le champ d'application de l'enquête sous pseudonyme 12
2.2 Difficultés et éclaircissements à apporter 13
2.3 Proposition d'évolution : extension et harmonisation 13
2.4 Coups d'achat 16
2.5 Notion de patrouille numérique et veille policière 17
3 Accès à la preuve numérique 19
3.1 Données stockées 19
3.1.1 Définition des catégories de données 19
3.1.2 Conservation des données 21
3.1.3 Réquisitions 22
3.2 Gel de données 23
3.3 Perquisitions et constatations 24
3.3.1 Dispositions spécifiques 24
3.3.2 Accès à distance 25
3.4 Analyses techniques et expertises 26
3.5 Interception 26
3.5.1 Cas spécifique de l'interception de flux réseaux 27
3.6 Géolocalisation 27
3.6.1 Rappel : Définition – Terminologie 27
3.6.2 La géolocalisation en temps réel avant la loi du 28 mars 2014 relative à la géolocalisation 28
3.6.3 La géolocalisation appréhendée par la loi du 28 mars 2014 29
3.7 Chiffrement 30
3.7.1 Rappel sémantique et définitions 31
3.7.2 Mise au clair des données chiffrées nécessaires à la manifestation de la vérité (articles 230-1 et suivants du Code de procédure pénale) 31
3.7.3 Captation de données 33

4 Coopération internationale 37
4.1 Convention du Conseil de l'Europe sur la cybercriminalité 37
4.2 Directive NIS 38
4.3 Coopération avec les pays tiers 38
5 CONCLUSION 41
Annexe I Infractions visées par les dispositions d'enquête sous pseudonyme
Annexe II RGPD & directive et projet de règlement e-privacy

1 Evolution de la compétence judiciaire

1.1 Compétence territoriale

Le sujet de la compétence territoriale étant intimement lié à la procédure pénale, que la dimension internationale d'Internet rend particulièrement complexe à appliquer, nous avions fait le choix dans le précédent rapport consacré à la réforme du Code pénal de traiter ce sujet dans le cadre de notre analyse des dispositions du Code de procédure pénale.

Aujourd'hui, les juridictions françaises pourront être reconnues compétentes dans un certain nombre de contentieux relatifs à Internet en application des règles prévues par le Code pénal.

Les règles de compétence se fondent sur deux critères combinés :

- Le lieu de commission de l'infraction ;
- La nationalité de l'auteur ou de la victime.

Selon le principe de territorialité posé par l'article 113-2 du Code pénal, « *La loi pénale française est applicable aux infractions commises sur le territoire de la République. L'infraction est réputée commise sur le territoire de la République lorsqu'un de ses faits constitutifs a eu lieu sur ce territoire* ».

Appliquée à Internet, cette compétence des juridictions françaises était retenue dès lors que les contenus illicites diffusés par Internet étaient accessibles depuis la France[1]. Toutefois, la seule accessibilité s'est avérée insuffisante pour les juges qui lui ont préféré le critère de l'orientation du site

[1] *A titre d'exemple, le Tribunal de grande instance de Paris (TGI Paris, 26 févr. 2002, CCE 2002/5. Comm. 77), confirmé par la Cour d'appel de Paris (Paris, 17 mars 2004, CCE 2005/4. Comm. 72, obs. Lepage), a considéré que l'article 113-2 du Code pénal est applicable en matière de délit de presse commis à partir ou grâce à internet, notamment dès lors que la publicité (élément constitutif de l'infraction) a été faite via internet et est accessible depuis la France. Dans cette affaire, « la mise à disposition du public d'un site de vente aux enchères d'objets nazis, qui peut être vu et reçu sur le territoire français et auquel l'internaute peut accéder, du fait de la simple existence d'un lien informatique "search" qui l'y invite, caractérise l'élément de publicité constitutif de l'infraction de délit d'apologie de crime de guerre, et sans qu'il soit besoin que l'internaute ait été démarché par le propriétaire du site ».*

Internet vers le public français[2] ou le *« centre des intérêts de la victime »*[3] et plus généralement des critères rattachant au territoire français les faits constitutifs de l'infraction[4].

La loi du 3 juin 2016 *renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale* est venue clarifier la qualification d'infraction « *commise sur le territoire de la République* » en introduisant le nouvel article 113-2-1 du Code pénal qui dispose que :

> *« Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République ».*

Pour les infractions commises en dehors du territoire français, d'autres critères permettent de retenir la compétence des tribunaux français :

- **La nature des faits** : il convient de distinguer selon la qualification criminelle ou délictuelle des faits :

    - En matière criminelle, la loi pénale française est applicable à tout crime commis par un Français hors du territoire de la République (art. 113-6, al. 1 du Code pénal).

    - En matière délictuelle, la loi pénale française n'est applicable aux délits commis par les Français hors du territoire de la République que « *si les faits sont punis par la législation du pays où ils ont été commis* » (art. 113-6, al. 2 du Code pénal).

      L'article 227-27-1 du Code pénal prévoit cependant une dérogation aux dispositions de l'article 113-6, alinéa 2, du Code pénal. Ainsi, les infractions prévues par les articles 227-22, 227-23, 227-25 à 227-27 (atteintes aux mineurs) du même Code commises à l'étranger par un Français ou une personne résidant habituellement sur le territoire français, relèvent de la loi française sans qu'une double incrimination ne soit nécessaire et sans que le ministère public ait le monopole des poursuites. Le but est

[2] Ont ainsi été retenus par les juges des critères tels que la langue utilisée et la disponibilité pour ce public des produits vendus pour fonder leur compétence (Crim. 9 sept. 2008, n°07-87.281).

[3] *Dans une ordonnance du 11 octobre 2012, le président du tribunal de grande instance de Nanterre, a conclu que « les juridictions françaises étaient compétentes pour connaître de l'entier préjudice occasionné par les atteintes alléguées à son droit à l'image » par des sites étrangers (TGI Nanterre, ord. ME, 11 oct. 2012, www.legalis.net). À cette fin, le juge a rappelé la jurisprudence de la Cour de justice de l'Union européenne (CJUE, gr. ch., 25 oct. 2011, eDate Advertising GmbH c/ X et Olivier M., Robert M. c/ MGN Ltd) selon laquelle « la personne qui s'estime lésée peut saisir soit les juridictions de l'État membre du lieu d'établissement de l'émetteur de ces contenus, soit les juridictions de l'État membre dans lequel se trouve le centre* ***de ses intérêts »****. En l'espèce, le juge a constaté que le centre des intérêts de la victime se situait en France, car elle y était née, elle y résidait avec sa famille et y exerçait son activité professionnelle.*

[4] La Chambre criminelle a ainsi considéré, concernant des propos diffamatoires diffusés à partir d'un site internet localisé à l'étranger, « *qu'en l'absence de tout critère rattachant au territoire de la République les propos incriminés, la circonstance que ceux-ci, du fait de leur diffusion sur le réseau internet, aient été accessibles depuis ledit territoire ne caractérisait pas à elle seule, un acte de publication sur ce territoire rendant le juge français compétent pour en connaître* » (Crim. 12 juillet 2016, n°15-86.645).

en effet de simplifier la répression des délits de diffusion de contenus illicites (corruption de mineur, enregistrement ou transmission, en vue de sa diffusion, de l'image pornographique d'un mineur, atteintes sexuelles sur mineur) sur Internet ;

- **La nationalité de la victime** : l'article 113-7 du Code pénal rend *« la loi pénale française applicable à tout crime ainsi qu'à tout délit puni d'emprisonnement, commis par un Français ou par un étranger hors du territoire de la République lorsque la victime est de nationalité française au moment des faits »*.

  Cette disposition serait susceptible de s'appliquer notamment aux victimes françaises d'actes de pédophilie dont les images seraient diffusées sur Internet ;

- **L'application d'une convention internationale :** Cette compétence des juridictions françaises est renforcée par l'article 689 du Code de procédure pénale qui permet également aux juridictions françaises de juger les auteurs d'infractions commises hors du territoire de la République lorsqu'une convention internationale donne compétence aux juridictions françaises pour connaître de l'infraction.

Enfin, il convient de noter que l'article 113-5 du Code pénal prévoit, pour les infractions de cybercriminalité commises à la fois sur le territoire français et à l'étranger, que :

> *« La loi pénale française est applicable à quiconque s'est rendu coupable sur le territoire de la République, comme complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi française et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère* ***».***

Recommandation n°1 : Statu quo sur la compétence

Le nouvel article 113-2-1 du Code pénal nous semble répondre aux incertitudes juridiques jusqu'alors existantes en matière de compétence pour la cybercriminalité et ce, notamment en ce qu'il se réfère au critère le plus adéquat qui est celui qui s'attache aux effets de l'infraction, en particulier sur la victime.

1.2 Juridictions spécialisées

Les Juridictions interrégionales spécialisées (JIRS) sont au nombre de huit : sept en métropole (Paris, Lille, Rennes, Bordeaux, Marseille, Lyon et Nancy) et une en Outre-mer (Fort-de-France). Le ressort de chacune d'elles couvre le ressort de plusieurs cours d'appel selon le découpage territorial défini par les articles D.47-3 et D.47-13 du Code de procédure pénale. Le lieu d'implantation de la JIRS détermine en pratique la qualité de « *procureur de la République de la JIRS* » et celle de *« procureur général de la JIRS »* encore appelés procureur de la République et procureur général « *de l'interrégion* ».

La compétence territoriale d'une JIRS s'étendant sur le ressort de plusieurs tribunaux de grande instance et sur le ressort de plusieurs cours d'appel, le procureur de la République de la JIRS et le procureur général de la JIRS entretiennent des liens étroits avec leurs homologues procureurs de la République et procureurs généraux non JIRS.

1.2.1 Les JIRS ne peuvent pas se saisir de toute infraction et leur champ de compétence infractionnel est limité.

Les JIRS sont compétentes pour l'enquête, la poursuite, l'instruction et le jugement des crimes et délits entrant dans le champ d'application des articles 706-73 (à l'exception du 11°, relatif aux crimes et délits constituant des actes de terrorisme et du 18°, relatif aux crimes et délits contribuant à la prolifération des armes de destruction massive), 706-73-1 et 706-74 du Code de procédure pénale, dans les affaires qui apparaîtraient d'une grande complexité.

Les JIRS sont compétentes pour un grand nombre d'infractions les plus graves et pour celles en lien avec la cybercriminalité. On peut notamment citer celles prévues par l'article 706-73-1 du Code de procédure pénale comme le délit d'escroquerie en bande organisée, prévu au dernier alinéa de l'article 313-2 du Code pénal, le délit d'atteinte aux systèmes de traitement automatisé de données à caractère personnel mis en œuvre par l'État commis en bande organisée, prévu à l'article 323-4-1 du même code et le délit d'évasion commis en bande organisée prévu au second alinéa de l'article 434-30 dudit code. Concernant ces infractions, il est possible de recourir à un régime partiel renforcé de la criminalité organisée avec toutes les techniques d'enquête spéciale, exception faite de l'article 706-88 du Code de procédure pénale relatif à la garde à vue de 96 heures.

En matière économique et financière, la compétence matérielle des JIRS, pour les affaires qui sont ou apparaîtraient d'une grande complexité, en raison notamment du grand nombre d'auteurs, de complices ou de victimes ou du ressort géographique sur lequel elles s'étendent, est fixée par l'article 704 du Code de procédure pénale.

Les JIRS exercent par ailleurs une compétence facultative. La loi ne prévoit aucune hypothèse dans lesquelles les juridictions interrégionales spécialisées auraient pour obligation de se saisir d'une procédure. En l'état, les JIRS ont traité 21% d'affaires économiques et financières et 79% d'affaires liées à la criminalité organisée et jusqu'à présent la cybercriminalité est peu identifiée en tant que telle.

La loi prévoit que les magistrats du siège et du parquet affectés auprès des juridictions spécialisées sont désignés à cette fin par les premiers présidents et les procureurs généraux des cours interrégionales. Il appartient à ces derniers d'apprécier la compétence des postulants au regard de leur expérience professionnelle et/ou des formations qu'ils ont suivies. Ces magistrats ainsi désignés sont dits « *habilités JIRS* ». Il convient de relever que le nombre d'habilitations JIRS (permanentes ou temporaires) ne correspond pas nécessairement au nombre de magistrats travaillant à temps plein au sein des JIRS, certains magistrats ayant en parallèle d'autres activités « *non JIRS* ». Des habilitations temporaires sont par ailleurs délivrées pour permettre le jugement des affaires durant les périodes de vacations. Les parquets généraux disposent d'un ou plusieurs avocats généraux référents qui constituent l'interface entre le premier et le second degré juridictionnel. Des assistants spécialisés peuvent, aux termes des articles 706 et 706-79 du Code de procédure pénale, être désignés aux fins de participer aux procédures relevant de la criminalité organisée.

Recommandation n°2 : Renforcement des JIRS dans le champ de la cybercriminalité.

Il conviendrait de prévoir l'habilitation « cybercriminalité » pour au moins un magistrat par JIRS

2 Enquêtes sous pseudonyme

2.1 Description du dispositif actuel

La liberté de la preuve est un principe érigé par l'article 427 du Code de procédure pénale qui dispose que : « *hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction* ». Toutefois l'accusation doit respecter le principe de la loyauté de la preuve consacré comme principe directeur du procès.

