Février 2025

RAPPORT N°20.48

Institut des Études
et de la Recherche
sur le Droit et la Justice

Pratiques et principes de l'enquête pénale à l'épreuve des nouvelles technologies d'investigation et de surveillance

Sous la direction de

Florence BELLIVIER et Juliette TRICOT

cd·po CENTRE DE DROIT PENAL ET DE CRIMINOLOGIE

Université Paris Nanterre

RAPPORT DE RECHERCHE

Cette recherche est issue de l'appel à projet :
L'appréhension des nouvelles technologies d'investigation et de surveillance par la procédure pénale

Sous la direction de

Florence BELLIVIER,
Professeure à l'Université Paris 1 (Panthéon-Sorbonne)

Juliette TRICOT,
Maîtresse de conférences à l'Université Paris Nanterre

Recherche co-écrite avec

Vissarion GIANNOULIS,
Maître de conférences à l'Université Paris Nanterre

Avec la collaboration de

Matthieu AUDIBERT,
Chef du département partenariats et coopération, conseiller juridique du chef du Commandement de la gendarmerie dans le cyberespace, docteur en droit de l'Université Paris Nanterre (Centre de droit pénal et de criminologie)

Antonin GUILLARD,
Doctorant au Centre de droit pénal et de criminologie (Université Paris Nanterre)

Maxime LASSALLE,
Maître de conférences à l'Université de Dijon

Sophie SONTAG-KOENIG,
Maîtresse de conférences à l'Université Paris Nanterre

Avec la participation de

Eleonora CERVELLERA,
Doctorante

Sophie MALLIARAKIS,
Magistrate

Fanny-Elisabeth ROLLET,
Doctorante

Djohar SIDHOUM-RAHAL,
Docteure

Vincent SIZAIRE,
Magistrat, maître de conférences associé à l'Université Paris Nanterre

Anfissa YEVTIHIDIS,
Doctorante

Le présent document constitue le rapport scientifique d'une recherche réalisée avec le soutien du Groupement d'Intérêt Public Institut des études et de la recherche sur le droit et la justice (Convention N°20.48). Son contenu n'engage que la responsabilité de ses auteurs.

Toute reproduction, même partielle est subordonnée à l'accord de l'IERDJ.

Cette recherche collective a été conduite du 15 janvier 2021 au 11 mars 2024[*].

Elle reposait sur une équipe de chercheurs, membres du Centre de droit pénal et de criminologie de l'Université Paris Nanterre, auxquels les responsables scientifiques adressent leurs vifs remerciements : Eleonora Cervellera, *doctorante*, Sophie Malliarakis, *magistrate*, Fanny-Élisabeth Rollet, *doctorante*, Djohar Sidhoum-Rahal, *docteure*, Vincent Sizaire, *magistrat*, *maître de conférences associé à l'Université Paris Nanterre*, Anfissa Yevtihidis, *doctorante*.

Ont plus particulièrement contribué à cette recherche[**] :

Matthieu Audibert
Chef du département partenariats et coopération, conseiller juridique du chef du Commandement de la gendarmerie dans le cyberespace, docteur en droit de l'Université Paris Nanterre (Centre de droit pénal et de criminologie)

Antonin Guillard,
Doctorant au Centre de droit pénal et de criminologie

Maxime Lassalle,
Maître de conférences à l'Université de Dijon

Sophie Sontag-Koenig,
Maîtresse de conférences à l'Université Paris Nanterre

Si la conception, la relecture et l'harmonisation ont été le fruit d'un travail toujours concerté entre les trois rédacteurs, ceux-ci se sont répartis le travail d'écriture proprement dit comme suit :

Introduction : Florence Bellivier
Partie 1 : Florence Bellivier (avec Vissarion Giannoulis pour la section 3, §2, point I)
Partie 2. Vissarion Giannoulis
Partie 3 et conclusions : Juliette Tricot

[*] Travail actualisé au 1er novembre 2024.
[**] Voir notamment, dans ce rapport la *cartographie des acteurs du recueil et de l'administration du renseignement et de la preuve numériques* réalisée par Antonin Guillard et Sophie Sontag Koenig.
Voir également leurs contributions ainsi que celle de Maxime Lassalle dans le numéro spécial de l'*AJ Pénal* (novembre 2023) : *« L'accès à la preuve obtenue par les nouvelles technologies d'investigation et de surveillance ».* Maxime Lassalle et Sophie Sontag Koenig ont en outre contribué à la rédaction de la réponse à l'appel à projets à l'origine de cette recherche. Matthieu Audibert a mis au service de cette recherche son expertise, facilitant notre compréhension de la matière, sa connaissance fine des acteurs en nous mettant en relation avec des acteurs importants du domaine, et son suivi minutieux et privilégié des sources officielles ou grises en alimentant régulièrement notre appareil documentaire.

Sommaire

PREMIERE PARTIE : USAGES

SECTION 1 : L'USAGE DES NTIS, DES MOTS AUX ACTES

SECTION 2 : UNE QUESTION DE MESURE(S)

SECTION 3 : COMMUNAUTES PROFESSIONNELLES

CARTOGRAPHIE DES ACTEURS DU RECUEIL ET DE L'ADMINISTRATION DU RENSEIGNEMENT ET DE LA PREUVE NUMERIQUES

DEUXIEME PARTIE : NORMES

SECTION 1 : GENEALOGIE DES MESURES NTIS

SECTION 2 : REGIMES DES MESURES NTIS

TROISIEME PARTIE : PERSPECTIVES

SECTION 1 : DESTABILISATION DES REPERES DE LA PROCEDURE PENALE

SECTION 2 : RECONFIGURATION DE L'ENQUETE PENALE

Introduction

1.- « Nous ne sommes pas des spécialistes de la technologie, on est venu nous chercher car nous sommes des techniciens de la procédure pénale »[1] : ces propos de l'avocat pénaliste Guillaume Martine, intervenant avec son confrère Robin Binsard dans l'affaire *EncroChat*, du nom d'un réseau téléphonique utilisé par des trafiquants de drogue surveillé par la gendarmerie française et qui a donné lieu à un procès long de 16 mois devant le tribunal correctionnel de Bruxelles[2], illustrent toute la difficulté et la richesse d'une étude sur les nouvelles technologies d'investigation et de surveillance dans le cadre de l'enquête pénale pour reprendre les termes de l'appel à projets auquel l'équipe du Centre de droit pénal et de criminologie de l'Université Paris Nanterre a répondu au printemps 2020. De prime abord, l'intérêt de cette recherche, qui a débuté le 15 janvier 2021 et s'est terminée le 11 mars 2024[3], est apparu résider dans la difficulté à cerner un objet aux frontières difficiles à maîtriser : des textes rares et arides énumérant des mesures d'enquête pouvant entrer dans la catégorie visée par l'appel à projets, une jurisprudence clairsemée, du moins au début de notre travail, un champ éclaté, aucune recherche d'ampleur en langue française, davantage en langue anglaise mais plutôt sur quelques techniques ou sujets précis, des praticiens peu enclins à s'exprimer sur ce thème – ou du moins peu sollicités pour le faire. Sans doute ces vides, couplés aux confinements successifs dus à la pandémie de Covid-19, expliquent-ils que le premier appel à projets lancé par la Mission de recherche Droit et Justice ait été infructueux et qu'au second un seul projet ait été présenté, le nôtre. Le champ était donc non seulement relativement vierge mais sans doute aussi glissant. Afin de trouver des prises, nous avons adopté une démarche cadrée, enrichie et ouverte.

2.- En premier lieu, le cadre retenu a été celui d'une liste de mesures d'enquête, que nous avons établie à partir du droit international, très influent en la matière, ainsi que du Code de procédure pénale qui les égrène sans ordre logique apparent de sorte que leur repérage requiert un effort d'identification que ne facilitent ni le plan du Code ni le libellé des dispositions. Aussi bien, dans une toute première approche, la lecture du Code induit à se concentrer sur les mesures qualifiées de techniques spéciales d'enquête alors même qu'elles sont loin de couvrir la variété des mesures s'appuyant sur les nouvelles technologies d'investigation et de surveillance et en représentent la version la plus attentatoire aux droits fondamentaux et partant, théoriquement du moins, celles dont le recours n'est pas ordinaire. Bien vite cependant, ce que suggère le Code lui-même lorsqu'il les désigne de manière résiduelle et vague (« *autres* techniques spéciales

[1] THIERRY Gabriel, « Robin Binsard et Guillaume Martine : ces avocats qui ferraillent contre la procédure Encrochat », *Dalloz actualité*, 19 janvier 2024.
[2] Le jugement a été rendu le 29 octobre 2024. Voir également CEDH, 17 octobre 2024, *A.L. et E.J. c/ France*, requêtes n° 44715/20 et 47930/21 (irrecevabilité pour défaut d'épuisement des voies de recours internes).
[3] Le texte ici présenté a été fixé dans sa forme définitive à la date du 1er novembre 2024.

d'enquête ») [4], il apparaît qu'elles ne constituent qu'un sous-ensemble d'un ensemble plus vaste dispersé dans le Code.
L'analyse normative du recours à ces mesures très fragmentées dans le droit français a semblé indispensable pour suggérer la nécessité d'un effort de reconstruction et de mise en ordre du cadre juridique.
L'exercice de reconnaissance dévoile alors une distribution – dynamique car susceptible d'évoluer dans le temps – des mesures tantôt dans le giron du droit commun tantôt dans la sphère des procédures dérogatoires, en particulier celle applicable à la criminalité et à la délinquance organisées.
Quant au premier, sont dégagées du livre premier du CPP, les réquisitions (art. 60-1, 77-1-1, 99-3) auxquelles s'ajoutent – par inclusion jurisprudentielle – l'injonction de donner un mot de passe ou – par extension jurisprudentielle et insertion normative – la conservation rapide (art. 60-2), les perquisitions et saisies de données informatiques stockées (art. 56 et 57-1) ainsi que la géolocalisation (art. 230-32) et l'infiltration numérique (art. 230-46). Quant à la seconde, sont tirées du livre quatrième du CPP et plus précisément du titre XXV consacré à la procédure applicable à la criminalité et à la délinquance organisées et aux crimes, les interceptions des correspondances émises par la voie des communications électroniques (art. 706-95), l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique (art. 706-95-1 et 2), le recueil des données techniques de connexion (art. 706-95-20), la sonorisation et la fixation d'images (art. 706-96 à 706-98) et la captation de données informatiques (art. 706-102-1, 3 et 5).
La seule lecture de cette liste signale combien l'objet de la recherche se laisse difficilement saisir. A l'hermétisme du vocabulaire s'ajoute tantôt le caractère énigmatique du contenu concret des mesures prévues, tantôt la superposition d'une pluralité de mesures pour un même objectif. Pour franchir l'obstacle, il est d'abord utile de disposer d'un instrument de déchiffrement ou plus exactement de traduction de la langue juridico-technico-technologique. Aussi bien, afin de maîtriser les termes – au sens propre – des questions posées, l'équipe a senti le besoin de se munir d'un glossaire. Annexé au présent rapport, il vise à accompagner le lecteur et à encourager l'effort de vulgarisation mais aussi de réflexion sur le choix des mots du droit.
Ensuite, une première manière de remettre de l'ordre ou, à tout le moins, de commencer à se repérer en posant quelques balises, peut être de partir du type d'information recherchée pour sérier les mesures qui le permettent et ainsi tenter de les ordonner entre elles. C'est ainsi que, de manière sans doute encore sommaire, il est possible de distinguer trois types d'information auxquels correspondent trois objectifs principaux : l'identification (qui ?), la localisation (où ?) et le mode opératoire (comment ?). Mais alors qu'on espérait ainsi ordonner les mesures, c'est un surcroît de désordre qui se dégage. Ainsi la localisation, qui peut être réalisée en temps réel ou *a posteriori*, est notamment permise par le recueil des données techniques de connexion (*ie* le recours à un appareil dit *IMSI-Catcher* qui simulant une fausse antenne-relais intercepte toutes les données de communication circulant dans un rayon donné) et la géolocalisation, cette dernière se réalisant à son tour par la pose d'une balise sur un véhicule, la réquisition (auprès des opérateurs de télécommunication) des éléments permettant le bornage d'un téléphone ou l'activation à distance (concrètement le « piratage ») d'un appareil connecté, toutes variantes qui relèvent de régimes distincts. S'agissant de la détermination du mode opératoire, elle peut être réalisée grâce à l'ensemble des mesures qui permettent de prendre connaissance du contenu des situations, productions et échanges sonores, visuels ou écrits. On y retrouve dans le champ du droit commun les réquisitions (dont la conservation rapide) des données conservées par les