Néanmoins, des techniques spécifiques d'enquête sont permises dans certains cas, par exemple pour lutter contre la criminalité organisée. De la même manière, pour faire face au défi posé par Internet et ses usages, la loi a introduit un moyen d'investigation adapté pour prouver certaines infractions commises par un moyen de communication électronique, en facilitant le recueil de preuves numériques, il s'agit de l'enquête sous pseudonyme.

Ainsi dans un premier temps, la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance a créé de nouvelles dispositions autorisant certains enquêteurs à procéder à des investigations sous pseudonyme sur Internet en matière d'atteintes portées aux mineurs, de traite des êtres humains et de proxénétisme (articles 706-47-3 et 706-35-1 du Code de procédure pénale).

2.1.1 Les investigations sous pseudonyme sur Internet : définition et différentiation

L'enquête sous pseudonyme sur Internet a pour objectif de faciliter la constatation de certaines infractions et lorsque celles-ci sont commises par un moyen de communication électronique, d'en rassembler les preuves, d'en rechercher les auteurs et de les identifier.

Les officiers ou agents de police judiciaire, les agents des douanes, les inspecteurs et les agents de l'ARJEL[5] spécialement habilités à cet effet peuvent utiliser cette technique d'enquête pour rassembler des indices numériques afin de prouver certaines infractions. L'enquête sous pseudonyme sur Internet consiste à interagir avec les suspects par échanges électroniques afin de recueillir des éléments de preuve d'une infraction, et ce sans aucune provocation à la commettre.

Les services opèrent sur Internet en utilisant un pseudonyme afin de mieux traquer les personnes qui commettent des infractions et de parvenir à pénétrer leurs réseaux. Les agents préservent leur anonymat en utilisant une identité d'emprunt pour participer aux échanges et être en contact avec les auteurs de ces infractions notamment sur les réseaux sociaux et sur différents forums.

L'enquête sous pseudonyme est parfois nommée « infiltration numérique » ; parfois le vocable de « *cyber-patrouilles* » est utilisé[6], voire même celui de « *cyber-infiltration* », ce qui relève d'un abus de langage, juridiquement erroné et de nature à susciter des réserves quant à son utilisation[7].

Cette technique spécifique d'enquête doit être distinguée de la « *veille* » sur Internet (cf. infra) et de l'infiltration. L'infiltration est une technique d'enquête d'exception qui ne doit être utilisée que par des

[5] Autorité de régulation des jeux en ligne
[6] Cf. Circulaire interministérielle n° CRIM-2010-7/E6 du 22 mars 2010 relative aux investigations sous pseudonyme sur Internet et au rôle du centre national d'analyse des images de pédopornographie
[7] JurisClasseur Fasc.1110 : infiltrations numériques - Myriam Quemener - 4 février 2015

enquêteurs spécialement habilités et seulement dans le cadre des investigations concernant des infractions prévues par les articles 706-73 et 706-73-1 du Code de procédure pénale. Cette technique spéciale d'enquête, aux termes de l'article 706-81 du Code de procédure pénale, est le fait pour un officier ou un agent de police judiciaire de « *surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs* ». Il est à cette fin autorisé à faire usage d'une identité d'emprunt, allant plus loin qu'un simple pseudonyme.

Moyen d'investigation intrusif, l'infiltration est strictement encadrée par la loi 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, quant aux actes répréhensibles autorisés pour les besoins de l'infiltration, et limitée dans le temps. À peine de nullité, l'opération d'infiltration doit être autorisée par l'autorité judiciaire par décision écrite et spécialement motivée.

2.1.2 Spécificités de l'enquête sous pseudonyme

A la différence de l'infiltration ou du coup d'achat (cf. infra), pour l'enquête sous pseudonyme sur Internet, il n'est pas nécessaire pour l'agent d'obtenir une autorisation préalable d'un magistrat et les opérations effectuées dans ce cadre ne sont pas limitées dans le temps.

Ces enquêtes sous pseudonyme doivent être menées par des officiers et agents de police judiciaire, affectés dans des services spécialisés désignés par arrêté conjoint[8] du ministre de l'Intérieur et du garde des Sceaux, ayant suivi une formation spécifique, et spécialement habilités à cet effet par le procureur général près la cour d'appel dans le ressort de laquelle ils exercent habituellement leurs fonctions, après agrément interne accordé par leur hiérarchie.

Ils peuvent procéder aux actes suivants sans en être pénalement responsables :

- participer sous un pseudonyme aux échanges électroniques ;
- être en contact par ce moyen de communication électronique avec les personnes susceptibles d'être les auteurs des infractions ;
- extraire, acquérir ou conserver par ce moyen des éléments de preuve et des données sur les personnes susceptibles d'être les auteurs de ces infractions ;
- extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus illicites dans des conditions fixées par décret.

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

Comme tout mode de recueil de la preuve, l'enquête sous pseudonyme est soumise au principe de loyauté permettant de garantir un procès équitable. La prééminence de ce principe de loyauté et la prohibition de la provocation à l'infraction sont autant de garde-fous encadrant le recours à ce moyen de preuve numérique. Si ces investigations autorisent la constatation des infractions et la provocation à la fourniture de la preuve de l'infraction, elles ne sauraient, à peine de nullité, avoir pour objet d'inciter à la commission d'une infraction. Ainsi, si l'enquêteur est autorisé à participer sous son « *pseudonyme* », à des échanges électroniques avec un internaute majeur, il ne saurait en revanche

[8] Arrêté du 21 octobre 2015 relatif à l'habilitation au sein de services spécialisés d'officiers ou agents de police judiciaire pouvant procéder aux enquêtes sous pseudonyme.

lui proposer, sans sollicitation expresse préalable, des contenus illicites, sous peine de faire encourir la nullité de la procédure.

2.1.3 Le champ d'application de l'enquête sous pseudonyme

L'enquête sous pseudonyme ne peut être utilisée que pour certaines infractions limitativement énumérées par la loi. Pour s'adapter aux techniques de plus en plus élaborées et astucieuses des délinquants pour échapper à toute identification et au recueil de preuves, le champ d'application de l'enquête sous pseudonyme a été progressivement étendu ces dernières années. Il porte aujourd'hui sur :

- la mise en péril de mineurs
- la traite des êtres humains et le proxénétisme,
- les infractions en matière de paris ou de jeux d'argent ou de hasard en ligne,
- le trafic illicite de médicaments et de produits de santé,
- les infractions constituant des actes de terrorisme, comme la provocation et l'apologie,
- les infractions relevant de la criminalité et de la délinquance organisées,
- le trafic illicite d'espèces sauvages,
- une atteinte à un système de traitement automatisé de données (STAD) bien spécifique.

Le tableau placé en Annexe I présente plus en détail le champ d'application de l'enquête sous pseudonyme, en précisant le texte ayant prévu la possibilité d'utiliser ce moyen d'enquête.

Si les articles 706-35-1, 706-47-3, 706-87-1 du Code de procédure pénale présentent le même socle d'actes autorisés, les articles 706-2-2 et 706-2-3 du Code de procédure pénale visant respectivement le trafic de produits de santé (ordonnance de 2013) et le trafic illicite d'espèces sauvages (loi de 2016) ont rajouté la possibilité d'extraire, acquérir ou conserver les données ou contenus, produits, substances, prélèvements ou services et, plus généralement, les éléments de preuve ou les données sur les personnes susceptibles d'être non seulement les auteurs mais aussi les complices de ces infractions. Cela introduit des possibilités nouvelles comme celle d'acheter en ligne un produit ou substance illicites.

Les douaniers peuvent également utiliser la technique de l'enquête sous pseudonyme dans le cadre du Code des douanes, mais un certain nombre de différences existent vis-à-vis des dispositions du Code de procédure pénale.

Pour les douanes, le champ d'application porte sur les délits douaniers de trafic illicite, de stupéfiants, de tabac et de contrefaçons[9]. Il a été étendu par la loi du 3 juin 2016 aux délits de trafic d'armes, de munitions et d'explosifs[10]. L'article 67 bis-1 du Code des douanes englobe à la fois les techniques de coup d'achat et d'enquête sous pseudonyme.

Ainsi pour user de la technique d'enquête sous pseudonyme, l'agent douanier, habilité par son autorité administrative et quel que soit son service d'affectation, doit y être autorisé par le procureur de la République.

[9] Loi de finances rectificative du 29 décembre 2012, créant l'ESP au sein de l'art. 67 bis-1 du Code des douanes.
[10] Loi 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, modifiant l'article 67 bis-1 du Code des douanes.

On constate donc que l'enquête sous pseudonyme qui était initialement une procédure dérogatoire, devient progressivement une procédure courante, même si son champ d'application est encore limité.

2.2 Difficultés et éclaircissements à apporter

Il convient de noter que le décret précisant les conditions de transmission, d'acquisition et de conservation des contenus illicites prévu au 4° de l'article 706-87-1 du Code de procédure pénale n'a pas encore été pris.

Or, si concernant l'application de l'article 706-47-3 du Code de procédure pénale et la recherche d'infractions prévues par l'article 227-23 du Code pénal, il est clair que le contenu illicite fait référence à une image pédopornographique, pour la recherche des infractions prévues aux articles 706-73 et 706-73-1 du Code de procédure pénale, la notion de contenus illicites manque indéniablement de précision.

A titre d'illustration, un produit stupéfiant est-il un contenu illicite ? En d'autres termes, il y a un problème de formulation. S'il s'agissait de permettre aux enquêteurs d'acquérir un produit stupéfiant proposé à la vente sur un forum (et de vérifier qu'il s'agissait bien de stupéfiant), il aurait été préférable d'adapter une formulation proche de celle utilisée dans les articles 706-2-2 et 706-2-3 du Code de procédure pénale « *3° Extraire, acquérir ou conserver par ce moyen les données ou contenus, produits, substances, prélèvements ou services et, plus généralement, les éléments de preuve [...]* ».

Recommandation n°3 :

Au travers du décret précisant les conditions de transmission, d'acquisition et de conservation des contenus illicites prévues au 4° de l'article 706-87-1 du Code de procédure pénale, il conviendrait de préciser la notion de contenus illicites et, au besoin, l'encadrer.

De manière générale, les difficultés apparaissent quant à l'applicabilité de l'enquête sous pseudonyme face au critère de bande organisée. Sauf à le présumer, il peut être très difficile d'établir la bande organisée. Dans le cas d'une attaque informatique pouvant être d'ampleur, il est possible qu'elle soit le fait d'une bande organisée, tout comme celui d'un seul individu qui aura certes utilisé de multiples services criminels, comme l'achat d'un virus et la location d'un réseau de botnet (« *cybercrime as a service* »). Sans moyen d'approfondir ce point, les enquêteurs ne pourront utiliser cette technique spécifique pour identifier un individu revendiquant l'attaque sur un forum par exemple.

2.3 Proposition d'évolution : extension et harmonisation

Par sa souplesse et sa mise en œuvre sans autorisation judiciaire, l'enquête sous pseudonyme constitue pour les OPJ et APJ un véritable moyen d'investigation à leur initiative.

Cette technique a plusieurs avantages. Elle permet d'assurer l'anonymat sur les réseaux des agents effectuant de telles investigations et de favoriser la préservation de leurs identités. Elle est une étape obligatoire pour certains réseaux sociaux demandant la création d'un profil pour accéder aux informations dites publiques sur le réseau social. Enfin, elle permet aux enquêteurs en intervenant de façon dissimulée, de rassembler plus facilement des indices numériques et de prouver ainsi plus aisément les infractions commises, mais aussi de contourner certaines difficultés et *in fine* de

permettre d'identifier des suspects. Sur ce dernier point, elle constitue parfois le seul moyen d'y parvenir.

Son champ d'application est aujourd'hui encore limité, il conviendrait de l'ouvrir à d'autres infractions. Le cas particulier des atteintes aux systèmes de traitement automatisé de données (STAD) mérite une attention toute particulière (articles 323-1 à 323-8 du Code pénal). Ces attaques informatiques sont au cœur de la cybercriminalité.

Et pourtant, seul le cas particulièrement restrictif de la commission d'une atteinte à un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, en bande organisée (article 323-4-1 du Code pénal) autorise l'enquête sous pseudonyme car il est alors possible d'appliquer les dispositions procédurales spécifiques résultant de l'application combinée des articles 706-72 et 706-73-1 du Code de procédure pénale. Ainsi, la diffusion en bande organisée de logiciels malveillants (virus informatiques) ne peut faire l'objet d'une enquête sous pseudonyme, alors même qu'une telle infraction est souvent facilitée par des échanges électroniques sur des plates-formes réservées à ces criminels. Cette technique pourrait faciliter l'identification des auteurs de ces infractions, en particulier au moment des premières étapes de leur commission.

Il est en conséquence dommage qu'une des dispositions emblématiques introduites pour lutter contre certaines formes de cybercriminalité ne puisse s'appliquer aux infractions qui sont au cœur de cette cybercriminalité.

Plusieurs options sont possibles.

Une première pourrait consister à étendre le bénéfice de l'enquête sous pseudonymes aux atteintes aux STAD en bande organisée, par la modification de l'article 706-73-1 du Code de procédure pénale qui renverrait à l'article 706-87-1 du Code de procédure pénale. L'inscription des atteintes aux STAD en bande organisée dans l'article 706-73-1 du Code de procédure pénale permettrait alors également d'offrir pour ces infractions en bande organisée les autres techniques dérogatoires d'enquête de l'article 706-73-1 du Code de procédure pénale.

Cette option nous apparaît trop restrictive et rencontrerait les difficultés évoquées supra quant à son applicabilité face au critère de bande organisée. Elle ne permet pas non plus de bénéficier de technique spécifique dans une grande majorité des enquêtes.

Une deuxième option consisterait à étendre à toutes les atteintes au STAD la technique d'enquête sous pseudonyme, en même temps que les autres techniques offertes par l'article 706-73-1 Code de procédure pénale[11]. Assez facile à prévoir en matière d'élaboration et de rédaction de texte législatif, c'est cette solution qu'a retenu la commission présidée par le procureur général Marc Robert dans son rapport de février 2014[12]. Sa préconisation n°49 fournit l'argumentation suivante :

« *De telles atteintes peuvent revêtir un degré de gravité particulièrement important dans certaines circonstances et que, par nature, la complexité des enquêtes à mener en ce domaine nécessite de pouvoir disposer de l'ensemble des moyens d'investigation existants*. »

Les critères de gravité et de complexité des faits exigés par le conseil constitutionnel dans ses décisions n°2004-492 du 2 mars 2004 et n° 2013-679 du 4 décembre 2013 seraient respectés. En effet, s'agissant

[11] à l'exception de la garde à vue de 96 heures réservée à la grande criminalité
[12] http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

du critère de complexité, les outils malveillants en vente sur les « *darknet*s » sont très perfectionnés et efficaces, capables d'infecter en très peu de temps des milliers de terminaux touchant à la fois des entreprises et des particuliers. L'extrême rapidité des outils et leur haute sophistication rendent les attaques redoutables et les enquêtes complexes. Dès lors, les outils dont disposent en réponse les enquêteurs doivent pouvoir leur permettre d'agir le plus rapidement possible et le plus efficacement possible.

Quant au critère de gravité, en termes de préjudices, sans être en bande organisée, une attaque informatique menée par un cyberdélinquant peut causer en quelques minutes des préjudices matériels par la destruction de fichiers, des préjudices financiers et de réputation importants.

L'analyse des infractions qui bénéficient déjà de cette technique à travers l'article 706-73-1 du Code de procédure pénale montre qu'elles sont punies de peines allant de 5 ans à 10 ans d'emprisonnement. Les atteintes aux STAD, quant à elles sont punies de peines allant de 2 ans d'emprisonnement pour la simple introduction à 15 ans de réclusion criminelle pour un sabotage. Dès lors, l'intégration de toutes les atteintes aux STAD dans l'article 706-73-1 du Code de procédure pénale[13] paraît cohérente du point de vue de l'échelle de gravité des peines.

Recommandation n°4 :

Intégrer l'ensemble des atteintes aux STAD dans l'article 706-73-1 du Code de procédure pénale afin d'autoriser la technique d'enquête sous pseudonyme pour ces infractions, en même temps que les autres techniques offertes par l'article 706-73-1 du Code de procédure pénale, à l'exception de la garde à vue de 96 heures.

De manière générale, ne faudrait-il pas envisager l'extension de l'enquête sous pseudonyme à toutes les infractions commises par un réseau de communications électroniques. Celles-ci, même si elles ne peuvent être qualifiées de graves, utilisent un moyen qui est propice à impacter de nombreuses victimes de façon simple et rapide, ce qui n'est pas le cas des procédés matériels, et leurs auteurs savent rester anonymes en ne laissant que peu de traces.

On conviendra qu'il faut donc une réponse spécifique et adaptée. Or l'enquête sous pseudonyme paraît être un des rares outils d'enquête efficace pour l'identification et la conservation des preuves. Le fait que seule une technique dérogatoire du droit commun soit applicable à ces infractions permettrait d'échapper à l'inconstitutionnalité puisqu'une seule technique dérogatoire qui a une réelle nécessité, ne peut constituer une atteinte disproportionnée aux droits et libertés fondamentales.

La Cour de cassation justifie, dans un arrêt du 6 mai 2002[14], ce recours à des techniques d'enquête contrevenant au principe de loyauté de la preuve face à la difficulté du constat des infractions ce qui est bien le cas en matière de cybercriminalité, cela ne peut être contesté.

Aussi il conviendrait d'autoriser cette technique d'enquête pour les infractions commises sur Internet, éventuellement en ne retenant que celles punies d'une peine d'emprisonnement d'un quantum

[13] La simple introduction n'est jamais retenue seule mais s'accompagne des infractions connexes de modification ou suppression de données. Au pire, il conviendrait d'exclure les infractions prévues par l'alinéa 1 de l'article 323-1.
[14] Cass. crim. 06/05/2002, n° 02-81-130, inédit.

minimum (2 ans comme pour les interceptions de communications électroniques) lorsque celles-ci sont réalisées par un moyen de communication électronique.

Recommandation n°5 :

Etendre le champ d'application de l'enquête sous pseudonyme aux infractions utilisant un réseau de communications électroniques, éventuellement en ne retenant que celles punies d'une peine d'emprisonnement d'un quantum minimum (2 ans).

L'extension progressive de l'enquête sous pseudonyme ne s'étant pas opérée de façon parfaitement cohérente, les textes actuels en la matière sont fragmentés (de nombreuses dispositions distinctes), incomplets et parfois imprécis. Cette accumulation de régimes résultant des réformes législatives successives, justifie que soit envisagée une refonte du cadre de l'enquête sous pseudonyme non seulement pour redonner de la visibilité à cette technique d'enquête mais également de la cohérence en lissant les particularités entre les régimes.

En particulier, il pourrait être étudié l'objectif d'aller au-delà de l'extraction d'éléments de preuve ou de données et ainsi porter les actes autorisés sur l'acquisition de substances, produits ou services illicites. Ceci dans un cadre judiciaire adapté qui pourrait par exemple faire intervenir le procureur de la République pour autoriser cet acte d'achat, respectant ainsi un parallélisme avec la technique du coup d'achat (cf. infra).

Au-delà de l'extension de l'enquête sous pseudonyme, il est ainsi nécessaire d'harmoniser et de moderniser les régimes procéduraux de l'enquête sous pseudonyme.

Recommandation n°6 :

Parallèlement à l'extension de son champ d'application, harmoniser et moderniser les régimes procéduraux de l'enquête sous pseudonyme.

2.4 Coups d'achat

La technique du coup d'achat a été introduite en matière de trafic de stupéfiants par la loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance. Elle est prévue par l'article 706-32 du Code de procédure pénale qui autorise les actes suivants :

> *« 1° Acquérir des produits stupéfiants ;*
>
> *« 2° En vue de l'acquisition de produits stupéfiants, mettre à la disposition des personnes se livrant à ces infractions des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication. »*

Les OPJ et APJ qui doivent nécessairement avoir l'autorisation d'un magistrat, peuvent commettre ces actes sans être pénalement responsables. Ils peuvent ainsi se faire passer pour des clients potentiels ou des facilitateurs du trafic par fourniture de moyens.

Comme tout mode de recueil de la preuve, le coup d'achat est soumis au principe de loyauté et la prohibition de la provocation à l'infraction, sous peine de faire encourir la nullité de la procédure.

Près de dix ans plus tard, la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, a étendu le coup d'achat aux délits en matière d'armes et de produits explosifs définis par l'article 706-73, 12° du Code de procédure pénale [15], que cette même loi a modifié dans son article 25 pour supprimer en particulier la condition de bande organisée.

Les **articles 25** et **127** de cette loi autorisent ainsi la technique particulière d'enquête du « **coup d'achat** » pour caractériser les infractions liées aux armes relevant du champ de la délinquance organisée, au bénéfice des **forces de l'ordre** (art. 25) et des **agents des douanes** (art. 27).

Seul diffère dans l'article 706-106 du Code de procédure pénale, par rapport à l'article 706-32 du Code de procédure pénale, l'ajout du dernier paragraphe :

> *« A peine de nullité, l'autorisation du procureur de la République ou du juge d'instruction, qui peut être donnée par tout moyen, est mentionnée ou versée au dossier de la procédure et les actes autorisés ne peuvent constituer une incitation à commettre une infraction. »*

Recommandation n°7 :

Pour faire suite à la recommandation n°3 relative aux acquisitions de contenus, autoriser les coups d'achat pour l'ensemble des dispositions autorisant les enquêtes sous pseudonyme relatives à la fourniture de produits ou de services en ligne.

2.5 Notion de patrouille numérique et veille policière

La « veille » sur Internet est une simple surveillance exercée par les services d'enquête dans les espaces ouverts au public, qui ne nécessite pas d'autorisation légale autre que celle qui résulte des articles 12 et 41 du Code de procédure pénale. Cette veille consiste en une surveillance active des réseaux (site web, forum de discussions, réseaux sociaux, Darknet…) en procédant à toute vérification utile ainsi qu'à la localisation de serveurs. Elle s'effectue sans moyen d'investigation particulier autres que le recours à un accès Internet ainsi qu'à des moteurs de recherche. Au regard de son pouvoir de constatation des infractions, tout agent ou officier de police judiciaire peut se rendre sur les sites ouverts au public pour constater une infraction et initier des enquêtes judiciaires.

Pour effectuer cette veille, les officiers et agents ou de police judiciaire[16] se connectent soit avec le profil de leur service, soit avec des faux comptes ou pseudonymes créés pour l'occasion. Ils effectuent alors une surveillance dans le cyberespace en pratiquant des patrouilles numériques. Toutefois, la possibilité d'user d'une identité d'emprunt est clairement pertinente et même incontournable dans certains cas pour identifier un suspect potentiel utilisant des moyens d'anonymisation, pour accéder aux réseaux sociaux, à des forums de discussions et à des blogs.

[15] Délits en matière d'armes et de produits explosifs prévus aux articles 222-52 à 222-54, 222-56 à 222-59, 322-6-1 et 322-11-1 du Code pénal, aux articles L. 2339-2, L. 2339-3, L. 2339-10, L. 2341-4, L. 2353-4 et L. 2353-5 du Code de la défense ainsi qu'aux articles L. 317-2 et L. 317-7 du Code de la sécurité intérieure.

[16] Comme les douaniers, les agents de la Direction générale de la concurrence, de la consommation et de la répression des fraudes, ou encore ceux de l'Autorité de régulation des jeux en ligne…

Dans le cadre du rapport Robert sur la cybercriminalité de février 2014[17], il a été souligné que la veille policière était une pratique courante et utile mais qu'elle était fragilisée au regard de cette question de l'usage d'un pseudonyme.

En effet, les articles cités dans la section précédente sur l'enquête sous pseudonyme paraissent, dans leur rédaction, soumettre, aux mêmes conditions, l'usage d'un pseudonyme qu'il soit ou non accompagné d'investigations. En liant ainsi le recours à un pseudonyme avec la prise de contact et l'acquisition d'éléments de preuve, la veille est limitée à quelques agents spécialisés et un champ infractionnel limité, alors même que, par nature, la surveillance doit revêtir une portée générale et ne requiert pas un encadrement normatif[18] au sens des alinéas 2 des articles 8 et 10 de la Convention européenne des droits de l'homme, car elle ne saurait être assimilée à une ingérence dans le droit au respect de la vie privée des personnes ou dans la liberté d'expression.

Aussi, conscient de la nécessité de lever les interrogations existantes, la recommandation n°46 du rapport concluait qu'il fallait ***« autoriser de manière générale, le simple usage d'un pseudonyme sur Internet par les officiers et agents de police judiciaire, lorsqu'ils ne s'accompagnent pas d'investigations particulières ».*** Le cas échéant, il ne s'agit alors plus de simples patrouilles numériques mais bien d'enquêtes sous pseudonyme, notamment dans le cadre de contacts avec un suspect.

Recommandation n°8 :

Autoriser l'usage d'un pseudonyme pour les patrouilles numériques de surveillance dans le cyberespace (disposition qui pourrait éventuellement être placée dans le Code de la sécurité intérieure).

[17] http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
[18] JurisClasseur Fasc.1110 : infiltrations numériques - Myriam Quemener - 4 février 2015

3 Accès à la preuve numérique

3.1 Données stockées

3.1.1 Définition des catégories de données

La notion de preuve numérique recouvre différents types de données auxquelles les autorités sont susceptibles de solliciter l'accès dans le cadre des enquêtes qu'elles conduisent. Après avoir exposé les définitions actuellement prévues par les textes, il faut s'intéresser à la notion de « *métadonnées* » et à la définition en cours de discussion au niveau européen.

3.1.1.1 Typologies des catégories de données :

a) Les données relatives au contenu

En droit français, les données relatives au contenu sont définies par référence au principe de confidentialité des correspondances qui s'applique aux courriers électroniques.