[4] *Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*, JORF n°0071, 24 mars 2019 ; ministère de la Justice, *Circulaire de présentation des dispositions de procédure pénale de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice relatives à l'enquête et à l'instruction applicables au 1er juin 2019*, CRIM N°2019-00329, 27 mai 2019.

opérateurs de télécommunications, auxquelles s'ajoutent les perquisitions et saisies ainsi que l'ensemble des mesures relevant de la sphère des procédures dérogatoires (sonorisation, fixation d'images, interception des communications, captation de données).

3.- En second lieu, il est très vite apparu que la méthode normative d'analyse et de reconstruction de ce cadre devait être doublement enrichie : par une analyse empirique, à partir des pratiques des acteurs intervenant à divers titres dans l'enquête pénale, des usages et non-usages de ces technologies ; par une analyse comparative destinée à éclairer la variété des options normatives, institutionnelles et professionnelles explorées à l'étranger dans un cadre très largement européanisé et aux dimensions également internationalisées.

4.- En troisième lieu, même si notre recherche porte sur les nouvelles techniques d'investigation et de surveillance (ci-après NTIS) dans l'enquête pénale, elle est de toutes parts cernée par quatre champs qui en constituent le nécessaire arrière-plan et sont aujourd'hui en plein bouillonnement : les liens entre renseignement et procédure pénale ; la conception de la place et du rôle de la science et des techniques dans leur rapport à la société et au droit ; l'évolution des règles relatives à l'obtention et à l'administration de la preuve dans l'enquête ; le recours aux fichiers dans l'enquête pénale.

5.- Tout d'abord, le recours aux NTIS illustre la porosité croissante de la frontière entre le renseignement et la procédure pénale, que certaines techniques venues du renseignement soient acclimatées dans la procédure pénale, comme le recours à un *IMSI-catcher*, ou que des informations obtenues dans le cadre du renseignement soient versées dans une procédure judiciaire[5]. La cartographie des acteurs de la procédure pénale et du renseignement présentée à la fin de la première partie en atteste. Les ambiguïtés de la notion de surveillance, à la frontière de la procédure pénale[6], traditionnellement destinée à identifier, poursuivre et juger les auteurs d'infraction, et de la police administrative, qui vise à prévenir les troubles à l'ordre public, sont emblématiques de cette évolution. C'est d'autant plus le cas que la notion de surveillance est, depuis une quinzaine d'années et surtout depuis les révélations d'Edward Snowden, employée de manière plus large, parfois associée aux adjectifs « globale » ou « généralisée » ou au complément du nom « de masse », pour désigner moins des procédures précises (pénales ou administratives) qu'un état de nos sociétés hyper-technicisées soumises à l'accumulation de modes variés de contrôle, impliquant l'État et de grands groupes privés, sachant que la surveillance des populations n'a, elle, rien de nouveau[7]. La nouveauté semble en revanche venir du recours massif aux technologies, ce qui conduit à évoquer un autre arrière-plan de la recherche.

6.- Ensuite, notre travail doit être situé dans le contexte du rapport que nos sociétés entretiennent à la science et à la technique. Là encore, il ne faut pas tomber dans le piège du « tout nouveau » - cela fait au moins deux siècles que la science au sens moderne du terme et la technique sont

---

[5] Voir TOUILLIER Marc (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, Dalloz, Les sens du droit, 2017 ; PIN Xavier, « Le Code de la sécurité intérieure substitut du Code de procédure pénale ? », *in* BEAUVAIS Pascal, CHILSTEIN David, DREYER Emmanuel (dir.), *Le droit pénal de l'avenir*, Lefebvre Dalloz, 2024, pp. 205-220.

[6] Sur le fait que dans certains cas, ici une opération douanière, la « surveillance » ne soit pas le terme approprié, voir THIERRY Jean-Baptiste, « Mal nommer les choses : la surveillance douanière », à propos de Crim. 13 décembre 2023, n°23-83.893, *AJ pénal* 2024, p. 470 : « La surveillance est et reste un acte « innommé » de constatation des infractions pénales ou douanières ».

[7] LYON David, « La surveillance globale dans un monde post-Snowden », *Communiquer*, 20, 2017, 49-65.
Voir AÏM Olivier, *Les théories de la surveillance. Du panoptique aux 'Surveillances Studies'*, Armand Colin, 2020.

promues, mais tenter de prendre la mesure de ce qui l'est, en quoi et avec quels effets. A cet égard, on peut faire trois constats qui semblent caractériser le rapport du monde actuel à la science et à la technique : celui d'une spécialisation toujours plus poussée ; celui d'une dépendance toujours plus grande des individus et des organisations aux technologies au point d'en être parfois fragilisés par exemple en cas de panne informatique d'envergure ; celui d'une ambivalence face à la science et la technique, à la fois objets de consommation et de critiques très vigoureuses. Cette ambivalence est aussi inhérente à la science et aux techniques qui libèrent en même temps qu'elles entravent. Là encore, la dialectique est des plus classique : les évolutions technologiques peuvent faire en sorte que des corps ne s'usent plus à la tâche mais, du même coup, créer du chômage ; la recherche sur l'embryon pourra peut-être permettre de découvrir les causes de l'infertilité mais elle suppose la destruction d'embryons humains ; les réseaux sociaux peuvent favoriser les mobilisations citoyennes mais aussi démultiplier la haine ou le harcèlement. La technique est-elle une entrave aux libertés, un instrument d'émancipation, un facilitateur ou un simple révélateur d'autres dynamiques à l'œuvre ? Ce rapport n'a évidemment pas pour but de répondre à cette question qui est à la frontière de l'éthique, de la philosophie et du droit mais l'interrogation reste en filigrane car elle rejaillit sur le droit et, plus précisément, le droit de la preuve qui est un des terrains où l'ambivalence de la science et de la technique est très marquée dès lors que la preuve scientifiquement obtenue sert aussi bien à accuser qu'à disculper.

7.- Les NTIS invitent en effet, en outre, à une réflexion sur les liens anciens mais toujours évolutifs entre enquête pénale, sciences et techniques du point de vue de la preuve qui est elle-même un champ en plein bouleversement au point de susciter des cours et des manuels spécifiques, alors même qu'il s'agissait naguère d'une question pratique capitale mais peu systématisée. Parmi les nombreux problèmes que pose la question de la preuve – celui du droit à la preuve[8], celui de la privatisation de la preuve[9], celui de ce qu'est une preuve, toute information n'en étant pas une –, celui de la preuve scientifique ou technique est fondamental à deux égards. Tout d'abord, les questions de la constitution de la preuve, de sa recevabilité, de sa possibilité d'être discutée, de la loyauté de son obtention[10] sont aujourd'hui sous la dépendance étroite du développement cumulatif des sciences et des techniques, chaque technique apportant sa contribution à la recherche des auteurs d'infractions et son lot de difficultés : l'on pense ici à la routinisation des empreintes génétiques dans le procès pénal[11] ou

[8] Voir AP 22 décembre 2023, n°20-20.648 et 21-11.330, *infra*, paragraphe n°214.

[9] GUILLOU Nicolas, « Les nouveaux modèles de participation de la société civile en politique criminelle », *RSC* 2024, p. 695 et s. Voir aussi, à propos du développement de l'exploitation des sources ouvertes désigné par l'OSINT (*Open Source Intelligence*) ou le ROSO (renseignement d'origine source ouverte), LECLERC Olivier, VERGES Etienne, VIAL Géraldine, « Preuves scientifiques et technologiques », *Cahiers Droit, Sciences &Technologies*, Chronique, 2022, p. 241 et s. ; AUMAITRE Aurélie, LETOQUEUX Hervé, « Apprivoiser les preuves numériques : la réception française de l'OSINT », *Délibérée*, 2023/2, pp. 49-55.

[10] Les NTIS contribuent largement au renouvellement de cette question classique de la tension entre provocation à la preuve et provocation à l'infraction. Voir, à propos de la géolocalisation, Crim. 28 mai 2024, n°23-86.390, « toute méthode d'investigation qui contribuerait à provoquer la commission de l'infraction est proscrite, le stratagème ainsi employé étant alors de nature à entraîner la nullité des actes de procédure. En dehors de cette hypothèse, le recours, par les autorités publiques, à un stratagème tendant à la constatation d'une infraction ou l'identification de ses auteurs ne constitue pas, en soi, une atteinte au principe de loyauté de la preuve. Pour qu'une telle atteinte soit constituée, il est nécessaire que le procédé employé, par un contournement ou un détournement d'une règle de procédure, ait pour objet ou pour effet de vicier la recherche de la preuve en portant atteinte à l'un des droits essentiels ou à l'une des garanties fondamentales de la personne suspectée ou poursuivie ».

[11] Voir entre autres références VAILLY Joëlle (dir.), *Sur la trace des suspects. L'incorporation de la preuve et l'indice à l'ère de la génétique*, éd. MSH, 2021 ; VAILLY Joëlle, *ADN policier*, PUF, 2024 ; SUPIOT Elsa, « Le procès pénal à l'épreuve de la génétique », Mission Droit et justice-ISJPS, juin 2017 ; SUPIOT Elsa et SIMON Anne (dir.), « Le procès pénal à l'épreuve de la génétique », *Cahiers droit, sciences & technologies* 9/2019, dossier, p. 19 et s.

encore à l'utilisation de moyens technologiques tels que la vidéotransmission[12]. A cet égard, le développement de l'intelligence artificielle, qui n'est pas directement abordé dans le rapport, mérite d'être conservé à l'esprit, en tant que l'intelligence artificielle peut « augmenter » la puissance de certaines technologies, par exemple permettre d'analyser beaucoup plus vite que ne le ferait un enquêteur les images contenues dans un téléphone portable, ou encore – mais nous voilà de nouveau à la lisière des procédures administrative et judiciaire – démultiplier la capacité de caméras de surveillance à détecter des signaux « anormaux », par exemple dans un stade[13]. Ensuite, si les NTIS présentent, notamment par rapport à la preuve par ADN, des spécificités, notamment en ce que leur terre d'élection est la criminalité grave, elles ont ceci de commun avec elle qu'elles contribuent à une réflexion aujourd'hui devenue indispensable sur la notion de « trace », dans diverses disciplines du reste[14]. En effet, comme pour l'ADN, les techniques en cause ont la particularité, notamment les données de connexion qui occupent aujourd'hui largement le devant de la scène, de provenir de l'activité des personnes suspectées elles-mêmes, ce qui ajoute à la spécificité de leur statut épistémologique. Ainsi que l'écrivent judicieusement trois auteurs : « avec la multiplication des traces numériques croît l'empire de la preuve, avec la multiplication des traces numériques accessibles à tout un chacun croît l'empire de l'enquête »[15]. La notion de traces est elle-même sujette à caution en ce qu'elle induit le soupçon d'une conduite négligente, tel le voleur qui laisse des traces sur la scène d'infraction, comparaison discutable à plusieurs égards tant les données sont moins « laissées » que collectées, ce qui conduirait à considérer que la conduite diligente imposerait alors le recours à des techniques de chiffrement, comme le dénonce une des personnes interviewées. Dans un sens voisin, contestant la thèse selon laquelle la surveillance serait devenue participative, un auteur estime qu'il ne faut pas « voir dans le fait que les citoyens concourent aux usages de ces plateformes sociales un signal d'illettrisme ou d'adhésion idéologique, mais au contraire celui d'une capture de leurs flux de communications par une architecture de la participation passant par la production de traces qui personnalisent les usages, documentent les passages et la présence dans les environnements numériques. L'ordre de priorités entre protection de la *privacy* et personnalisation de l'expérience numérique semble être alors inversé, face à ces traces dont la pérennité et les utilisations secondaires (autant à des fins commerciales que sécuritaires) échappent aux utilisateurs »[16].

---

[12] Voir LEBORNE Jérôme, « La vidéojustice : la justice pénale à l'ère de la vidéo », *Cahiers droit, sciences & technologies* 13/2021, p. 93 et s. *Adde* : *Loi n° 2023-1059 du 20 novembre 2023 d'orientation et de programmation du ministère de la Justice 2023-2027* dite « Loi justice » (article 63-3 sur l'examen médical par vidéo-transmission en cas de prolongation de la GAV) ; art. 803-5 du Code de procédure pénale pour permettre l'intervention d'un interprète par l'intermédiaire de moyens de télécommunication au cours de la garde-à-vue ou de l'audition libre d'une personne majeure ; Crim. 16 oct. 2024, n°24-84.966 sur le régime de la comparution par visioconférence du mineur devenu majeur en cours de procédure.

[13] Voir LASSALE Alice, « De "Big Brother" à "Big Data". L'avenir de la police administrative à l'ère de la vidéosurveillance intelligente », *RFDA* 2024, p. 955 et s. ; GUILLARD Antonin et BELLIVIER Florence, « JOP 2024 : ne pas gâcher la fête ? », *Revue juridique de la Sorbonne*, décembre 2023, n° 8, p. 217 et s. Sur la question spécifique des drones, ces aéronefs sans personne à bord, voir TURPIN Dominique, « Les drones, dangers pour la sécurité et pour les libertés », *RFDA* 2024, p. 923 et s.

[14] Voir, en histoire, l'article classique de GINZBURG Carlo, « Signes, traces, pistes. Racines d'un paradigme de l'indice », *Le débat*, 1980/6, p. 3 et s., discuté par exemple par MORSEL Joseph, « Le diable est-il dans les détails ? L'historien, l'indice et le cas singulier », *in* CALBERAC Yann, LAZAROTTI Olivier, LEVY Jacques, LUSSAULT Michel (dir.), *Cartes d'identités. L'espace au singulier*, Paris, Hermann, 2019, p. 123 et s.

[15] LECLERC Olivier, VERGES Étienne et VIAL Géraldine, « Preuves scientifiques et technologiques », *Cahiers Droit, Sciences & Technologies* [En ligne], 15, 2022, p. 242.

[16] CASILLI Antonio, « Quatre thèses sur la surveillance numérique de masse et la négociation privée », Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle, La documentation française, 2014, p. 424. Sur une discipline en émergence, la « traçologie » voir RIBAUX Olivier, *De la police scientifique à la traçologie. Le renseignement par la trace*, Lausanne, EPFL Press, 2023.

8.- Enfin, le travail d'enquête passe aujourd'hui nécessairement par la consultation de ces outils, en grand nombre, que sont les fichiers contenant des données nominatives, qu'ils soient détenus par des tiers à la procédure, des opérateurs de communication par exemple, ou la police elle-même. Si l'accès aux fichiers tenus par des tiers est notamment encadré par les 60-1, 77-1-1 et 99-3 du Code de procédure pénale, sous la modalité des « réquisitions », il n'en reste pas moins que leur multiplication est source de difficultés, pour les enquêteurs et les personnes concernées, qui se vérifieront pour les NTIS lorsque leur mise en œuvre passe par la consultation d'un fichier ou résulte en une information qui sera intégrée dans un fichier[17].

9.- Avec ces éléments contextuels constamment à l'esprit, les membres de l'équipe de recherche ont analysé les mesures d'enquête repérées comme « nouvelles technologies d'investigation et de surveillance » de façon parallèle d'une part lors de réunions ou de séminaires, d'autre part au moyen d'entretiens avec des acteurs de terrain.

10.- En premier lieu, outre les nombreuses séances de travail de l'équipe restreinte, qui ont émaillé la recherche, nous avons organisé cinq réunions élargies.
La première, le 31 mars 2021, a lancé la recherche en mettant en présence l'équipe au complet, c'est-à-dire, outre l'ensemble des membres de l'équipe de recherche, les divers experts qui ont accepté de nous accompagner, soit pour contribuer à l'analyse comparative, soit pour alimenter la réflexion interdisciplinaire[18].
Cette première rencontre a permis de confirmer les intuitions et hypothèses à l'origine du projet de recherche mais aussi de préciser certains points de méthode, en particulier s'agissant de l'approche comparative. Les confirmations ont concerné d'abord l'objet de la recherche, composé d'une liste de mesures d'enquête qui, pour être provisoire car susceptible d'ajouts révélés par la recherche, est suffisamment compréhensive. A ensuite été conforté le choix de partir des pratiques des acteurs pour les confronter aux catégories de l'enquête pénale et aux impératifs de la protection des droits fondamentaux. Pour ce faire, retracer la généalogie de l'introduction des mesures étudiées, en complément de l'analyse approfondie du cadre normatif (national et international) est apparu pertinent. Quant aux précisions, elles intéressent la dimension comparative du projet. Si, dans un premier temps, il avait été question de procéder à une analyse vraiment comparative du recours aux NTIS dans quelques pays choisis, les spécialistes des droits étrangers ont très vite attiré notre attention sur le fait qu'une étude de droit comparé serait beaucoup trop ambitieuse dans le cadre temporel et financier fixé pour la recherche. En revanche, le déplacement de la comparaison entre droits nationaux vers la dimension européenne devait, selon nos interlocuteurs, s'avérer fructueuse, ce qui a en effet été le cas. Sur un certain nombre de points, en effet, par exemple les données de connexion, la jurisprudence européenne permet une réflexion comparée de la façon dont les différents États procèdent à sa réception.

Une seconde réunion de travail de l'équipe de recherche a eu lieu le 28 juin 2021 afin de préciser la répartition des tâches, la méthode de travail et le calendrier. Elle a permis d'attribuer à chaque

---

[17] Voir MORNET Alice, *Les fichiers pénaux de l'Union européenne. Contribution à l'étude de la protection des données à caractère personnel*, Mare&Martin, 2023 ; CHAUVELOT Aurore, « Le contrôle, par la chambre de l'instruction, de l'accès des personnels habilités aux fichiers de police judiciaire », *RSC* 2024 p.407 ; à propos du fichier de traitement des antécédents judiciaires, voir CNIL, *Délibération de la formation restreinte n°SAN-2024-017 du 17 octobre 2024 concernant le ministère de l'Intérieur et des Outre-Mer et le ministère de la Justice*, 6 novembre 2024.

[18] Arié Alimi, avocat ; Jérôme Barlatier, lieutenant-Colonel de Gendarmerie ; Daniele Caianiello, professeur à l'Université de Bologne ; Vanessa Franssen, professeure à l'Université de Liège ; Bernard Harcourt, professeur à l'Université de Columbia, directeur d'études à l'EHESS ; Gavin Robinson, Assistant Professor, Université d'Utrecht ; Benjamin Vogel, Senior Researcher, Max Planck Institute for the Study of Crime, Security and Law.

membre de l'équipe l'étude d'une mesure d'enquête[19], selon un canevas commun discuté lors de la réunion[20] et d'identifier des référents de droit étranger pour les éclairages de droit étranger/comparé que des recherches ultérieures ne manqueront sans doute pas d'apporter.
La troisième réunion de l'équipe de recherche organisée le 18 octobre 2021 visait à confronter les résultats des études réalisées et à préparer la phase d'entretiens par l'identification des acteurs (profils et contacts) et la confection de questionnaires[21]. Elle a permis d'illustrer la très grande hétérogénéité des mesures étudiées tout en révélant des besoins et questions transverses ou communes : ainsi tout d'abord du besoin de proposer une histoire problématisée de ces mesures (laquelle manque doublement dans la mesure où elle ne semble pas avoir été réalisée alors qu'elle est nécessaire à la compréhension de la construction des dispositifs procéduraux actuels) ; ainsi, ensuite, de la question des usages de ces mesures (présence ou absence de données statistiques, effets de la mesure -attendus, connus, induits-, fréquence -usages routiniers, ponctuels ou inexistants-, coûts/économie de la mesure, variabilité selon les acteurs) et de leur articulation (cumuls, obsolescence-remplacement) ; ainsi enfin de leur compatibilité avec les droits fondamentaux (compatibilité envisagée lors de la mise en place de la mesure, appréciée par un organe ou une juridiction de contrôle (Conseil constitutionnel, Cour européenne des droits de l'homme, Cour de justice de l'Union européenne), critères de gravité de l'atteinte, conditions de légitimité de l'atteinte, en particulier proportionnalité). Au cours de cette réunion, la composition de l'équipe de recherche s'est modifiée, avec le départ de H. Farraj vers d'autres horizons et l'arrivée de M. Audibert et A. Guillard, tous deux doctorants[22] au CDPC et travaillant sur ces questions.
A l'issue de la réunion, il est convenu que chaque membre complète l'étude de « sa » mesure et insère une fiche synthétique de présentation de celle-ci permettant de faciliter l'analyse comparée des mesures, fournisse une liste des services, structures ou personnes à interviewer et propose des questions dans la perspective d'un entretien mené suivant la méthode de l'entretien en sciences sociales (questions ouvertes sans réponse induite).
Un questionnaire type, susceptible d'ajustements selon le profil de la personne interrogée, a ensuite été élaboré par F. Bellivier, J. Tricot et V. Giannoulis[23].
Le 3 avril 2023 nous avons organisé une journée d'études, à l'Université Paris Nanterre, afin de discuter des « réceptions comparées de la jurisprudence européenne sur la conservation et l'accès aux données en procédure pénale »[24] avec cinq collègues étrangers, deux français et deux magistrats français. Cette séance fut décisive non seulement pour observer les complexités infinies de l'application de la jurisprudence européenne dans d'autres États que la France, qui permettent de mettre en perspective le « dialogue » qui s'est instauré entre la CJUE, la Cour de cassation française et le Conseil d'État français en matière de données de connexion, mais