En application de l'article L32-3 du Code des communications électroniques et des postes, la confidentialité couvre le contenu de la communication, l'identité des correspondants, l'intitulé du message et les documents joints à la communication.

Les données de contenu ne sont pas définies par la Convention de Budapest sur la Cybercriminalité mais désignent, selon le Rapport explicatif, « *le contenu informatif de la communication, à savoir le sens de la communication ou le message ou l'information transmis par la communication (autre que les données relatives au trafic)* ».

b) Les données informatiques

Bien que plusieurs dispositions fassent référence à la notion de « *données informatiques* », aucune définition n'est fournie par le droit français.

Généralement, la notion de « *données informatiques* » renvoie aux données stockées et/ou accessibles via un système d'information. Il est donc utile de se référer à la définition insérée dans la Convention de Budapest : « *toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction* ».

c) Les données relatives au trafic

Ce type de données est défini par le droit français applicable aux réseaux de communications électroniques et aux services de communication au public comme étant « *toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou en vue de sa facturation* ». Elles « *s'entendent des informations rendues disponibles par les procédés de communication électronique, susceptibles d'être enregistrées par l'opérateur à l'occasion des communications électroniques dont il assure la transmission et qui sont pertinentes au regard des finalités poursuivies par la loi* ».

La directive vie privée et communications électroniques ou *E-privacy* repose sur la même définition mais précise en son considérant 15 que « *les données relatives au trafic peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau* ».

La Convention de Budapest quant à elle donne la définition suivante : « *toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type du service sous-jacent* ».

d) Les données de connexion

En droit français, la définition de ce type de données résulte des règles juridiques applicables aux hébergeurs, d'une part, et aux prestataires de services de communication au public, d'autre part. Elles comprennent (i) les données techniques (par exemple, les données d'identification, le mode technique de communication) et (ii) les informations relatives à l'abonné (par exemple, l'identifiant de connexion).

Une telle définition peut être comparée à celle donnée par la Convention de Budapest, qui définit les « *informations relatives aux abonnés » comme « toute information, contenue sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de service et qui se rapporte aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir: a) le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ; b) l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de service ; c) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de service*. »

La directive *E-privacy* emploie quant à elle la notion de « *données de localisation* » définies comme : « *toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ». Le considérant 14 précise que cette notion couvre notamment : « la latitude, la longitude et l'altitude du lieu où se trouve l'équipement terminal de l'utilisateur, la direction du mouvement, le degré de précision quant aux informations sur la localisation, l'identification de la cellule du réseau où se situe, à un moment donné, l'équipement terminal, ou encore le moment auquel l'information sur la localisation a été enregistrée* ».

3.1.1.2 Vers une définition de la notion de « métadonnées ».

Dans le cadre de l'affaire Tele2[19], la Cour de justice de l'Union européenne (CJUE) a eu à connaître de la nature des métadonnées. Ainsi, elle relève que ce type de données « *permettent de retrouver et d'identifier la source d'une communication et la destination de celle-ci, de déterminer la date, l'heure,*

[19] Arrêt de la Cour de justice de l'Union européenne dans les affaires jointes C-203/15 Tele2 Sverige AB c. Post- och telestyrelsen et C-698/15 Secretary of State for the Home Department c. Tom Watson et autres, 21 décembre 2016

la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que de localiser le matériel de communication mobile. Au nombre de ces données figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, en particulier, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée ».

Il est intéressant de noter que pour la CJUE ces données sont tout aussi sensibles que le contenu même d'une correspondance privée. Elle relève que les métadonnées fournissent *« les moyens d'établir (…) le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications* ».

Sur un plan législatif, il faut relever qu'une définition des métadonnées est actuellement en cours de discussion dans le cadre de l'examen de la proposition de règlement vie privée et communications électroniques ou *E-privacy* (qui a pour vocation de remplacer la directive e-privacy). Le texte proposé par la Commission prévoit que les *« métadonnées de communications électroniques* » correspondent aux « *données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication* ».

Ainsi définies, les métadonnées se distingueraient du « *contenu de communications électroniques* » décrit comme « *le contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son ». « Métadonnées » et « contenu* » feraient partie de l'ensemble plus large constitué par les données de communications électroniques.

3.1.2 Conservation des données

Le débat sur la conservation des données par les différents opérateurs et prestataires de services de communication électronique continue d'être d'actualité. Ainsi par deux décisions successives, la Cour de Justice de l'Union européenne a fragilisé les dispositions existantes :

- Le 8 avril 2014, en invalidant la directive 2006/24/CE du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication ;
- Le 21 décembre 2016, dans l'arrêt conjoint évoqué plus haut, les législations de la Suède et du Royaume-Uni ont été épinglées, précisant que le droit de l'Union s'oppose à une règlementation nationale prévoyant une obligation de conservation des données généralisée et indifférenciée au motif que ceci crée une ingérence très importante dans la vie privée des individus dont les données sont conservées.

En revanche, dans cette dernière décision, la Cour de Justice de l'Union européenne a estimé que le droit de l'Union européenne ne s'opposait pas à une règlementation nationale imposant une conservation ciblée des données pour lutter contre la *« criminalité grave* » sous certaines conditions :

- limiter clairement et précisément, « au strict nécessaire » les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation et offrir des garanties suffisantes à cet égard ;
- se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé aux autorités nationales compétentes ;
- respecter les droits fondamentaux que sont le respect de la vie privée et la protection des données à caractère personnel ;
- soumettre l'accès aux données à certains garde-fous (notamment : un contrôle préalable par une autorité indépendante) ;
- conserver les données sur le territoire de l'Union européenne.

En France et dans d'autres pays européens, la législation sur la conservation des données n'a pas pour fondement la directive de 2006, mais la question se pose de sa conformité avec les conclusions de la CJUE en 2016. Des travaux sont actuellement menés par la Commission européenne, à la demande du Conseil de l'Union européenne[20] pour faire des propositions dans le contexte de l'évolution à venir en 2018 de la directive e-Privacy.

3.1.3 Réquisitions

Au regard de l'importance que prennent les données au sein du monde numérique d'aujourd'hui, leur accès ne peut se faire que de manière encadrée par l'utilisation d'une réquisition. Le Code de procédure pénale encadre les réquisitions visant les données stockées via les articles 60-1, 77-1-1 ainsi que 99-3 du Code de procédure pénales. La réquisition est ainsi bien définie par l'article 77-1-1 du Code de procédure pénale (enquête préliminaire) :

> *« Le procureur de la République ou, sur autorisation de celui-ci, l'officier de police judiciaire, peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces documents, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel ».*

Ces articles permettent aux autorités publiques de **requérir**, de **toute personne**, de **tout établissement** ou **organisme privé ou public** ou de **toute administration publique**, sous certaines conditions et dans le cadre de leurs missions, des données stockées sans en informer préalablement le ou les titulaires de ces données.

Cette réquisition ne peut être effectuée que sur demande ponctuelle, écrite et motivée, visant des personnes nommément désignées, identifiées directement ou indirectement, ou d'autres ressources numériques.

A l'exception des métiers présentant une sensibilité identifiée par la loi (avocats, organismes de presse, parlementaires, etc.) mentionnés aux articles 56-1 à 56-5 du Code de procédure pénale, le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de 3 750 euros.

[20] http://www.consilium.europa.eu/fr/meetings/jha/2017/06/08-09/ Conseil "Justice et affaires intérieures", 08-09/06/2017, Justice pénale dans le cyberespace

On notera les progrès réalisés au cours des années récentes avec la mise en place de différentes initiatives renforçant l'efficacité et la transparence de ces procédures :

- En France, les enquêteurs et magistrats peuvent dorénavant recourir aux infrastructures mises en œuvre par l'agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ) pour servir d'interface avec les grands opérateurs de communications électroniques français ;
- Les services d'enquête français ont mis en place des guichets uniques, médiateurs chargés de faciliter les relations avec les opérateurs ;
- Enfin, sur le plan international, de nombreux prestataires de services de communication électronique mettent à disposition des interfaces automatisées pour assurer la réception des demandes officielles et publient des rapports de transparence.

3.2 Gel de données

La convention du Conseil de l'Europe n°185, signée à Budapest le 23 novembre 2001, et son protocole additionnel, fait à Strasbourg le 28 janvier 2003, est le premier traité international sur les infractions commises via Internet, traitant en particulier des infractions au droit d'auteur, de la fraude informatique, de la pornographie mettant en scène des enfants ainsi que des infractions liées à la sécurité des réseaux.

Elle contient également une série de pouvoirs et de procédures tels que le gel de données, la perquisition de réseaux informatiques et l'interception. Son préambule énonce poursuivre « *une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale* ».

Le gel de données est ainsi bien défini par l'article 16 de la Convention de Budapest qui dispose :

> *« 1. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.*
>
> *« 2. Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et protéger l'intégrité desdits données pendant une durée aussi longue que nécessaire, jusqu'à maximum 90 jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite. »*

L'Article 60-2 du Code de procédure pénale permet une mise en application concrète de cette convention :

> *« […] L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant*

excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

« Les organismes ou personnes visés au présent article mettent à disposition les informations requises par voie télématique ou informatique dans les meilleurs délais. Le fait de refuser de répondre sans motif légitime à ces réquisitions est puni d'une amende de 3 750 Euros. Les personnes morales peuvent être déclarées responsables pénalement dans les conditions prévues par l'article 121-2 du Code pénal de l'infraction prévue au présent alinéa. La peine encourue par les personnes morales est l'amende, suivant les modalités prévues par l'article 131-38 du Code pénal.

« Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les catégories d'organismes visés au premier alinéa ainsi que les modalités d'interrogation, de transmission et de traitement des informations requises ».

Le fait de s'abstenir de répondre sans motif légitime dans les meilleurs délais à cette réquisition est puni d'une amende de 3 750 euros.

On note toutefois des différences entre les termes utilisés dans la convention et ceux du Code de procédure pénale (« *données électroniques spécifiées, y compris celles relatives au trafic* », d'une part et « *contenu des informations consultées* », d'autre part). En outre cela n'est applicable que si une enquête judiciaire a été préalablement ouverte en France.

Recommandation n°9 – Améliorer la transposition du gel de données tel que prévu par la Convention de Budapest

Aligner les dispositions de l'article 60-2 alinéa 2 du Code de procédure pénale avec celles prévues par l'article 16 de la Convention de Budapest du Conseil de l'Europe, notamment s'agissant des données visées. Par ailleurs, ce gel de données (ou préservation) doit pouvoir être ordonné sans qu'il soit besoin d'ouvrir une enquête judiciaire.

3.3 Perquisitions et constatations

Les perquisitions sont les opérations réalisées dans des lieux privés en vue de procéder à la recherche d'éléments matériels de preuve. Des constatations et donc la recherche de traces et d'indices peuvent aussi être réalisées sur les lieux de la commission d'une infraction. Naturellement, des éléments de preuve informatiques ont pu être recueillis dès qu'ils ont été rencontrés dans l'histoire judiciaire, mais des dispositions spécifiques ont été progressivement introduites.

3.3.1 Dispositions spécifiques

Ainsi, l'article 56 (ainsi que les articles 76 et 97) du Code de procédure pénale prévoit explicitement la possibilité de saisir des données informatiques ou une copie physique de ces données, réalisée en la présence des personnes qui assistent à la perquisition. Egalement, il peut être prescrit la destruction sur leur support original non saisi des données dont l'usage ou la détention sont illégaux.

Le placement sous-main de justice est matérialisé par la réalisation d'un scellé.

Recommandation n°10 : Les articles sur la perquisition pourraient prévoir la possibilité de réaliser des scellés numériques protégeant de façon vérifiable l'intégrité des données mais permettant la lecture et le transfert ultérieur par voie électronique (pour analyses par un expert ou un technicien par exemple).

Enfin, le Code de procédure pénale détaille les mesures particulières mises en œuvre dans des lieux sensibles tels que le cabinet d'un médecin, d'un avocat ou d'un organisme de presse.

Recommandation n°11 : Les articles sur la perquisition dans les lieux sensibles pourraient prévoir des mesures spécifiques adaptées à la saisie de données numériques : autoriser la copie de données (là où les textes actuels visent toujours uniquement les documents ou objets), préciser le rôle des experts ou personnes requises qui assistent les enquêteurs ou les magistrats au cours de la perquisition (notamment sur leur droit à visualiser pendant la perquisition l'ensemble des données afin de réaliser le tri des données qui peuvent être saisies) et prévoir la possibilité de réaliser des accès à distance à des données depuis ces lieux (voir section suivante).

3.3.2 Accès à distance

L'action dans l'espace numérique suppose la possibilité de stocker et d'accéder à des données à distance, dans le même bâtiment, la même ville, dans le même pays ou dans un autre pays. Aussi, depuis l'avènement de la convention du Conseil de l'Europe sur la cybercriminalité, plusieurs dispositions ont été introduites pour permettre l'accès à ces données dans le cadre des enquêtes judiciaires.