[19] Réquisition de documents (M. Lassalle) ; Injonction de donner un mot de passe (M. Lassalle) ; Géolocalisation (D. Sidhoum-Rahal) ; Perquisition informatique (S. Sontag) ; Saisie de données informatiques stockées (J. Tricot) ; Interception des correspondances émises par la voie des communications électroniques (E. Cervellera) ; Fixation d'images de certains lieux et véhicules (H. Farraj) ; Sonorisation de certains lieux et véhicules (F.E. Rollet) ; Conservation rapide de données informatiques stockées (V. Giannoulis) ; Captation des données informatiques (V. Sizaire) ; Accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique (A. Yevtihidis) ; Infiltration numérique (S. Malliarakis) ; IMSI-Catcher (F. Bellivier).
[20] 1.- Bases légales 2.- Historique de l'introduction de la mesure en droit français 3.- Moteurs ou facteurs de l'introduction de la mesure 4.- Traits généraux 5.- Régimes et modes de justification 6.- Mise en œuvre 7.- Bibliographie.
[21] En équipe élargie, la réunion avait pour but de faire un tour de table des contributions mesure par mesure, de déterminer les personnes à interviewer et présenter l'actualité des NTIS.
[22] Matthieu Audibert a depuis soutenu sa thèse : *Le recueil de la preuve numérique. Enjeux et perspectives en procédure pénale*, Université Paris Nanterre, thèse soutenue le 4 novembre 2024.
[23] Voir annexe « Questionnaire type ».
[24] Voir annexe « Journées d'études »

également pour orienter notre recherche sur les liens entre « données pénales »[25] et données personnelles.
Enfin, le 19 janvier 2024, nous avons encore changé de format : cette fois, les trois rédacteurs du rapport ont présenté les hypothèses principales du travail en cours de rédaction et les auteurs de la cartographie le résultat de leur labeur à un public composé des acteurs de terrain interrogés au cours de la recherche mais aussi de trois observateurs extérieurs[26]. Intitulée « Que font les NTIS à l'enquête pénale ? », cette journée visait à approfondir l'hypothèse selon laquelle la procédure pénale et, plus précisément l'enquête, est affectée, selon diverses modalités et à divers égards, par elles.

11.- En second lieu, et parallèlement, l'approche empirique a consisté à interroger des acteurs de terrain selon une méthodologie qui sera présentée dans la première partie.
A son tour, comme l'approche normative, l'approche empirique a confirmé l'extrême diversité et complexité du paysage « institutionnel » et opérationnel au sein duquel se déploient les mesures étudiées. Et si le vocabulaire appelait un glossaire, le paysage a conduit à s'essayer à un exercice peu commun pour les juristes : réaliser une cartographie des acteurs impliqués dans les procédures mobilisant les nouvelles technologies d'investigation et de surveillance, tant ceux relevant du renseignement que ceux relevant de la procédure pénale ou ceux encore qui interviennent à un titre ou un autre pour les besoins du renseignement ou de la procédure pénale.
Que toutes les personnes qui ont participé à cette recherche, selon les diverses modalités décrites, reçoivent l'expression de notre gratitude pour nous avoir aidé à constituer un objet de recherche, établir un réseau, nous former, éprouver des méthodes !

12.- Pour aborder cet objet de prime abord fuyant que sont les NTIS, les chercheurs de l'équipe se sont tout d'abord fixé des objectifs modestes : saisir les ressorts de la construction de cet ensemble dans ce maquis de textes d'origine et de nature diverses qu'est devenue la procédure pénale ; interroger les acteurs qui, tout au long de la procédure qui fait vivre les textes, s'y confrontent ; mesurer les innovations et les continuités avec les techniques plus traditionnelles d'enquête ; apprécier une éventuelle distorsion entre les NTIS et les grands principes qui gouvernent la procédure pénale. Au bout du compte, il s'avère que les usages comme les normes relatifs aux nouvelles technologies d'investigation et de surveillance sont à la fois révélateurs et moteurs de mutations profondes qui affectent l'enquête pénale depuis une trentaine d'années, qui plus est dans un monde pris dans le tourbillon de la production, de la conservation et de l'utilisation des « données » (*data*). Au soutien de cette démonstration, une construction du propos tel une fusée à trois étages (usages, normes, perspectives) est apparue cohérente.
Tout d'abord, pensant au lecteur qui trouverait la matière trop aride, nous avons eu à cœur d'adoucir l'entrée dans l'univers des NTIS, en commençant par une analyse au plus près des pratiques des acteurs confrontés à ces techniques, qu'ils les fabriquent, s'en servent (parfois avant que la loi ne vienne les réglementer), en contrôlent l'usage ou les contestent. Si l'enquête de terrain révèle une forme d'évidence de l'usage des NTIS, d'emblée présentées comme connues et efficaces, l'approfondissement du questionnement fait apparaître, y compris chez ceux qui sont confrontés quotidiennement à ces mesures, des doutes de divers ordres, ce qui contribue sans doute à ce que les NTIS, du fait même de leur haute technicité, servent à souder une communauté professionnelle (*partie 1*).
La perplexité des acteurs se comprend fort bien si l'on examine la généalogie et les régimes des mesures NTIS. L'apparition des NTIS comme l'évolution du régime de chacune d'elles ont eu lieu de manière pour ainsi dire spontanée au rythme de l'essor des technologies numériques

[25] *Infra*, partie III.
[26] Voir annexe « Journées d'études ».

perçues et conçues à la fois en tant que menaces contre lesquelles il fallait lutter et en tant qu'outils qu'il fallait absolument intégrer à la procédure pénale. A cet égard, la consultation des principaux manuels de procédure pénale récents qui, tous, intègrent les NTIS, montre bien qu'à la suite de la loi, la doctrine absorbe la nouveauté sans véritablement s'interroger sur les effets de continuité ou de rupture qu'elle induit – tout au plus les adjectifs « intrusif »[27] au sens de ce qui porte atteinte à la vie privée ou « dissimulé »[28] seront-t-ils utilisés ou bien l'accent sera-t-il mis sur le caractère spécial des preuves obtenues par ces techniques[29]. Au-delà de cette conscience partagée de ce que les NTIS font partie du paysage tout en y occupant une place particulière en raison de leur technicité – *a fortiori* pour les « autres techniques spéciales d'enquête » –, l'effort doctrinal porte surtout sur le choix du cadre préexistant dans lequel les auteurs les intègrent : certains évoquent telles techniques, la perquisition ou la réquisition informatique par exemple, dans le même paragraphe que leurs homologues physiques, d'autres les distinguent ; la plupart traitent des NTIS au titre des actes d'enquête, eux-mêmes intégrés dans un développement sur les pouvoirs de la police ou dans un autre sur l'information, et les répartissent dans les passages relatifs à l'enquête préliminaire ou de flagrance ou à l'instruction, d'autres mènent une analyse qui transcende les types d'enquête (y inclus l'instruction), ne distinguant que là où il faut distinguer, d'autres encore insistent sur la double finalité des mesures – administrative ou judiciaire – , d'autres, enfin, minoritaires, évoquent les NTIS au titre des principes régissant la preuve, notamment la loyauté. Ce dernier parti serait sans doute le plus convaincant si le Code de procédure pénale comportait des dispositions générales relatives à la preuve et, plus encore, à la preuve scientifique[30]. Compte tenu de cette lacune, on comprend bien pourquoi la majorité des présentations des NTIS dans les ouvrages de doctrine reflète le fait que chaque intervention du législateur pour valider une mesure déjà employée en pratique a eu un caractère ponctuel et qu'aucune n'a procédé d'une vision d'ensemble, à la notable exception près de l'introduction en droit français des (autres) « techniques spéciales d'enquête ». Cette catégorie est paradoxale puisqu'elle est relativement homogène tout en étant résiduelle (« autres ») et son régime contraste avec la consécration disparate des autres mesures NTIS insérées dans les cadres juridiques préexistants de l'enquête préliminaire, de flagrance ou de l'instruction sans véritable articulation et, notamment sans réflexion sur le lien entre les mesures numériques qui miment leur double du monde réel et les mesures numériques dès l'origine (*digital native*) (*partie 2*). Les pratiques et les mots des acteurs comme le contexte de leur encadrement juridique montrent combien les technologies d'investigation et de surveillance sont autant les témoins que la source des transformations de l'enquête pénale : elles conduisent à l'adaptation des pratiques d'enquête tout en mettant en lumière une perturbation des principes de l'enquête. Il convient toutefois de s'efforcer de ne pas en rester au constat de la déstabilisation des repères mais de tenter de l'expliquer en examinant le phénomène de « mise en données »[31] du monde. La rencontre du droit des données personnelles et de la procédure pénale fait ainsi advenir un nouvel objet : la donnée numérique pénale, qui pourrait permettre de faire baisser certaines des tensions affectant le champ fuyant des NTIS (*partie 3*).

---

[27] Voir PARIZOT Raphaële, *Procédure pénale*, Lefebvre Dalloz, 2024, p. 253, n° 330, p. 271, n° 351

[28] VERNY Edouard, *Procédure pénale*, Lefebvre Dalloz, 9ème éd., 2024, p. 312, n° 468.

[29] Voir un manuel non de procédure pénale mais de droit de la preuve : VERGES Etienne, LECLERC Olivier, VIAL Géraldine, *Droit de la preuve*, PUF, 2ème éd., 2022, troisième partie, p. 495 et s., n° 442 et s.

[30] Voir DEMARCHI Jean-Raphaël, *Les preuves scientifiques et le procès pénal*, LGDJ, 2012.

[31] Conseil d'État, *Le numérique et les droits fondamentaux*, *op.cit*.

Première partie : Usages

13.- Si notre méthode a d'abord été normative (centrée sur la généalogie des textes et leur interprétation), elle a également vite et parallèlement revêtu une dimension empirique en se confrontant à la façon dont les acteurs s'emparent ou non de ces techniques et du discours qu'ils produisent sur elles.

S'agissant de la partie empirique, nous nous sommes entretenus avec neuf personnes (ou dix si l'on compte un entretien réalisé à l'improviste et à la volée avec le collègue d'un de nos enquêtés) : un policier, un officier de police judiciaire investigateur en cybercriminalité, un gendarme spécialisé en NTIS, cinq magistrats (dont l'une qui a été avocate pendant de longues années), deux avocats, un directeur d'une entreprise de sécurité, un officier de liaison cybergendarmerie, soit un échantillon fidèle à la palette des acteurs intervenant dans la procédure pénale et utilisant des NTIS.
La forme des entretiens a varié : la plupart ont eu lieu sur le lieu de travail de l'enquêté mais occasionnellement à distance, deux fois dans un café ; l'entretien était mené par au moins deux membres de l'équipe, parfois plus (jusqu'à quatre). Les entretiens ont duré en moyenne deux heures.
Quelques jours avant le rendez-vous, l'enquêté(e) recevait un questionnaire-type que nous avions décliné en fonction de sa qualité et de ses fonctions et que nous adaptions au cours de l'entretien. Tantôt l'entretien était enregistré, tantôt non. Les entretiens ont tous été transcrits mais pour des motifs de confidentialité nous n'avons pas fait figurer les transcriptions en annexe. Pour ces mêmes motifs, et en accord avec les enquêtés, leurs propos sont repris mais ne leur sont pas attribués nominativement. Seul a été mentionné le métier de chaque enquêté car il permet de situer le propos[32]. Afin de compléter les entretiens, certains des membres de l'équipe ont suivi une formation d'une matinée sur l'investigation numérique dispensée le 13 décembre 2023, organisée en distanciel par le « Printemps de l'investigation numérique et la JFC pénale CNEJITA [Journée de formation continue pénale de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées] »[33]. Tous nos enquêtés nous ont dit qu'ils se tenaient à notre disposition pour répondre à d'autres questions qui nous viendraient par la suite. Ainsi pouvons-nous dire qu'au terme de ces quatre années de travail ou presque, nous avons créé une petite communauté de personnes soudées autour de l'objet NTIS, qu'il s'agisse des acteurs du terrain ou des universitaires, heureux de dialoguer entre eux lors des séminaires que nous avons organisés et désireux, semble-t-il, de pouvoir prolonger les réflexions élaborées ensemble.

14.- Outre les séminaires et les entretiens, notre équipe, soit restreinte, soit élargie (avec les auteurs de la cartographie), s'est très souvent réunie, à distance ou en présence, pour évoquer les avancées comme les lacunes du travail et chacun a complété ses réflexions par quelques

---

[32] Ce qui conduit aussi à désigner de manière indistincte policiers et gendarmes par « enquêteur ».
[33] Le programme était le suivant et donnera aisément une idée de la technicité du domaine :
-Déchiffrement de *Keepsafe*-aperçu de *Yahoo Takeout*, par Ludovic Ravaux, expert ;
-Scènes de crimes numériques par Frédéric Bouquet, expert ;
-Introduction au reverse engineering (invité extérieur) ;
-Signature de l'agent sur dispositif *Apple* via *Rasberry* et *Screenshots Android*, par Ildut de Parcevaux, expert ;
-Sources d'information *Forensic* à partager (partie 1), par Christelle Gloecker, expert.

coups de téléphone ou réunions à distance avec des acteurs du terrain. Tous les documents ont été partagés sur un espace numérique sécurisé et accessible aux trois rédacteurs du rapport.

15.- Centrée sur les entretiens fournis que nous avons eus avec les acteurs interrogés, le cas échéant complétés par des références à des articles qui étoffaient judicieusement telle ou telle remarque, cette partie consacrée aux acteurs se veut au plus près de ce qui nous a été dit et qui est, dès lors, souvent cité entre guillemets car il nous est apparu que tout ce qui était dit avait pour l'analyse une valeur en soi, venant de la part de professionnels chevronnés soucieux de réfléchir à leur travail et, précisément, à la façon dont ils appréhendent les NTIS (à la fois l'expression, la notion et la chose). En ce sens, cette présentation ne prétend évidemment pas à l'exhaustivité – irréalisable – ni même à la représentativité : sans doute d'autres acteurs auraient-ils dit d'autres choses et il se peut que notre recherche produise un effet de loupe, grossissant certaines observations, par exemple l'usage qui nous est apparu comme routinier de certaines NTIS. Il se trouve toutefois que, sans doute parce que les personnes que nous avons rencontrées avaient une sensibilité à ces questions, une expérience et l'envie de la partager, les échanges que nous avons eus avec elles ont grandement stimulé notre analyse des mesures regroupées sous l'expression « nouvelles technologies d'investigation et de surveillance ».
En outre, en eux-mêmes et indépendamment de leur apport à nos réflexions, les entretiens se sont révélés une mine d'informations et c'est la raison pour laquelle une partie entière leur est consacrée. Commencer par là en restant au plus près des formules employées par nos interlocuteurs permet à la fois de les remercier du temps qu'ils nous ont consacré, de pénétrer une matière aride et technique en l'incarnant et de mettre en lumière une autre forme de complexité que celle des textes et des grands principes qui gouvernent la matière. Nous avons toutefois anonymisé les propos car c'était une demande générale. Le masculin (« enquêté ») est évidemment générique. Restituer les mots de façon fidèle n'impliquait toutefois pas de ne pas ranger les idées selon l'ordre qui nous a paru le plus cohérent et qui découle du questionnaire soumis aux acteurs. Tout d'abord, il s'avère que ceux qui pratiquent quotidiennement les NTIS n'appréhendent pas cet ensemble de techniques avec certitude, qu'il s'agisse des mots mêmes ou des actes qui relèvent de la catégorie (*section 1*). Ensuite, les personnes interrogées sont allées plus loin en exprimant des points de vue parfois convergents, parfois divergents sur la mesure des mesures mises en œuvre au titre des NTIS (*section 2*). Enfin les NTIS se sont révélées être bien plus qu'une modalité d'obtention des preuves dans une enquête pénale, à savoir un facteur de construction d'une communauté professionnelle (*section 3*). Tous les propos, réflexions, interrogations émanant des enquêtés sont rendus plus intelligibles par la cartographie insérée entre les première et deuxième parties du rapport et qui a pour finalité de visualiser les différents acteurs impliqués dans le recueil et dans l'administration du renseignement et de la preuve numériques. La carte figure le processus d'orientation, de collecte, d'analyse et de diffusion des informations obtenues tant par les services de renseignement que par la police judiciaire. La place de chaque acteur interrogé dans le cadre de l'enquête empirique peut être ainsi appréhendée d'un coup d'œil.

Section 1 : L'usage des NTIS, des mots aux actes

16.- Nous avons jugé bon de commencer l'entretien, après les présentations d'usage, par les trois questions suivantes : « Qu'évoque pour vous la formule « technologies ou techniques d'investigation et de surveillance ?», « Avez-vous / êtes-vous amené (e) à faire usage de ces techniques ou technologies ? », « La catégorie « technique spéciale d'enquête » est-elle ou non opératoire à vos yeux ? ».

Il apparaît que si l'expression « nouvelles technologies d'investigation et de surveillance », directement empruntée au texte de l'appel à projets, n'est pas utilisée en tant que telle par les praticiens (et l'acronyme encore moins, tant il est difficile à prononcer), elle leur évoque toujours quelque chose. Les acteurs ont leur vocabulaire et leurs définitions, y compris des techniques spéciales d'enquête (TSE) (*§1*), même si les actes entrant dans l'ensemble « NTIS » sont décrits plutôt au moyen d'une énumération ouverte que de façon systématique (*§2*).

§1.- Les mots et les définitions

17.- Parfois, les enquêtés fournissent une définition abstraite quitte à ce qu'elle soit redondante (« l'emploi des nouvelles technologies dans le cadre de la recherche d'une manifestation de la vérité sur une infraction », enquêté, enquêteur spécialisé en nouvelles technologies, ci-après NT) ou qu'elle caractérise la mesure NTIS par son régime (c'est ce qui « nécessite une autorisation particulière et un contrôle supplémentaire, ce qui sort du cadre classique, par exemple la géolocalisation, tout ce qui n'est pas classique », enquêtés juges des libertés et de la détention, ci-après JLD). Un enquêté magistrat définit même la technique comme « ce qui fait le pont entre le renseignement et le judiciaire ». Des enquêtés JLD insistent sur le particularisme en ces termes : « C'est tout ce qui nécessite un savoir-faire particulier. Dans notre vocabulaire interne, on parle d'ordonnances particulières ». Toutefois les acteurs ont, la plupart du temps, précisé que la définition qu'ils donnaient, s'ils en donnaient, était située. Ainsi, à propos des techniques spéciales d'enquête, sous-catégorie des NTIS, l'un d'entre eux s'exprime en ces termes : « Compte tenu de mon expérience cela recouvre une sous-catégorie liée au secret de la défense nationale et évoque le lien entre le renseignement et la procédure pénale, ainsi que la porosité entre le renseignement et la procédure pénale » ; c'est une « passerelle » (enquêté avocat). Un autre enquêté : « Ce sont les personnes en charge du pilotage qui utilisent l'expression "TSE" (par contamination des interlocuteurs). Les techniciens, eux, c'est-à-dire 90 % des personnes ne l'utilisent pas » (spécialiste des NT dans une entreprise privée).
Majoritairement, toutefois, les acteurs rencontrés n'ont pas pu définir de façon générique l'ensemble « NTIS » mais ont procédé par énumération. Un enquêté, lui, préfère parler de « matériel numérique » qu'il définit ainsi : « tout ce qui contient des puces, donc ça peut être un ordinateur, un téléphone, un GPS, une clé USB, tout ce qui contient du stockage numérique » (enquêté enquêteur spécialiste en NT).

§2.- Les actes : une énumération ouverte et opératoire

18.- On en vient rapidement aux actes car, selon un enquêté JLD,

> « la formule "technologies ou techniques d'investigation et de surveillance" ne désigne pas un ensemble cohérent qui peut être défini matériellement. Il y a des règles spécifiques mais aucun cadre spécifique. Donc ce n'est pas l'enquête qui est spécifique mais les actes. La spécificité vient par petits bouts et non pas d'une cohérence d'ensemble ».