3.3.2.1 Perquisitions à distance

Ainsi, l'article 57-1 (ainsi que les articles 76-3 et 97-1) du Code de procédure pénale autorise deux types d'accès à distance :

- Au cours de la perquisition, à des données accessibles depuis un système se trouvant sur les lieux de la perquisition ou disponibles pour ce système ;

- Ultérieurement, depuis un service d'enquête judiciaire, dans les mêmes conditions.

Si les données sont stockées en dehors du territoire national, la saisie doit être réalisée dans le respect des conventions internationales. En particulier, l'article 32 b) de la convention du Conseil de l'Europe sur la cybercriminalité prévoit la nécessité d'obtenir le *« consentement légal et volontaire de la personne autorisée à divulguer ces données* ».

Recommandation n°12 : Etant donné le volume des données considéré, il pourrait être envisagé d'autoriser le placement sous scellé numérique de données stockées dans des infrastructures d'informatique en nuage, plutôt que leur rapatriement traditionnel sur un support utilisé par les enquêteurs.

3.3.2.2 Accès à distance aux courriers électroniques stockés

Le contexte de interceptions judiciaires introduit une notion complémentaire liée à l'accès à distance à des données stockées au travers de la possibilité offerte, dans le cadre des enquêtes sur certaines infractions de criminalité organisée, par l'article 706-95-1 du Code de procédure pénale l'accès « *à*

distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique ».

Recommandation n°13 : Cette disposition pourrait être étendue à d'autres données personnelles qui ne relèvent pas de la correspondance privée et associées à un identifiant informatique, telles que celles qui sont placées dans des espaces de stockage en ligne. Enfin, en vue d'éviter une trop forte asymétrie avec le régime des interceptions, elle pourrait aussi être étendue à d'autres crimes et délits graves que ceux visés aux articles 706-73 et 706-73-1 du Code de procédure pénale.

3.4 Analyses techniques et expertises

Les analyses techniques et les expertises judiciaires sont réalisées dans le domaine numérique dans les mêmes conditions que celles qui prévalent dans tous les domaines de preuve. Toutefois, les experts ou techniciens sont beaucoup plus souvent amenés à intervenir dès le moment de la découverte et de la saisie des données, et sont parfois amenés à réaliser des opérations techniques (notamment de tri) sur les lieux des constatations ou de la perquisition.

C'est l'article 60 du Code de procédure pénale qui prévoit les réquisitions aux personnes qualifiées (aux fins de procéder à des constatations ou à des examens techniques ou scientifiques). Ce même article renvoie aux formes de l'expertise judiciaire pour la réalisation des rapports remis aux enquêteurs ou aux magistrats.

Recommandation n°14 : En vue de faciliter l'appui technique au cours des perquisitions aux enquêteurs – y compris spécialisés – qui les réalisent, on pourrait prévoir la possibilité pour un sachant dans un domaine particulier d'être requis pour assister à distance aux opérations techniques et guider les enquêteurs ou les techniciens.

Cela pourrait être particulièrement utile pour des perquisitions réalisées dans un environnement complexe (entreprise, hébergeurs), outre-mer ou encore dans des lieux dont les conditions physiques d'accès sont restreintes (danger chimique, biologique ou nucléaire). Cela aurait évidemment l'intérêt de multiplier la capacité d'assistance des experts en question.

3.5 Interception

Autre mode de collecte de preuves numériques, l'interception de correspondances a été formalisée dans le droit français par la loi de 1991 relative au secret des correspondances émises par la voie des communications électroniques, aussi bien dans le champ judiciaire que dans celui du renseignement. Il est régi par les articles 100 et suivants du Code de procédure pénale qui permettent « *l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques ». Cette dernière formulation est issue d'une clarification apportée par la loi n°2016-731 du 3 juin 2016 ; auparavant le texte visait de façon peut-être plus restrictive les « correspondances émises par la voie des télécommunications* ».

C'est ce même texte qui est utilisé aussi bien pour les interceptions de communications téléphoniques que pour des échanges réalisés par Internet.

Recommandation n°15 : Alors même que la plateforme nationale des interceptions judiciaires n'est pas soumise à l'obligation de réaliser des scellés dits fermés, les enregistrements d'interceptions sont de façon générale soumis à l'obligation de réaliser des scellés fermés (article 100-4 du Code de procédure pénale). Il pourrait être offert l'option de remplacer le scellé fermé par un scellement numérique, tel qu'évoqué dans la recommandation n°10 plus haut.

Recommandation n°16 : En outre, l'article 100-5 du Code de procédure pénale prescrit la retranscription des correspondances. Cette notion pourrait être étendue à la possibilité de retranscrire la nature technique des échanges (visite d'un site Web, établissement d'une connexion sur un réseau de communication, etc.) de façon à couvrir plus spécifiquement les interceptions réalisées sur une connexion Internet.

3.5.1 Cas spécifique de l'interception de flux réseaux

Lors des enquêtes réalisées dans le champ de la cybercriminalité, il est souvent nécessaire de pouvoir retracer l'origine ou la destination des connexions à un serveur informatique, par exemple pour faciliter la localisation ou l'identification d'une personne maîtrisant le système de commande et de contrôle d'un botnet ou des personnes qui en sont les victimes.

Recommandation n°17 : Sans qu'il soit nécessaire de procéder à l'interception de l'intégralité des échanges, le Code de procédure pénale pourrait prévoir la possibilité d'enregistrer uniquement les flux réseaux (parfois appelés *netflows*) contenant les adresses IP d'origine et de destination des connexions, le volume et la nature des données échangées – en particulier au travers du port de communication utilisé.

3.6 Géolocalisation

3.6.1 Rappel : Définition – Terminologie

Au sens large, la géolocalisation est une technique de détermination de la situation géographique à un instant donné d'un lieu, d'une personne, d'un véhicule, d'un objet.

Il convient toutefois de distinguer deux catégories de géolocalisation que les enquêteurs peuvent être amenés à réaliser dans le cadre d'une enquête ou d'une information judiciaire :

- **La géolocalisation en temps réel** qui consiste à suivre à tout moment les déplacements d'un objet et le cas échéant, de la personne qui le détient. Cette technique permet aux enquêteurs un suivi dynamique d'un objet ou de son possesseur et ce, sans prendre le risque d'être repéré par des délinquants. En pratique, deux techniques de géolocalisation en temps réel sont utilisées :
    - Le suivi dynamique de télécommunications ;
    - Le dispositif dédié à la géolocalisation (balise) placé sur un moyen de transport ou tout objet.

- **La géolocalisation en temps différé** qui consiste pour les enquêteurs à déterminer les déplacements d'un objet et de son possesseur plusieurs jours ou mois après qu'ils aient eu lieu. A cette fin, les enquêteurs sollicitent la transmission de données conservées notamment par les opérateurs de communications électroniques ou par toute personne ou tout organisme public ou privé permettant de retracer lesdits déplacements. Ce procédé permet notamment de recueillir des éléments permettant d'établir ou d'exclure la présence du possesseur d'un objet à proximité du lieu de commission de l'infraction.

Les juges distinguent la géolocalisation « *en temps différé* » de la géolocalisation « *en temps réel* » par son caractère moins attentatoire à la vie privée. Ainsi, la chambre criminelle de la Cour de cassation rattache la géolocalisation en différé à des textes généraux :

- l'article 60-1 du Code de procédure pénale lors d'une enquête de flagrance,
- l'article 77-1-1 du Code de procédure pénale qui règlemente les réquisitions aux fins de communication dans le cadre de l'enquête préliminaire et
- l'article 81 du Code de procédure pénale concernant les actes d'information jugés utiles pour la manifestation de la vérité auquel peut se livrer le juge d'instruction.

Les dispositions spécifiques introduites par la loi du 28 mars 2014 ne lui sont pas applicables, comme l'a d'ailleurs rappelé la chambre criminelle de la Cour de cassation dans un arrêt du 2 novembre 2016[21].

Compte tenu des développements nombreux entourant la géolocalisation en temps réel et du caractère attentatoire à la vie privée de cette technique d'investigation, les débats ci-après se concentreront sur cette technique.

3.6.2 La géolocalisation en temps réel avant la loi du 28 mars 2014 relative à la géolocalisation

Avant la loi du 28 mars 2014, le législateur n'avait pas spécifiquement encadré cette technique spéciale d'investigation. Ainsi, une pratique judiciaire s'était développée sur la base des textes généraux relatifs aux réquisitions (cf. supra).

Cette pratique a toutefois donné lieu à plusieurs décisions de jurisprudence importantes en la matière :

- **Par un arrêt du 2 septembre 2010[22]**, la Cour européenne des droits de l'homme (CEDH) a considéré que la surveillance par GPS d'une personne soupçonnée de terrorisme n'était pas contraire au droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme en posant des critères précis de validité de ce dispositif (proportionnalité aux buts légitimes poursuivis et nécessité dans une société démocratique). La condamnation de la France pouvait être ainsi crainte, le législateur n'ayant pas encadré à cette époque cette technique d'investigation.

- **Par un arrêt du 22 novembre 2011[23],** la chambre criminelle de la Cour de cassation a validé le recours par un juge d'instruction la pose d'une balise permettant de suivre et relever les déplacements d'un véhicule en se fondant sur l'article 81 du Code de procédure pénale et ce, au motif que cette surveillance avait été effectuée sous le contrôle d'un juge, ce qui constituait

[21] Cass. Crim. 2 nov. 2016, n°16-82.376
[22] CEDH, 2 sept. 2010, n°35623/05, Uzun c/Allemagne
[23] Cass. Crim., 22 nov. 2011, n°11-84.308

une garantie suffisante contre l'arbitraire et que cette mesure était proportionnée au but poursuivi. La Cour ne s'était toutefois pas penchée sur la licéité des opérations en temps réel réalisé par le Parquet.

- La Cour de cassation se prononce sur ce point par **deux arrêts en date du 22 octobre 2013**[24] et considère que la technique de géolocalisation constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge. Implicitement, la chambre criminelle exclut la compétence du procureur de la République pour la géolocalisation en temps réel.

L'ensemble de ces arrêts mettaient en évidence la nécessité de légiférer sur la question.

3.6.3 La géolocalisation appréhendée par la loi du 28 mars 2014

La loi n°2014-372 du 28 mars 2014 introduit ainsi des dispositions spécifiques sur la géolocalisation en temps réel aux articles 230-32 à 230-44 du Code de procédure pénale, la géolocalisation en temps différé continuant de relever des textes généraux sur les réquisitions.

La loi établit les infractions permettant de recourir à la géolocalisation et détermine les autorités compétentes pour autoriser une telle opération ainsi que la durée de ces autorisations.

Le recours à la géolocalisation en temps réel est désormais possible en cas d'investigations pour :

(i) les délits contre les personnes punis d'une peine d'emprisonnement supérieure ou égale à 3 ans,
(ii) les autres crimes et délits punis d'au moins 5 ans d'emprisonnement,
(iii) les enquêtes ou information judiciaire en recherche des causes de la mort, des causes de la disparition et enquêtes en recherche d'une personne en fuite.

Dans le cadre de l'enquête de police (flagrance ou préliminaire), le législateur est allé au-delà de la jurisprudence en autorisant le recours par le procureur de la République à un tel procédé pour une durée maximale de quinze jours consécutifs. A l'issue de ce délai, cette opération est autorisée par le juge des libertés et de la détention (JLD) pour une durée maximale d'un mois renouvelable. Au cours de l'instruction, elle est autorisée par le juge d'instruction, pour une durée de quatre mois renouvelable.

Le législateur est également venu encadrer les hypothèses d'introduction dans un lieu privé (professionnel ou d'habitation) afin d'installer un dispositif de géolocalisation. Le JLD et le juge d'instruction sont les seuls à pouvoir autoriser cette opération et ce, toutefois à la condition que l'infraction soit passible d'une peine d'au moins 5 ans d'emprisonnement.

Récemment, la loi n°2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme autorise également le procureur à recourir aux mesures de géolocalisation pour 48 heures à compter de l'ouverture d'une information judiciaire par un juge d'instruction désigné.

Certains lieux bénéficient d'une protection absolue (on ne peut y pénétrer à l'insu et sans le consentement du propriétaire ou de l'occupant) : cabinet d'un avocat ou son domicile, locaux d'une entreprise de presse, domicile d'un journaliste, domicile d'un magistrat, cabinet d'un médecin d'un

[24] Cass. Crim., 22 oct. 2013, n°13-81.945 et n°13-81.949

notaire ou d'un huissier, d'un député, d'un sénateur ou d'un magistrat, les lieux abritant des éléments couverts par le secret de la défense nationale.

Il existe par ailleurs des exceptions à l'autorisation de procéder à la géolocalisation. Ainsi, le législateur a prévu en cas d'urgence (risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens) que le dispositif de géolocalisation pouvait être mis en place par un OPJ. Toutefois, afin d'assurer un minimum de sécurité juridique, le magistrat, informé immédiatement, peut ordonner la mainlevée de la mesure. La chambre criminelle de la Cour de cassation est très sévère s'agissant de la notification sans délai au magistrat de cette mesure mise en place en urgence[25].

De même, l'intervention du magistrat n'est pas nécessaire pour permettre la location d'un téléphone portable ou d'un véhicule de la victime de l'infraction sur laquelle porte l'enquête ou la personne disparue, dès lors que l'opération a pour objet de retrouver la victime, l'objet qui lui a été dérobé ou la personne disparue et que la mesure est prise dans l'intérêt de cette dernière.