A la question de savoir quels actes correspondent aux NTIS, l'un des enquêtés répond : « conservation, géolocalisation, TSE en lien avec le secret défense, intrusion dans un terminal informatique, sonorisation des lieux » (enquêté avocat). Un autre nous parle d'emblée de l'accès aux correspondances stockées (enquêté magistrat). Un autre s'exprime négativement : « La sonorisation est située hors NTIS » selon lui (enquêté avocat). Mais ce qui est remarquable est que spontanément, les personnes interrogées ne déterminent pas de façon nette les actes qu'elles pratiquent et qui reposent sur des nouvelles technologies d'investigation et de

surveillance. C'est plutôt lorsque nous leur demandions si elles pratiquaient telle mesure, puis telle autre qu'elles répondaient par l'affirmative ou la négative. Ainsi un enquêté magistrat nous a-t-il présenté la géolocalisation en temps réel comme très fréquente pour savoir où se trouvent les mis en cause, connaître leurs pérégrinations bien que la jurisprudence se soit durcie[34] ; selon le même interlocuteur l'article 706-95-1 CPP (accès aux correspondances stockées par la voie des communications électroniques) est régulièrement utilisé pour accéder à des serveurs contenant de la matière probante ; les écoutes téléphoniques, selon le même interlocuteur, c'est une « tarte à la crème », « très balisée ». En revanche, la sonorisation et la captation d'images sont « ultra liberticides », selon le même enquêté, et donc utilisées parcimonieusement, d'autant que le dispositif est compliqué à installer et désinstaller et qu'il faut des enquêteurs formés ; plus rarement il sera fait usage d'un pseudonyme pour la vente d'armes sur le *darknet* ou la pédopornographie et ce même enquêté a vu une fois une infiltration pour des trafics de cigarettes.
Un autre enquêté insiste sur la fréquence du recours aux NTIS : « oui, on en fait usage tous les jours. Surtout des perquisitions sans assentiment, des interceptions de correspondances aussi et parfois des sonorisations » (enquêtés JLD).

19.- L'énumération devenait alors opératoire : elle portait sur les techniques utilisées parce qu'elles marchent. Dès lors qu'elle n'était pas spontanée, l'énumération n'était en général de prime abord pas hiérarchisée, et ce n'est qu'après coup, au titre de l'utilité (sur laquelle voir *infra*), qu'un ordre pouvait se dessiner.
Ainsi, pour l'accès aux correspondances stockées, un enquêté spécialisé en NT estime qu'elle

> « n'est pas très utile (sauf terrorisme par exemple) car il faut l'autorisation de l'opérateur. Il est plus simple de se procurer le téléphone. Et de toute façon, les mecs qui font du terrorisme, les 3/4 du temps, essaient de ne pas utiliser des mails. Puis, même s'ils utilisent des mails, ils utilisent des mails sécurisés ou cryptés ou autres qui sont basés en Russie ou ailleurs dans d'autres pays qui ne communiquent pas ; donc de toute façon ça va être compliqué ».

L'accès aux données de connexion est « très souvent » utilisé « notamment concernant les campagnes d'e-mails frauduleux mais on est dépendant du bon vouloir des opérateurs » (même enquêté).

Un enquêté avocat prédit qu'« avec la fin de l'âge d'or des dossiers montés sur écoutes » (parce qu'il existe de nombreuses techniques qui permettent d'échapper aux écoutes), « l'avenir c'est la captation de données », bien plus facile que l'interception téléphonique et qui présente l'avantage de ne pas laisser de trace.
« La conservation s'inscrit dans la captation », selon ce même enquêté car aujourd'hui le contenu serait moins intéressant que les données de connexion ou de trafic (ce qui confirme en l'amplifiant la formule d'Edward Snowden, citée en troisième partie du rapport : « *Megadata in aggregate is content* »[35] mais Snowden poursuit : « *It tells a story about you which is made up of facts, but is not necessarily true* »[36]).

---

[34] Crim., 9 mai 2018, n° 17-86.558 : les opérations de géolocalisation en temps réel, réalisées dans le cadre fixé par les articles 230-32 et s. du Code de procédure pénale, doivent être autorisées par écrit par le magistrat compétent, avant la mise en place du dispositif.
[35] « Les données massives agrégées, c'est du contenu », traduction libre.
[36] « Elles racontent à votre propos une histoire qui est faite de faits mais qui n'est pas nécessairement vraie », traduction libre.

L'*IMSI-catcher* a pu être utilisé dans une affaire mais en vain car il faut que les personnes surveillées utilisent leur téléphone portable (enquêté avocat) ; un autre enquêté, OPJ, dit que l'*IMSI-Catcher* est encore « peu connu ».
La « sonorisation » est située hors NTIS selon un enquêté avocat car elle présente des risques non seulement pour l'agent (« se faire détroncher », c'est-à-dire démasquer, selon l'argot policier, employé ici par un enquêté JLD) mais aussi pour la procédure du fait d'un échec technique ou de la découverte du dispositif par la cible. Mais c'est utile d'après lui car les notes vocales ne laissent pas de traces et ne peuvent donc pas être captées. Selon cet enquêté avocat, on « redécouvre des actes anciens : filature, pose de caméras, sonorisation ». Toutefois, « une sonorisation est plus difficile à mettre en œuvre qu'une écoute, puisqu'elle implique un risque pour l'enquêteur qui doit se déplacer sur les lieux pour installer le dispositif ; en revanche, la sonorisation est plus facile à appliquer techniquement qu'une fixation d'images » (enquêtés JLD). La contrainte technique explique aussi que « dans l'ensemble, il vaut mieux travailler directement sur l'appareil qu'à distance car cela permet d'accéder aux données avant le cryptage quand elles sont encore en clair » (enquêté enquêteur spécialiste en NT). Ou encore : « l'accès aux données se fait plutôt par la voie de la perquisition. Les enquêteurs saisissent l'ordinateur et extraient les données par eux-mêmes plutôt que de demander l'accès par l'intermédiaire des opérateurs privés » (enquêtés JLD).

Section 2 : Une question de mesure(s)

20.- Une fois l'objet identifié – plus ou moins –, nous sommes entrés dans le vif du sujet en interrogeant les acteurs sur leurs pratiques ou, plus exactement, en les invitant à une réflexivité sur celles-ci qui visait à nous permettre de prendre la mesure des mesures en question : mesure de la nouveauté inscrite dans leur intitulé (*§1*), mesure de l'utilité qu'elles procurent (*§2*), mesure des limites rencontrées dans la mise en œuvre des NTIS (*§3*), mesure d'une éventuelle démesure ou disproportion dans le recours aux preuves issues des NTIS (*§4*).

§1.- Mesure de la nouveauté

21.- La nouveauté des « nouvelles technologies d'information et de surveillance » doit être relativisée. D'un côté, certains la contestent, d'une part, en proposant un tournant qui date déjà (« les mesures ne sont pas nouvelles » selon un enquêté officier de liaison ; « ça fait plus de vingt ans qu'elles sont là, c'est juste qu'on a mis du temps, même les gens en général ont mis du temps à les accepter » dit un spécialisé en NT ; « les fadettes et le bornage sont utilisées depuis très longtemps », d'après des enquêtés JLD) ou en précisant lesquelles sont vraiment nouvelles (« la conservation de données » selon un enquêté avocat) (*I*), d'autre part, en soulignant une parenté entre monde réel et monde virtuel (*II*). D'un autre côté, la nouveauté semble provenir du caractère toujours évolutif des mesures (*III*).

I.- Le tournant

22.- Interrogés sur les dates ou moment clés qui ont conduit à l'utilisation des NTIS, les acteurs évoquent en général les attentats de 2015, d'une part, et la généralisation du *smartphone* d'autre part. Ainsi un enquêté avocat évoque-t-il un double tournant qu'il date de 2012-2015 : l'un « formel » avec la lutte contre le terrorisme qui se traduit par « l'évolution des textes et

l'évolution des pratiques avec un caractère désinhibé », l'autre « informel : la pratique – l'usage des mesures NTIS à partir de 2012 ». Un autre évoque une autre origine : « Ce sont les gendarmes qui, dans le cadre des infractions financières, ont les premiers été confrontés au problème de savoir comment collecter des preuves dispersées dans des ordinateurs » (enquêté investigateur spécialisé en NT). Quant aux effets de la généralisation de l'usage du *smartphone*, elle est évoquée en ces termes :

> « tout est dans les téléphones » (enquêtés JLD) ;
>
> « si ça vous intéresse, faites les archives de vos réseaux sociaux, vos comptes réseaux sociaux, regardez à l'intérieur avec un regard critique le nombre de données à l'intérieur de ces trucs-là, c'est effarant ; ces éléments replacés dans un contexte judiciaire c'est une mine d'or » (enquêté investigateur spécialisé en NT).

Ou encore : « L'avènement des technologies a fait que ça s'est énormément démocratisé et tout un chacun enfin voilà je vais prendre l'exemple ici vous avez tous un téléphone smartphone qui est connecté qui interagit au quotidien avec différents espaces différents serveurs dédiés » (enquêté investigateur spécialisé en NT), le même enquêté utilisant cette formule frappante : « Les gens c'est des fantômes qui m'accompagnent », au sens où les personnes sont dans leur téléphone.

Dans la même veine, le rapport du Sénat consacré aux modalités d'investigation recourant aux données de connexion dans le cadre des enquêtes pénales évoque, lui, une « dépendance aux données de connexion »[37].

II.- Les NTIS entre monde réel et monde virtuel

23.- La nouveauté provient du fait que les technologies en question ont partie liée avec l'informatique et numérique, donc l'immatériel (elles produisent des données, elles passent par des ordinateurs ou des portables ou même maintenant le *cloud* ou l'intelligence artificielle). Toutefois, certaines des NTIS peuvent être qualifiées de « natives » (une géolocalisation par exemple), d'autres imitent le monde réel (une perquisition informatique par rapport à une perquisition dans un domicile par exemple). Un des enquêtés s'est montré loquace sur ce dernier point, utilisant le monde réel pour expliquer le monde numérique : une enquête informatique, c'est

> « une perquisition qu'on fait dans un disque dur, si on peut faire le parallèle. On va vraiment fouiller, parce qu'il faut savoir qu'un disque dur – là j'en ai encore un actuellement qui tourne – c'est minimum 500 000 fichiers. Donc, il faut vraiment fouiller, il faut savoir où aller chercher. Mais, après c'est comme si vous faites une perquisition chez quelqu'un : vous ne savez pas comment il range ses affaires, comment il range ce truc, ça, il faut chercher » (enquêté spécialisé en NT).

Le même s'exprime ainsi :

> « En fait, lors d'une perquisition c'est le même principe : c'est qu'effectivement vous êtes sur l'ordinateur, la page Facebook est ouverte, son Google drive est ouvert où toutes ses données sont dessus, oui c'est ouvert vous pouvez y accéder ; si ce n'est pas ouvert, c'est un autre lieu, c'est comme si c'était un autre lieu et vous n'y êtes pas directement ; vous avez besoin d'utiliser des codes » ;
>
> « Si c'est le code qui permet de déverrouiller l'ordinateur, ça ne pose aucun problème, parce que c'est du physique, c'est directement là. C'est comme si on prenait la clé de l'appartement avant d'aller en perquisition. Par contre,

[37] CANAYER Agnès, BONNECARRERE Philippe, *Rapport Sénat n° 110*, 15 novembre 2023, pp. 36-37.

effectivement si c'est du Facebook ou autre, je pense qu'il faudra au moins demander de l'aide au magistrat. C'est lui qui prendra la décision ».

La différence entre le monde matériel et immatériel est également nuancée lorsque le même acteur explique : « ce n'est pas parce que c'est de l'immatériel [le *cloud*] qu'il ne faut pas à un moment donné aller récupérer ce qui est stocké à distance sur des serveurs ».
Reste que les deux mondes sont différents : « Une perquisition c'est limité dans l'espace et dans le temps. Je suis chez vous, je vais faire ça chez vous, pas perquisitionner chez le voisin. En revanche, en perquisition informatique, je peux récupérer des données dont je ne sais pas où elles sont localisées » (enquêté investigateur spécialisé en NT).

24.- L'analogie n'a pas que des vertus pédagogiques, elle est également utilisée dans la littérature spécialisée pour déterminer le régime applicable. Commentant un arrêt sur la vidéosurveillance, un magistrat écrit : « La vidéosurveillance n'est finalement que le remplacement d'un œil humain, que ce soit ou non celui d'un enquêteur, par un œil électronique. La jurisprudence estime que l'autorisation du propriétaire suffit pour que l'enquêteur intervienne dans les parties communes et procède à des constatations visuelles (Crim. 8 août 2018). Par ailleurs, ont été validées des réquisitions en vue d'accéder en permanence aux parties communes d'un immeuble, sans qu'il soit nécessaire de requérir le bailleur chaque fois que les développements d'une enquête amènent les enquêteurs à devoir pénétrer dans ces lieux (Crim. 12 avr. 2023) »[38]. A propos de la géolocalisation par activation à distance d'un appareil électronique, un auteur s'interroge : « [s]'agit-il d'une adaptation aux évolutions technologiques ou d'une transformation profonde des moyens d'enquête ? »[39]. Enfin, évoquant l'activité de la 13ème chambre du TJ de Paris, son coordonnateur observe : « De manière générale, on peut dire qu'il y a deux types de dossier qui sont jugés par la chambre, les escroqueries et les affaires de cybercriminalité *stricto sensu*. Les premières se font de plus en plus *via* internet. Par exemple, les escroqueries au faux investissement se font uniquement sur internet, alors qu'il y a vingt ans, cela pouvait reposer sur des envois de courrier papier ou seulement au téléphone. En revanche, il y a des dossiers qui se passent exclusivement dans le numérique, que ce soit des affaires de piratage ou d'attaques en déni de service [[40]]. Les magistrats doivent se mettre à jour pour comprendre ces univers-là. Il faut connaître ce qu'est la "blockchain", l'environnement informatique des entreprises, les pares-feux ou encore les virus ». A propos d'un dossier en particulier, il décrit ainsi les liens entre monde réel et monde numérique : « Ce que nous avons fait de novateur dans ce dossier, c'est que nous avons dit que même dans la crypto-sphère, les règles de base du code de la consommation qui protègent les consommateurs pouvaient trouver à s'appliquer » [41].

III.- Une perpétuelle nouveauté

25.- C'est surtout le caractère évolutif des techniques qui saute aux yeux des acteurs : « Les nouvelles technologies bien évidemment c'est la preuve actuelle mais c'est la preuve de demain. L'ADN à côté ça reste l'ADN mais bon… » (enquêté investigateur spécialisé en NT).

---

[38] PAMARD D., Note sous Crim., 8 novembre 2023, n° 23-81.636, *AJ Pénal* 2023, p. 560.
[39] LARONDE-CLÉRAC C., « Dispositions de la loi Justice relatives à l'enquête : simplification et modernisation ? » *AJ Pénal* 2024, p. 8.
[40] Une attaque en *déni* de *service* ou DDoS vise à rendre inaccessible un serveur afin de provoquer une panne ou un fonctionnement fortement dégradé du service.
[41] DAÏEFF G., « Cybercriminalité : "Il y a un enjeu de protection du pays et des acteurs économiques par le biais des peines" », *D. actu*, 12 septembre 2023, propos recueillis par G. THIERRY, journaliste.

> « Les technologies évoluent très rapidement » (enquêté magistrat) et « les délinquants aujourd'hui eux par contre vont beaucoup plus vite que nous. L'inconvénient, c'est un gros point noir mais pour lequel on ne peut rien faire car c'est logique dans un système contradictoire, c'est qu'aujourd'hui toutes les techniques qu'on utilise, tout ce qu'on fait et les façons dont on le fait, toutes les données, tout est marqué dans la procédure, tout apparaît au tribunal » (enquêté enquêteur spécialiste en NT).
> Les « personnes qu'on recherche savent se prémunir contre la géolocalisation ou la sonorisation en louant une voiture tous les deux ou trois jours ou en changeant d'appartement » (enquêté magistrat) ;
> « les hackers savent se construire une forteresse numérique » (même enquêté).

Au fond, les nouvelles technologies ne sont plus nouvelles mais elles seront toujours nouvelles, sinon innovantes, charriant par là-même une problématique liée à l'exclusivité et au secret.
Du reste, ce caractère d'innovation permanente et nécessaire est parfois invoqué pour déplorer le retard pris dans la mise à jour de certains protocoles, ainsi des adresses IP :

> « aujourd'hui en France, on utilise encore à plus de 80% les adresses IP dites V4, donc les adresses IP constituées de 4 blocs des chiffres séparés par des points. Le problème c'est qu'aujourd'hui en fait il n'y a plus assez d'adresses IP V4, donc on ne peut pas dépasser un certain nombre pour tout le monde ». « Du coup, enfin quand vous demandez par exemple à Free, parce que c'est les spécialistes et ce n'est pas cher, donc on économise, je voudrais les téléphones qui avaient cette adresse IP tel jour à telle l'heure, vous allez vous retrouver avec 200 numéros. Après effectivement ça demande du travail pour discriminer et finalement trouver le numéro qui nous intéresse vraiment. On y arrive mais c'est compliqué et c'est pour ça on est vraiment dépendant des autres dans ces cas-là » (enquêté spécialisé en NT).

§2.- Mesure de l'utilité

26.- Sans surprise – car l'enquête pénale utilise depuis longtemps des moyens que l'on peut qualifier de techniques et scientifiques – les acteurs soulignent que le recours aux NTIS est fréquent, routinier, parallèle à « l'avènement des technologies » en général (enquêté OPJ). Les techniques sont elles-mêmes devenues « habituelles » (enquêté OPJ), résultat à la fois d'un besoin (*I*) et d'une efficacité, variable toutefois (*II*).

I.- Un besoin

27.- Tous les acteurs (sauf cet avocat qui conteste la mesure « *in abstracto* ») affirment que les mesures sont utiles, qu'on « ne peut pas s'en passer », surtout pour les infractions clandestines ou complexes (montages financiers par exemple qui exigent des « outils fins », enquêté magistrat), « dans les affaires de terrorisme et de bande organisée » (enquêté avocat), mais même de façon plus générale pour tous types d'infraction (« on ne peut pas se passer des mesures NTIS dans le cadre de l'enquête pénale » affirment deux enquêtés JLD), d'autant que dans beaucoup de cas le *modus operandi* passe par l'usage d'un téléphone ou d'un ordinateur. Ainsi : « beaucoup de véhicules qui sont volés aujourd'hui, sont volés grâce à la nouvelle technologie : par un ordinateur qu'on va brancher sur la voiture pour enlever les codes ou des choses comme ça » (enquêté enquêteur spécialiste en NT).

> « Et je vois plus aucun magistrat faire l'économie, c'est même le contraire d'une analyse NTEC [enquêteur spécialisé dans les technologies numériques], même sur des infractions où foncièrement ça n'est pas de la cybercriminalité. La cybercriminalité c'est l'ensemble des exactions susceptibles de recevoir une qualification pénale soit qui ont été facilitées soit qui sont directement liées aux nouvelles technologies. Il y a bon nombre de fois où je suis sollicité, ça rentre pas dans le champ, c'est juste si "éventuellement tu peux me faire ça", si tu me trouves un élément, voilà c'est une vieille photo, un SMS, un vieux mail, une géolocalisation » (même enquêté).

28.- La question des besoins paraît prioritaire sur celle des critères qui n'a été abordée qu'ensuite à travers deux interrogations : sur quoi vous fondez-vous pour déterminer si vous pouvez avoir recours à une NTIS ? Parmi les NTIS, comment sélectionnez-vous celles qui vous paraissent les plus pertinentes ?
A la première, et hormis le critère du risque pour l'enquêteur, on répond en général que c'est la gravité de l'infraction qui détermine le choix d'une NTIS (« une forme de gradation entre les actes existe quand même car les plus graves comme la sonorisation sont généralement autorisés après d'autres actes moins sévères », enquêtés JLD) ; un enquêté précise *a contrario* que dans les affaires ordinaires, « ce n'est pas encore un réflexe », alors que cela peut s'avérer très utile (enquêté investigateur spécialisé en nouvelles technologies) ». Selon les interlocuteurs, les critères sont fournis par le droit (enquêté magistrat) ou sont en lien avec ce que l'on recherche, « intuitifs » : « rien d'écrit », « si on décide de le faire, c'est qu'on y croit » (enquêté OPJ).

> « Parfois un magistrat va vouloir mettre systématiquement une personne sur écoutes alors que dans mon service on sait que c'est inutile. Mais quelques jours avant l'interpellation, on met la ligne sous géolocalisation car si la personne n'est pas là au moment de l'interpellation, on passe pour des cons » (même enquêté OPJ).

Parmi les critères, on énonce le caractère intrusif de la mesure ou l'équipement technologique de la personne suspectée ou la formation des enquêteurs ou la lourdeur d'une installation. La question du coût est davantage approfondie (à notre initiative le plus souvent). Un acteur observe qu'il n'y a pas d'obstacles financiers car les TSE sont peu utilisées et « au point où on en est… ») (enquêté magistrat). Il remarque toutefois que « [l]es frais d'expertise informatique sont très élevés » (même enquêté magistrat). Un autre concède que dans son service, « on ne nous refuse rien » (enquêté OPJ) ; un autre : « dans les affaires terroristes c'est une certitude, ils utilisent tous les moyens à leur disposition », y compris injecter un virus dans un téléphone, « il faut quelqu'un en permanence pour analyser ce qui se passe au téléphone et donc c'est un travail monumental » (enquêté OPJ). Un autre évoque d'autres coûts : la formation des experts en nouvelles technologies ainsi que les licences d'exploitation (enquêté investigateur NT). Enfin, un autre mentionne un autre besoin ou, plus précisément, le fait que le recours aux NTIS comble un manque : « étant donné que les OPJ sont en sous-effectif, ces mesures permettent de pallier le manque de personnel en leur permettant de faire plus de travail, d'utiliser ces mesures pour ne pas être sur le terrain » (enquêtés JLD).

Quant à la seconde question, un enquêté magistrat y répond en qualifiant les NTIS de « boîte à outils », suggérant ainsi qu'il n'y a pas de hiérarchie et que l'on prend l'outil destiné à l'objectif recherché.