Enfin, le législateur précise que la mesure concerne le territoire national. La circulaire publiée par la direction des affaires criminelles et des grâces du ministère de la justice le 1er avril 2014 préconise le recours à une demande d'entraide pénale internationale quand il s'avère nécessaire de mettre en œuvre ou de poursuivre une géolocalisation hors du territoire national.

Recommandation n°18 : Il est proposé de supprimer la notion de « *véhicule* » de l'article 230-32 du Code de procédure pénale pour la remplacer par une notion plus large qui dépasse le seul rapport terrestre. Ainsi, il pourrait être fait référence à la notion générale de *« moyens de déplacement et de transport »* ou aux *« véhicules terrestres, navires, aéronefs, embarcations, engins pilotés, télépilotés ou autonomes ».*

3.7 Chiffrement

Les moyens techniques à disposition pour chiffrer des contenus sont à la fois utiles pour préserver des informations de nature particulièrement sensibles (obligation de confidentialité, secret professionnel, secret défense) mais peuvent également constituer des obstacles pour les enquêteurs dans le cadre de leurs investigations pour la manifestation de la vérité quand ces mêmes moyens sont utilisés par les cyberdélinquants.

Ainsi les services d'investigations américains (FBI) ont pu avoir recours aux services d'une entreprise spécialisée ou d'experts techniques indépendants pour avoir accès à des données présentes sur un iPhone alors qu'Apple avait refusé de coopérer en communiquant des données relatives à la vie privée.

Dans un jugement rendu le 30 septembre 2017, la Justice américaine a tranché en considérant que le FBI n'a pas à communiquer les méthodes utilisées, ni le prix de l'acte qui ont conduit à extraire les données du smartphone d'Apple (un 5c). Obliger le FBI à fournir de telles informations pourrait conduire à des mesures de rétorsions populaires à l'encontre de la ou des société(s) ou du/des individu(s) qui sont parvenus à pirater ledit smartphone, voire permettre à des individus mal intentionnés de parfaire leurs méthodes et ainsi rendre le travail du FBI encore plus compliqué en cas de futures affaires similaires.

[25] Cass. Crim. 17 nov. 2015, n°15-84.025P

3.7.1 Rappel sémantique et définitions

De nombreuses sources viennent rappeler les définitions utiles pour comprendre les problématiques du chiffrement. Reprenons les définitions[26] qui font consensus et correspondent à la réalité scientifique :

- Le **chiffrement** est le procédé avec lequel on rend la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement. Concrètement, lorsqu'on chiffre un document, on transforme à l'aide de la clé de chiffrement un message en clair en un message incompréhensible (dit texte chiffré) pour celui qui ne dispose pas de la clé de déchiffrement (en anglais *encryption*).

- Le **déchiffrement** est logiquement l'opération inverse du chiffrement. C'est donc le processus transformant le texte chiffré en texte clair. Concrètement, cela consiste à retrouver le message original d'un texte chiffré dont on possède la clé de déchiffrement (en anglais *decryption*).

- Le **décryptage** consiste à retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement. On parlera aussi de cassage. Corollairement les termes crypter et cryptage sont impropres et ne doivent pas être utilisés.

3.7.2 Mise au clair des données chiffrées nécessaires à la manifestation de la vérité (articles 230-1 et suivants du Code de procédure pénale)

Dans ce contexte linguistique dans lequel chaque terme recouvre un sens, le législateur a préféré choisir la notion de *mise au clair des données chiffrées nécessaires à la manifestation de la vérité*. Il apparaît que cette notion de mise au clair est assez large pour viser à la fois les opérations de déchiffrement ou de cassage si nécessaire.

Ainsi l'article 230-1 du Code de procédure pénale disque que :

> *« Sans préjudice des dispositions des articles 60, 77-1 et 156, lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire.*
>
> *« Si la personne ainsi désignée est une personne morale, son représentant légal soumet à l'agrément du procureur de la République, de l'officier de police judiciaire ou de la juridiction saisie de l'affaire le nom de la ou des personnes physiques qui, au sein de celle-ci et en son nom, effectueront les opérations techniques mentionnées au premier alinéa. Sauf si elles sont inscrites sur une liste prévue à l'article 157, les personnes ainsi désignées prêtent, par écrit, le serment prévu au deuxième alinéa de l'article 60 et à l'article 160.*
>
> *« Si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction*

[26] http://www.ryfe.fr/2011/08/les-mots-crypter-et-cryptage-n%E2%80%99existent-pas/ (CC BY SA)

d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au présent chapitre ».

Par ailleurs, l'article 230-2 du Code de procédure pénale vient préciser que

« Lorsque le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire décident d'avoir recours, pour les opérations mentionnées à l'article 230-1, aux moyens de l'Etat couverts par le secret de la défense nationale, la réquisition écrite doit être adressée au service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information, avec le support physique contenant les données à mettre au clair ou une copie de celui-ci. Cette réquisition fixe le délai dans lequel les opérations de mise au clair doivent être réalisées. Le délai peut être prorogé dans les mêmes conditions de forme. À tout moment, l'autorité judiciaire requérante peut ordonner l'interruption des opérations prescrites.

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

« Les données protégées au titre du secret de la défense nationale ne peuvent être communiquées que dans les conditions prévues aux articles L. 2312-4 à L. 2312-8 du code de la défense.

« Lorsqu'il s'agit de données obtenues dans le cadre d'interceptions de communications électroniques, au sein du traitement mentionné à l'article 230-45, la réquisition est adressée directement à l'organisme technique désigné en application du premier alinéa du présent article ».

La question se pose de savoir si, en vue de la mise au clair et en l'absence de coopération de l'opérateur mobile ou fournisseur d'accès Internet, il est permis afin d'accéder à l'intégralité des messageries chiffrées non seulement d'avoir recours à des techniciens mais également à des personnes qui pourraient être qualifiées de « hackers » car détenant des technologies non encore mises à la disposition des enquêteurs (cf. FBI aux Etats-Unis).

Ainsi les dispositions légales prévoient la possibilité d'une expertise (article 156 du Code de procédure pénale) ou le recours en vue des constatations ou de la réalisation des examens techniques ou scientifiques par le procureur de la République ou l'officier de police judiciaire sur autorisation de ce dernier à toutes personnes qualifiées (article 77-1 du Code de procédure pénale).

Recommandation n°19 : Le texte apparaît assez large pour considérer qu'en cas de nécessité et en l'absence d'autres choix, le recours à des experts / techniciens au sens large pourrait être envisagé dans le respect de la vie privée et que pour les besoins de l'enquête pour des faits spécialement graves.

Une actualité récente permet également de souligner le caractère sensible de cette question. En effet, le 10 janvier 2018, par décision de la Cour de cassation (arrêt n°3478), le Conseil constitutionnel a été saisi d'une question prioritaire de constitutionnalité sur l'application de l'article 434-15-2 du Code

pénal (introduit par la loi du 16 novembre 2001 et modifiée 3 juin 2016 pour augmenter le quantum de l'amende) qui prévoit que :

> *« Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du Code de procédure pénale*
>
> *« 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 ».*

Il est en effet reproché à cette disposition de ne pas permettre au mis en cause de faire usage de son droit au silence, ni de son droit de ne pas s'auto-incriminer. En ce sens elle serait susceptible d'être contraire au principe du droit au procès équitable prévu par l'article 16 de la Déclaration des Droits de l'homme été du Citoyen du 26 août 1789, au principe de présomption d'innocence, duquel découle le droit de ne pas s'auto-incriminer et le droit de se taire, prévu à l'article 9 de la Déclaration des Droits de l'homme été du Citoyen du 26 août 1789.

Sans préjuger de l'issue de cette procédure, si cette action devait aboutir à déclarer anticonstitutionnelles les dispositions de l'article 434-15-2 du Code pénal, cela signifierait que la tâche qui incombe aux enquêteurs devient de plus en plus délicate, en l'absence de coopération qui serait alors justifiée par des droits supérieurs. Il convient de rappeler également que la disposition vise *« quiconque »* ce qui est en réalité d'application plus large que le seul mis en cause dans un procès. Cela peut en effet concerner un prestataire technique, un tiers.

Recommandationn°20 : En présence d'une annulation/abrogation de cette disposition pour anticonstitutionnalité, il conviendrait peut-être de mieux circonscrire l'application de ce texte à l'instar des textes déjà applicables au cas d'entraves à l'exercice de la justice.

Pour mémoire, l'article 434-15-2 du Code pénal a déjà donné lieu à des condamnations (Cour d'appel de Poitiers le 23 octobre 2015 confirmant la décision de première instance : infraction suffisamment établie et confirmation des peines prononcées dont confiscation du matériel saisi)[27].

3.7.3 Captation de données

La captation de données informatiques (articles 706-102-1 à 706-102-9 du Code de procédure pénale) est une technique d'enquête instituée par l'article 36 de la loi du 14 mars 2011 (LOPPSI) et s'inspirant directement des articles 706-96 à 706-102 du Code de procédure pénale relatifs à la sonorisation et à la fixation d'images de certains lieux ou véhicules[28] :

> *« Si les nécessités de l'enquête relative à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention peut, à la requête du procureur de la République, autoriser par ordonnance motivée les officiers*

[27] Cour d'appel de Poitiers, 23 octobre 2015, N° Rôle 15/00866

[28] Articles introduits par loi Perben II du 9 mars 2004.

et agents de police judiciaire requis par le procureur de la République à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder en tous lieux à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques audiovisuels.[…] »

3.7.3.1 Une technique limitée à la criminalité et à la délinquance organisées

Cette technique permet de capter en temps réel des données à l'insu de l'intéressé. Elle ne peut être mise en œuvre que pour les infractions qui relèvent de la criminalité et de la délinquance organisée et sont inventoriées aux articles 706-73 et 706-73-1 du Code de procédure pénale.

3.7.3.2 Une technique étendue à toutes les formes d'enquête

Jusqu'à la loi du 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme, une captation ne pouvait être opérée qu'au cours d'une instruction, sur ordonnance motivée du juge d'instruction. Désormais, la loi en étend la possibilité aux autres enquêtes, sur décision du juge des libertés et de la détention.

3.7.3.3 Une technique aussi utilisée par les services de renseignement

La loi du 24 juillet 2015 relative au renseignement (article L. 853-2 du Code de la sécurité intérieure) autorise les services de renseignement à utiliser la technique de captation de données à distance, « *lorsque les renseignements ne peuvent être recueillis par un autre moyen légal autorisé* ». Cette faculté est ouverte aux agents des services du « *premier cercle* » (L.811-2) et, pour certaines finalités, aux agents du « *deuxième cercle* » (L.811-4), dont la liste est fixée par l'article R853-2 du Code de la sécurité intérieure.

3.7.3.4 Une mise en œuvre à des fins judiciaires restreinte à certains services

Seuls les unités et services, dont la liste est précisée par l'article D.15-1-6 du Code de procédure pénale, peuvent y avoir recours :

- la direction centrale de la police judiciaire (DCPJ) et ses directions interrégionales et régionales ;
- la direction générale de la sécurité intérieure (DGSI) ;
- les offices centraux de police judiciaire ;
- la force d'intervention de la police nationale ;
- la sous-direction de la police judiciaire (SDPJ) de la gendarmerie nationale ;
- le service central de renseignement criminel (SCRC) de la gendarmerie nationale ;
- les sections de recherches de la gendarmerie nationale ;
- les sections d'appui judiciaire de la gendarmerie nationale ;
- le groupe d'intervention de la gendarmerie nationale (GIGN).

3.7.3.5 Les modalités de la captation de données

Sa durée, renouvelable une fois, est de quatre mois. Le dispositif technique peut être installé *in situ* ou, grâce à un logiciel, par le biais d'une transmission par un réseau de communication électronique (art. 706-102-5 du Code de procédure pénale).

La captation peut être réalisée en tous lieux (public ou privé, y compris cybercafés ou bornes d'accès publiques[29]). Une autorisation du juge des libertés et de la détention ou du juge d'instruction est cependant requise pour l'installation du dispositif technique dans un lieu d'habitation en dehors du créneau horaire 6h/21h (article 706-102-5 du Code de procédure pénale). Ce même article interdit la captation au cabinet ou domicile d'un avocat, au sein d'une entreprise de presse, au cabinet d'un médecin, d'un huissier, d'un avoué, au bureau et au domicile d'un parlementaire ou d'un magistrat.

Les articles 706-102-1 à 706-102-9 du Code de procédure pénale ne permettent pas de prendre le contrôle d'un système d'information, mais uniquement d'accéder à certaines données (stockées, saisies ou affichées et transitant par les périphériques audiovisuels). Contrairement à la perquisition, celle-ci peut durer et s'affranchit de l'obligation de présence de la personne concernée. Elle a pour effet « *de mettre l'enquêteur dans la situation de quelqu'un qui observerait derrière l'utilisateur d'un ordinateur* [30]» et prendre connaissance d'un contenu avant qu'il ne soit chiffré, d'être témoin, en temps réel, des échanges sur des forums de discussion, « *chat* » etc. La captation permet aussi de prendre connaissance des textes qui seront ultérieurement placés sur un périphérique (disque dur, clef USB, CD-Rom, etc.). C'est une technique d'enquête assez proche des interceptions judiciaires.

La transcription des données se limite aux données utiles à la manifestation de la vérité, tandis que les enregistrements des données informatiques sont détruits, à la diligence du procureur de la République ou du procureur général à l'expiration du délai de prescription (article 706-102-9 du Code de procédure pénale).

3.7.3.6 L'adaptation de la loi aux modes de communication

La loi, dans sa rédaction initiale, permettait d'accéder aux données telles qu'elles s'affichent sur l'écran par saisie de caractères. L'évolution des modes de communication par voie électronique a conduit le législateur à élargir la captation aux sons et aux images reçus et émis par des périphériques audiovisuels. Des applications téléphoniques (par exemple *Skype*), souvent utilisées par les cybercriminels, échappaient au champ des interceptions judiciaires. Les sociétés proposant ces services « *over the top* » ne sont en général pas considérées comme des opérateurs de communications électroniques au sens de l'article L.33-1 du Code des postes et communications électroniques. Ces sociétés, généralement établies à l'étranger, refusent de répondre aux demandes de déchiffrement émises par les autorités françaises. La loi du 13 décembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme corrige cette anomalie pour l'ensemble des infractions visées à l'article 706-73 du Code de procédure pénale. Peuvent désormais faire l'objet d'une

[29] Dans sa délibération n°2009-200 du 16 avril 2009, la CNIL s'est inquiétée de la capacité ainsi donnée de capter toutes les images affichées sur l'écran de tous les ordinateurs d'un point d'accès public à internet, et ce, à l'insu des utilisateurs.

[30] Etude d'impact annexée au projet de loi.

captation, non seulement les frappes de caractères et les données, mais aussi images et sons reçus et émis lors de l'utilisation d'un service audiovisuel en ligne.

3.7.3.7 De la loi à la pratique

A la fin de l'année 2017, la presse s'est faite écho de la création à venir d'un service technique national de captation judiciaire, placé au sein de la direction générale de la sécurité intérieure et chargé de mettre à disposition ces solutions techniques. Cette annonce augure d'une application imminente de ces dispositions, particulièrement attendues par les enquêteurs et les magistrats chargés des faits de terrorisme et de criminalité organisée.

4 Coopération internationale

Une lutte efficace contre la Cybercriminalité sous l'angle de la répression suppose une coopération non seulement des différents services d'investigation et d'enquête, des acteurs publics avec les acteurs privés (hébergeurs, fournisseurs de services d'accès à Internet), mais également une coopération entre Etats et organismes internationaux. Un Etat ne peut pas lutter seul contre ce phénomène criminel.

Il existe quelques initiatives internationales dans la lutte contre la cybercriminalité (Nations-Unies, Interpol, Europol, Union européenne, Union africaine, CEDEAO et Conseil de l'Europe. Des accords de coopération stratégique et opérationnelle entre Europol et les pays tiers facilitent les échanges d'informations et la coopération pratique.

4.1 Convention du Conseil de l'Europe sur la cybercriminalité

Mais à ce jour, la seule convention de portée internationale faisant référence en la matière est la Convention de Budapest du 23 novembre 2001 signée sous l'égide du Conseil de l'Europe traite des infractions possibles à l'égard des droits d'auteur, de la sécurité des réseaux informatique, des fraudes en général et aussi de la lutte contre la pornographie enfantine. Un texte unique en son genre qui dépasse le seul cadre du Conseil de l'Europe puisque 56 pays du monde entier ont adhéré à ce jour, dépassant largement les frontières de l'Europe (Canada, USA, Japon, Australie, Sénégal …) et plus de 70 autres pays s'en inspirent pour élaborer leur législation interne. Il est important que de plus en plus de pays y adhèrent et que chacun puisse faire la promotion de ses règles, ainsi que de ses protocoles additionnels.

Cette convention est le seul instrument cohérent et rassembleur en matière de lutte contrat la cybercriminalité et le recueil de la preuve numérique. Il s'agit d'un premier traité international sur les infractions pénales commises via l'Internet. Elle a pour objectif d'harmoniser les règles de procédure d'obtention de preuve en matière de coopération policière, d'entraide judiciaire et d'extradition. Il sert de référence pour tout pays souhaitant élaborer une législation en la matière en prévoyant l'harmonisation des comportements devant être réprimés dans les droits nationaux (législation appropriée), des règles de procédure et des moyens d'obtention de la preuve au niveau national, et des règles d'obtention de preuve en matière de coopération policière, d'entraide judiciaire et d'extradition. Des dispositions spécifiques sont prévues en matière de conservation et de divulgation de données, point de contact 24/7 dans le cadre de la coopération internationale (articles 29-35 de la Convention de Budapest) et sur le plan procédural national, s'agissant de disposition en matière de perquisition et saisies, interception de données informatiques. A défaut d'un consensus pour la création d'un texte d'ampleur internationale contraignant en matière de cybercriminalité, la Convention de Budapest est la seule alternative.

Une grande réunion internationale OCTOPUS se tient en outre tous les 18 mois avec l'ensemble des acteurs concernés ce qui permet d'échanger pour faire le point sur des nouvelles pratiques et ainsi avoir une veille sur les outils et usages développés par les cybers délinquants et les réponses techniques et juridiques efficaces à y apporter.

4.2 Directive NIS

La Directive Network and Information Security (NIS) adoptée le 6 juillet 2016 qui a fait l'objet de près de trois ans de négociations et qui devra être transposée au plus tard le 9 mai 2018 dans le droit national de chacun des Etats membres de l'Union européenne permet de place l'Union européenne en pointe en matière de cybersécurité. Elle prévoit en effet le renforcement des capacités nationales de cybersécurité et établit un cadre formel de coopération entre Etats membres, auquel l'ANSSI entend prendre une part active. La directive prévoit également le renforcement de la cybersécurité d'opérateurs issus de secteurs clés ainsi que de certaines plateformes numériques.

Structurée autour de plusieurs axes, la directive prévoit le renforcement des capacités nationales de cybersécurité :

- Les États-membres devront notamment se doter d'autorités nationales compétentes en matière de cybersécurité, d'équipes nationales de réponse aux incidents informatiques (CSIRT) et de stratégies nationales de cybersécurité. Respectivement en France, l'ANSSI, le CERT-FR et la stratégie nationale pour la sécurité du numérique.

- L'établissement d'un cadre de coopération volontaire entre Etats membres de l'Union européenne via la création d'un « *groupe de coopération* » des Etats membres sur les aspects politiques de la cybersécurité et un « *réseau européen des CSIRT* » des Etats membres afin notamment à faciliter le partage d'informations techniques sur les risques, vulnérabilités.

- Enfin, des règles européennes communes en matière de cybersécurité des prestataires de services numériques dans les domaines de l'informatique en nuage, des moteurs de recherche et places de marché en ligne seront instaurées.

4.3 Coopération avec les pays tiers

L'Amélioration de la coopération avec les pays tiers s'inscrit parmi les objectifs prioritaires poursuivis par l'Union européenne.

C'est grâce à une coopération étroite avec les pays tiers au moyen notamment de l'échange des meilleures pratiques, d'enquêtes communes, du renforcement des capacités et de l'entraide judiciaire que la lutte contre la cybercriminalité pourra être plus efficace. Il est important d'améliorer l'efficacité et promouvoir l'utilisation des traités d'entraide judiciaire (TEJ) en vue de mettre fin à l'appropriation de la compétence extraterritoriale par des pays tiers.

Dans ce contexte, il est manifeste que le plus grand nombre de demandes émanant des services répressifs sont transmises aux États-Unis et au Canada. Or le taux de divulgation des grands fournisseurs de services américains en réponse aux demandes formulées par les autorités de justice pénale européennes est malheureusement inférieur à 60 %. Il convient de rappeler ici que, selon le chapitre V du règlement général sur la protection des données consacré aux transferts de données à caractère personnel vers des pays tiers ou à des organisions internationales, les TEJ et d'autres accords internationaux constituent le mécanisme privilégié pour permettre l'accès aux données personnelles détenues hors de l'Union.

Des mesures concrètes doivent être prises pour protéger les droits fondamentaux des suspects ou des prévenus lorsqu'un échange d'informations a lieu entre les services répressifs européens et les pays tiers, notamment en ce qui concerne les garanties quant à l'obtention rapide, sur la base d'une décision judiciaire, d'éléments de preuve pertinents, des données des abonnés ou des métadonnées détaillées et des données relatives au contenu (si elles ne sont pas cryptées) de services répressifs et/ou de fournisseurs de services en vue d'améliorer l'entraide judiciaire. Il est important d'étudier de nouveaux moyens de recueillir et d'obtenir efficacement les preuves électroniques hébergées dans des pays tiers, dans le plein respect des droits fondamentaux et de la législation européenne en matière de protection des données, en accélérant et en simplifiant l'utilisation des procédures d'entraide judiciaire et, le cas échéant, de la reconnaissance mutuelle entre législations adéquates.

Des travaux sont en cours au sein du comité de la Convention sur la cybercriminalité du Conseil de l'Europe concernant l'interprétation de l'article 32 de la Convention de Budapest qui porte sur l'accès transfrontière à des données informatiques stockées (« *preuves dans le nuage* »).

Mais certains s'inquiètent du fait que l' adoption d'un protocole additionnel ou d'orientations visant à élargir le champ d'application de cette disposition au-delà du régime établi par la convention, qui constitue déjà une exception d'importance majeure au principe de territorialité, serait inopportune car de telles mesures pourraient permettre aux services répressifs d'accéder à distance et sans entrave à des serveurs et à des ordinateurs situés dans d'autres juridictions sans avoir recours à l'entraide judiciaire ou à d'autres instruments de coopération judiciaire mis en place en vue de garantir les droits fondamentaux des personnes, dont la protection des données et le respect de la légalité, et notamment, en particulier en application de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Ainsi, dans l'affaire opposant Microsoft au Gouvernement US en cours d'examen par la Cour Suprême des Etats-Unis, la question est de savoir si Microsoft était fondée à refuser de fournir des informations sur des emails stockés sur des serveurs en Irlande. Le gouvernement fédéral a fait valoir que Microsoft devrait se conformer au mandat, en vertu du *Stored Communications Act*, mais Microsoft conteste la demande estimant que les mandats de perquisition US ne pouvaient pas s'appliquer au-delà des frontières américaines. C'est dans ce contexte que la Commission européenne a décidé de soumettre en décembre 2017, au nom de l'Union européenne, un *amicus brief* devant la Cour suprême, en tant que partie tierce dans le but de fournir au tribunal des informations supplémentaires pertinentes dans une affaire concernant le transfert de données personnelles par Microsoft de l'Union européenne vers les États-Unis pour s'assurer que la Cour suprême pendra en compte les règles européennes applicables en la matière.

Des discussions en cours entre la Grande-Bretagne et les Etats-Unis mettraient en place une collaboration étroite entre ces deux Etats qui autoriseraient, sous prétexte d'une plus grande célérité, l'accès direct à des données par l'autorité judiciaire étrangère directement auprès des opérateurs nationaux. Cela impliquerait toutefois une réciprocité.

Sur ce point, il est important de rappeler les dispositions de la directive 2016/680 concernant les traitements de données à caractère personnel mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales devant être transposées d'ici le 6 mai 2018. Le projet de loi « CNIL3 » actuellement débattu, après avis

de la CNIL du 30 novembre 2017[31], a pour objet la mise en conformité du droit national avec le « *paquet européen de protection des données* » adopté par le Parlement européen et le Conseil le 27 avril 2016 (cf. Annexe 2 ci-dessous).

Recommandation n°21 : Sauf à être en présence des législations d'un niveau adéquat comportant les mêmes règles en matière de protection de la vie privée et des données à caractère personnel, il conviendrait avant tout de privilégier et donc de rendre plus efficaces et rapides les moyens déjà mis en place dans le cadre des TEJ.

Pour en savoir plus : Rapport sur le marché unique du numérique du 6 décembre 2017 des députés Eric Bothorel et Constance Le Grip.

[31] Délibération n°2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du 6 janvier 1978

5 CONCLUSION

Ce rapport clôt les réflexions du Groupe de travail Cyberlex – CECyF sur les moyens de rendre plus efficace la lutte contre la cybercriminalité, tant au travers des règles prévues par le Code pénal (premier rapport de janvier 2017) que celles édictées par le Code de procédure pénale (présent rapport de janvier 2018).

Les travaux du Groupe se sont limités ici à une lecture critique des dispositions du Code de procédure pénale qui pouvaient être plus spécialement concernées par la lutte contre la cybercriminalité et ses spécificités techniques, notamment au travers des règles édictées en matière de collecte de la preuve numérique. Il apparaît que les propositions qui nous semblent devoir être prises en compte dans un bref délai concernent avant tout l'enquête sous pseudonyme, comme nouvelle procédure d'enquête numérique, qui constitue nettement un des moyens d'investigation les plus adaptés dans le monde du cyber. Les autres propositions de ce rapport sont naturellement également à prendre en compte dans une perspective d'anticipation et de prévisibilité des actions à venir.

Les nombreux débats qui ont animé le Groupe de travail Cyberlex – CECyF ont fait émerger d'autres chantiers, tels que les dispositions prévues par le Code des postes et communications électroniques, la future loi de transposition de la Directive NIS (Directive Network and Information Security) ou de la Directive 2016/680 concernant les traitements de données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales en cours de transposition par la loi « CNIL3 » sur la procédure pénale, qui représentent des enjeux actuels importants pour la lutte contre la cybercriminalité.

Enfin, au vu de la complexité des règles et de leur éclatement, et ce dans la suite logique des travaux conduits depuis presque deux ans, il apparaît de plus en plus nécessaire qu'un Code du Numérique soit édité, en tant que Corpus de règles applicables en matière de technologies de l'information et de la communication associées au droit pénal et à la procédure pénale. Ainsi le Groupe de travail Cyberlex – CECyF pourrait prochainement proposer un glossaire et une architecture de ce Code afin de contribuer de manière encore plus efficiente à une meilleure lisibilité des textes qui doivent être parfaitement connus de tous les acteurs de la lutte contre la cybercriminalité pour espérer une application réelle et effective.

ANNEXE I – Infractions visées par les dispositions d'enquête sous pseudonyme

Infractions visées	Prévues par les articles correspondants	Articles prévoyant l'ESP	Loi à l'origine
Mise en péril de mineurs : Provocation envers un mineur à commettre une infraction relative aux produits stupéfiants ou à la consommation habituelle ou excessive de boissons alcooliques … corruption, propositions sexuelles à mineur de 15 ans, pédopornographie	Art. 227-18 à 227-24 du Code pénal	Article 706-47-3 CPP	Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance, modifié par la loi n°2014-1353 du 13 novembre 2014 (art.20)
Recours à la prostitution d'un mineur ou d'une personne vulnérable	Art.225-12-1 à 225-12-4 du Code pénal	Article 706-35-1 CPP	Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance, modifié par la loi n°2014-1353 du 13 novembre 2014 (art.20)
Traite des êtres humains	Art.225-4-1, 225-4-8 et 225-4-9 du Code pénal	Article 706-35-1 CPP	Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance, modifié par la loi n°2014-1353 du 13 novembre 2014 (art.20)
Proxénétisme	Article 225-5 et 225-6 du Code pénal	Article 706-35-1 CPP	Loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance, modifié par la loi n°2014-1353 du 13 novembre 2014 (art.20)
Infractions commises à l'occasion de paris ou de jeux d'argent ou de hasard en ligne	LOI n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne	Art.59	LOI n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne

Infractions visées	Prévues par les articles correspondants	Articles prévoyant l'ESP	Loi à l'origine
Infractions aux produits de santé	Art. L. 5421-2, L. 5421-3, L. 5421-13, L. 5426-1, L. 5432-1, L. 5432-2, L. 5438-4, L. 5439-1, L. 5451-1, L. 5461-3 et L. 5462-3 du CSP Art. L. 213-1 du Code de la Consommation (produits mentionnés à l'article L. 5311-1 du CSP)	Article 706-2-2 CPP	Ordonnance n°2013-1183 du 19 décembre 2013 (art.23) relative à l'harmonisation des sanctions pénales et financières relatives aux produits de santé …
Atteinte à un système de traitement automatisé de données (STAD) à caractère personnel mis en œuvre par l'Etat, commis en bande organisée	Art. 323-4-1 CP	Art. 706-72 CPP combiné avec l'article 706-87-1 CPP	Loi n°2014-1353 du 13 novembre 2014 (art. 18)
Criminalité organisée	Art. 706-73 du CPP	Article 706-87-1 CPP	Loi n°2014-1353 du 13 novembre 2014 (art. 18), modifiée la loi n°2015-993 du 17 août 2015 (art.11)
Délit d'escroquerie en bande organisée, Délits de dissimulation d'activités ou de salariés Délits de blanchiment Délits d'association de malfaiteurs Délit de non-justification de ressources…	Art.706-73-1 du Code de procédure pénale - dernier alinéa de l'article 313-2 du Code pénal ;	Article 706-87-1 CPP	Loi n°2015-993 du 17 août 2015 (art.11)
Terrorisme : provocation et apologie…	Art. 706-73 (11°)	Article 706-87-1 CPP	Loi n°2014-1353 du 13 novembre 2014 (art. 18), modifiée la loi n°2015-993 du 17 août 2015 (art.11)
Trafic d'espèces animales ou végétales protégées ou menacées et infractions à la réglementation	Art. L. 415-3 du code de l'environnement, Article L. 441-1 (tromperie) du code de la consommation lorsque l'infraction porte sur tout ou partie d'animaux ou de végétaux	Article 706-2-3	Loi n°2016-1087 du 8 août 2016 (art.130)

ANNEXE II - RGPD & directive et projet de règlement e-Privacy

Dans son rapport sur la lutte contre la cybercriminalité (2017/2068 (INI)) de la Commission des libertés civiles, de la justice et des affaires intérieures auprès du Parlement européen de juin 2017, il a été reconnu qu'un cadre juridique efficace pour la protection des données est indispensable pour instaurer la confiance dans le monde en ligne et permettre tant aux consommateurs qu'aux entreprises de tirer pleinement profit des avantages du marché unique numérique et de lutter contre la cybercriminalité.

Ainsi le nouveau règlement général sur la protection des données à caractère personnel (ci-après « GDPR ou RGPD ») sera applicable à compter du 25 mai 2018. Il modifie et complète la Loi Informatique et Libertés du 6 janvier 1978, déjà amendée à plusieurs reprises pour prendre en compte les évolutions des usages et des technologies, dont la dernière fois, le 7 octobre 2016, à la suite de l'entrée en vigueur de la loi pour une République numérique intégrant en droit français par anticipation certaines dispositions prévues par le GDPR.

En tant que changement de paradigme, le RGPD instaure un principe de responsabilisation de chacun des acteurs privés (entreprises, sous-traitants, donneurs d'ordre) dans la sécurisation des systèmes d'information et des données.

Le RGPD concerne les données des personnes physiques, structurées et non structurées, collectées et traitées par les entreprises, qu'elles soient hébergées au sein de l'entreprise ou dans le cloud, ou bien que les traitements soient confiés à des prestataires, notamment dans le cadre de contrats d'infogérance. Ces données peuvent être collectées auprès des clients, des prospects, des partenaires et des salariés.

Pour contraindre les entreprises à s'y conformer et créer ainsi un Marché Unique Numérique, le législateur européen a prévu des sanctions dissuasives, pouvant aller jusqu'à 20 millions d'euros, ou 4 % du chiffre d'affaires mondial des contrevenants.

Les entreprises doivent mettre en œuvre des processus de protection des données à caractère personnel, répondant à une dizaine de grands principes :

- Principe de transparence : les données doivent être traitées de manière loyale et transparente, après communication aux personnes concernées d'une information complète sur leur traitement, formulée dans des termes simples.
- Principe de limitation des finalités : les données doivent être collectées pour une finalité précise, et ne doivent pas être réutilisées ultérieurement pour une autre finalité, sauf consentement exprès et information préalable des personnes concernées.
- Principe d'un consentement renforcé : les personnes concernées doivent en principe donner leur accord pour le traitement de leurs données, et ce de manière non ambigüe, ou pouvoir s'y opposer tout aussi facilement.
- Principe de minimisation des données et de Privacy by Default : seules les données adéquates, pertinentes et nécessaires à la finalité du traitement doivent être collectées et utilisées.
- Principe d'exactitude des données : des mesures doivent être prises pour s'assurer que les données sont exactes et mises à jour, et que celles qui sont inexactes sont effacées ou rectifiées sans tarder.

- Principe de proportionnalité de la durée de la conservation des données : les données ne peuvent être conservées que pendant la durée nécessaire au regard de la finalité du traitement.
- Principes de sécurité, d'intégrité et de confidentialité des données : des mesures de sécurité doivent être prises afin de protéger les données.
- Principe de licéité : un traitement n'est licite que si la personne concernée a consenti au traitement, ou bien si le traitement est nécessaire à l'exécution d'un contrat, au respect d'une obligation légale, à la sauvegarde des intérêts vitaux de la personne concernée, ou aux fins des intérêts légitimes poursuivis par le responsable du traitement.
- Principe de *Privacy by design* : le principe de protection des données individuelles doit être pris en compte dès le début du projet et la conception des systèmes de traitement.
- Principe de responsabilisation des acteurs : les sous-traitants deviennent co-responsables. Plusieurs entreprises peuvent se voir reconnaître conjointement responsables de manquements au GDPR.
- Principe « d'accountability » : l'entreprise doit être en mesure de démontrer la mise en œuvre des procédures de protection des données personnelles visant à respecter les obligations du GDPR. Les procédures de mise en conformité doivent être appropriées, permanentes et auditées régulièrement. En contrepartie, les entreprises ne seront plus tenues de déclarer leurs traitements de données personnelles à la CNIL.

Un projet de loi relatif à la protection des données personnelles (version du 13 décembre 2017) dit également « loi de toilettage de la loi du 6 janvier 1978 modifiée ») pour prendre en compte le RGPD est actuellement en cours de discussion. La loi devrait être adoptée au plus tard en mars 2018. Le projet de loi « CNIL 3 » actuellement débattu a déjà fait l'objet de critiques de la part de la CNIL. Si cette dernière considère que le projet de loi répond globalement à l'objectif fixé de transposition et d'adaptation au droit français des nouvelles règles européennes et souligne le caractère symbolique de ne pas abroger la loi fondatrice du 6 janvier 1978, elle regrette les délais trop cours pour examiner les dispositions, un défaut de lisibilité de l'état du droit et une réelle occasion manquée pour procéder au réexamen du droit de la protection des données.

Ainsi, dans le domaine spécifique des traitements de données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales (directive n°2016/680), le projet de loi « CNIL3 » consacre ses articles 70-1 et 70-25 et suivants à sa transposition en droit français. Sauf en cas de menace grave et immédiate pour la sécurité publique d'un autre Etat ou pour la sauvegarde des intérêts essentiels de la France, l'autorisation préalable à un transfert des données provenant d'un autre Etat est requise conformément à son droit national, notamment quand le transfert de données hors de l'Union européenne est nécessaire à l'une des finalités énoncées au 1° de l'article 70-1 du projet de loi. Une décision d'adéquation pourra être requise en application de l'article 36 de la directive ou tout au moins des garanties appropriées en ce qui concerne la protection des données dans un instrument juridiquement contraignant résultant d'une convention mise en œuvre avec des Etats tiers ou résulter de dispositions juridiquement contraignant exigées à l'occasion de l'échange de données.

Il conviendra de suivre attentivement l'évolution du texte sur ces points notamment et analyser la portée des dispositions qui seront adoptées finalement à l'issue des débats parlementaires sur le projet de loi « CNIL 3 ».

Dans ce contexte législatif assez riche il doit être aussi mentionné le Projet de règlement européen ePrivacy

Le projet de règlement européen e-Privacy a pour ambition de remplacer la directive e-Privacy adoptée en 2002. La Commission européenne a proposé début 2017 une première version avec pour objectif de protéger les libertés et droits des usagers, personnes physiques ou morales, de services de communication électronique. Ce règlement impactera les pratiques actuelles des acteurs de réseaux sociaux, d'objets connectés ou de téléphonie, notamment dans leur approche marketing.

Les principaux objectifs de ce texte sont :

- de s'appuyer sur le RGPD pour désigner les autorités de contrôle et définir les sanctions ;
- d'étendre la protection des droits des usagers aux nouveaux services de communication ;
- de simplifier les règles concernant les témoins de connexion de type « cookie » ;
- d'obtenir le consentement préalable à toute prospection directe afin de limiter le spam ;
- de garantir la confidentialité des méta-données au même titre que les données elles-mêmes et de limiter leur usage à la nécessité du service, à la facturation ou dans le cadre du consentement de l'usager.

Toujours en cours de rédaction, ce texte fait l'objet de désaccords profonds entre :

- d'une part, les représentants des acteurs commerciaux présentant un intérêt légitime à traiter les données ou métadonnées, version présentée par le comité IMCO ("marché intérieur et protection des consommateurs") ;
- d'autre part, les représentants de défense des droits et les autorités de protection des données présentant une vision plus protectrice des usagers concernant les craintes de limitation d'accès aux services et de traçabilité des équipements électroniques, version défendue par la commission LIBE ("Libertés civiles, de la justice et des affaires intérieures").

Cette dernière position, plus protectrice des usagers, a été adoptée par le Parlement européen le 19 octobre dernier. Les articles faisant encore l'objet de débats concernent le traitement et le stockage des métadonnées (articles 6 à 8). Plusieurs organes européens ont exprimé le souhait de voir ce règlement entrer en vigueur à la même date que le RGPD le 25 mai 2018. Mais au vu des derniers développements, de la procédure européenne et des lobbyings actifs, il est d'ores et déjà acquis que le texte ne pourra pas être adopté avant fin 2018 – début 2019.