II.- Efficacité

29.- Si l'efficacité est d'emblée peu interrogée car semblant évidente, les acteurs apportent des nuances mesure par mesure en invoquant des contraintes (voir *supra* n°18 sur l'énumération des actes).
Selon un enquêté, « les policiers travaillent bien, la plupart du temps ils ont raison » (à propos de la géolocalisation « qu'il faut motiver depuis 2019 et qui est devenue difficile à contester », enquêté avocat). Le même fait le « constat général que désormais ça va plus vite et c'est plus facile », en particulier grâce à la plateforme nationale des interceptions judiciaires (PNIJ), qui permet que tout soit plus fluide et plus simple. La PNIJ facilite le recours aux mesures NTIS car « elle centralise les demandes et consolide le recours aux mesures » (même enquêté).

Sur le caractère probant,

> « en reprenant ces éléments des nouvelles technologies, on arrive très facilement à trouver des éléments, si c'est pas des éléments de preuve (ce qui va persuader l'esprit d'une vérité auprès d'un juge ou auprès d'un magistrat ou auprès d'un enquêteur) c'est le petit bout de ficelle. Moi quand un collègue amène un dossier je trouve toujours quelque chose qui lui permet dans le contexte général de la procédure de pouvoir rebondir ou de réorienter, de pouvoir tirer une ficelle. Pour moi les nouvelles technologies c'est une nouvelle forme d'accessibilité à la preuve et qui est bien plus importante que l'ADN, qui est bien plus importante que la toxicologie » (enquêté investigateur spécialisé en NT).

§3.- Mesure des limites

30.- Quand bien même les mesures NTIS sont, chacune dans son registre, utiles et efficaces, elles n'en sont pas moins, aux dires des acteurs de la procédure pénale, soumises à des limites que l'on peut attribuer à cinq séries de facteurs : le manque d'instrument de mesure de la mesure (*I*) ; des repères vacillants (*II*) ; la technicité des mesures (*III*) ; la dépendance aux opérateurs (*IV*) et la valeur probante des preuves obtenues par le biais des mesures NTIS (*V*).

I.- Instrument de mesure

31.- Pour dire qu'une mesure est utile et efficace, il faut, d'une part, pouvoir prendre la mesure de son utilisation, d'autre part, pouvoir mesurer sa capacité à atteindre l'objectif poursuivi. Or, sur le premier point, les données manquent et, sur le second, c'est la possibilité même d'obtenir cette information qui paraît évanescente.

A.- Mesure de l'activité

32.- De l'avis général, on ne dispose pas de statistiques qui permettraient de quantifier le recours aux NTIS, ce qui, par exemple, distingue notablement la preuve par le recours aux NTIS et la preuve par empreinte digitale ou génétique ou encore le renseignement.
Interrogés, les acteurs sont souvent un peu pris de court :

> « [a]ucune statistique à ma connaissance, il doit y en avoir » (enquêté OPJ) ;
> « [l]'État français est bien fait. Donc il doit y en avoir. Mais où ? Au ministère de l'Intérieur ? Il est toujours utile de savoir de quoi on parle et ce serait utile en termes de contrôle démocratique. Mais les chiffres bruts ne serviraient pas à

grand-chose. Il serait intéressant de savoir si les enquêteurs se sont approprié telle ou telle mesure » (enquêté magistrat) ;

« [v]ous ne l'aurez pas, il n'y a pas d'indicateurs chez nous. C'est ce qui est problématique, chacun mène son enquête comme il veut, si vous n'avez pas un garde-fou, en général un supérieur hiérarchique, qui vous dit dans tel cas de figure fais ci fais ça » (enquêté investigateur spécialisé en NT).

Certains enquêteurs évoquent des « statistiques informelles sur le nombre de saisines du JLD » (enquêté magistrat), là où un autre nuance : « on pourrait faire nos propres statistiques », on sait qu'il y a « un système de comptabilisation des ordonnances produites chaque jour qui est conservé mais on ne sait pas si c'est centralisé pour créer des statistiques » (enquêtés JLD).

B.- Mesure de l'impact

33.- La mesure de l'impact est doublement délicate, d'une part, parce que pour y procéder, encore faudrait-il savoir ce que l'on cherche, d'autre part, en raison de la division du travail entre ceux qui enquêtent et ceux qui jugent.

En premier lieu, même si « on ne peut pas se passer des TSE », « on jette un filet, on ramasse des tas de trucs » (enquêté magistrat), ce qui ne signifie pas un travail à l'aveugle car « on sait où on jette les filets », le même enquêté voulant dire par là que « [l']on est dans le judiciaire » et non « dans le préventif » (même enquêté).

En second lieu, il est généralement admis qu'il est difficile de mesurer l'apport concret de tel élément de preuve à la résolution de telle affaire en raison du cloisonnement entre l'enquête et le procès mais aussi du manque de temps dont disposent les parquetiers :

« Oui, c'est toujours regrettable, parce qu'au final il y a des affaires, notamment il y a toujours des affaires qu'on a plus à cœur que d'autres, et effectivement c'est très rare qu'on ait une remontée parce qu'en fait les services sont tellement sous l'eau », « quand ils terminent quelque chose, ils passent tellement vite à la suivante qu'ils n'y pensent pas », « c'est frustrant, on fait avec » (enquêté spécialisé en NT).

Le même estime que si le Parquet fait régulièrement appel à lui, c'est sans doute que son travail sert à quelque chose, quand bien même il serait utile selon lui que les attentes des parquetiers soient explicitées.

Sans le sentiment de frustration, mais avec celui de l'évidence, les instances chargées de l'autorisation expriment la même incapacité à juger du bien-fondé de la mesure :

« On ne peut pas avoir une réflexion globale sur l'enquête ni apprécier la place et l'importance des mesures qu'on nous demande d'autoriser. On ne voit qu'une petite partie de l'enquête et non l'intégralité. En outre l'urgence dans laquelle on doit traiter les demandes d'autorisation ne nous permet pas de réfléchir à la place des mesures NTIS dans celle-ci » (enquêtés JLD).

Du côté de l'enquête, on relativise cette impossibilité de connaître la contribution de la preuve à la résolution des enquêtes :

« [s]i je ne trouve pas d'éléments, c'est quand même intéressant pour l'enquête : il n'y a pas d'éléments. Ça permet de dire soit que l'infraction n'a pas été commise soit que ce n'est pas avec ce matériel là, mais c'est un élément pertinent quand même. Systématiquement » (enquêté spécialisé en NT).

Par exemple :

« Comme je l'explique à chaque fois sur une affaire, si vous me demandez aujourd'hui d'aller voir les factures sur l'ordinateur, moi je ne pourrais jamais affirmer qu'une facture est fausse parce que ce qui fait que la facture est fausse c'est que le magasin qui est censé l'avoir émise dit "je n'ai pas émis cette

> facture", c'est le seul moyen d'être sûr à 100% que la facture est fausse. Avoir des fausses factures sur votre ordinateur, c'est pas interdit en soi si vous ne les avez pas utilisées pour obtenir quelque chose derrière, tant qu'elle n'a pas été diffusée, tant qu'elle n'a pas été utilisée. Tout le monde peut faire des spécimens juste pour s'amuser. Moi clairement je ne pourrai jamais affirmer que la facture est fausse tant qu'elle n'a pas été vérifiée en tout cas auprès du magasin. Ce n'est pas mon rôle, moi j'ai trouvé des factures ; à l'enquêteur de déterminer de cette façon-là si c'est faux ou pas et c'est là la difficulté » (même enquêté).

Dès lors il faut expliquer aux « jeunes » que :

> « [t]on but c'est que tu constates, après c'est à l'enquêteur parfois d'aller faire le lien et de la même façon nous on est juste là pour orienter l'enquête et donner un faisceau d'indices ; ce n'est pas forcément une preuve qu'on va avoir, c'est un faisceau d'indices dans certaines affaires. Et c'est notre travail après effectivement de bien l'expliquer dans nos rapports et de le donner à un enquêteur » (même enquêté).

Pour un enquêté spécialiste en nouvelles technologies d'investigation dans une entreprise, ne pas avoir de retour officiel sur ce à quoi a servi le traitement est « un gage de sécurité » (enquêté qui précise que personne, dans l'entreprise, n'est au courant du cadre de l'enquête, des personnes ni des infractions et qu'en outre les services travaillent de façon « cloisonnée », « à partir d'un numéro de carte SIM, création de codes d'accès à l'OPJ avec date d'entrée et date de sortie »).

II.- Des repères vacillants

34.- Si les acteurs recourent à ces mesures parce qu'ils les trouvent globalement utiles, on les sent parfois désorientés par un manque de repères qui semble tenir à deux causes, liées entre elles : la difficulté à se repérer dans les textes et, par voie de conséquence, le risque qui pèse sur la validité de la procédure.

35.- Tout d'abord, certains disent faire « un peu de voltige » car les textes sont préparés à la hâte, sans conscience des contraintes opérationnelles et parce qu'on manque de jurisprudence ; dès lors « on se sent seul », « et encore à Paris, on a de la matière » (enquêté magistrat). Plus précisément, la multitude de fondements est source de perplexité : quel texte appliquer ? Selon quelle logique ? Et ce d'autant plus que parfois il est difficile de comprendre ce que l'intitulé de la mesure signifie. Ainsi, à propos de la section 5 « De l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique (Articles 706-95 à 706-95-3) », « on se pose les questions suivantes : qu'est-ce qu'une correspondance stockée ? Pourquoi le texte ne vise-t-il pas une donnée ? un document ? Que comprendre par "au moyen d'un identifiant informatique" ? Comment penser et qualifier les objets ? », par exemple, les serveurs ou les courriels stockés sur les téléphones ? (même enquêté).

Un autre acteur dit avoir du mal à définir le contenu des mesures ou à mettre en œuvre certaines distinctions, par exemple entre url et objet mail qui sont des données mixtes, à la fois de contenu et de connexion (enquêté avocat). Un autre explique qu'« au Royaume Uni, la distinction entre données stockées et données en circulation constitue un enjeu pour les avocats » (enquêté avocat).

Les enquêteurs s'abritent, quant à eux, derrière les magistrats ;

> « Si vous avez un doute, demandez l'avis du magistrat, expliquez-lui la situation et il aura peut-être un avis. Comme c'est lui qui va de toute façon défendre le

> dossier au tribunal, c'est à lui de savoir ce qu'il veut défendre ou pas. S'il estime qu'il ne pourra pas défendre tel choix ou que cela n'a pas d'intérêt, il vous dira non. Dans le cadre de l'enquête, on dépend du magistrat » (enquêté enquêteur spécialiste en NT).

36.- Ensuite, et par voie de conséquence, des inquiétudes s'expriment sur la validité des procédures : « on y a va parce qu'il faut y aller mais ce n'est pas très rassurant » (enquêté magistrat). Or, « on ne peut pas tellement compter sur le JLD » car le seul refus d'un JLD que cet acteur a essuyé concernait une sonorisation dans un restaurant entre un corrupteur et un corrompu et le JLD n'a pas motivé son refus (enquêté magistrat). Si, dans certains domaines comme le trafic de stupéfiants, de nombreuses demandes en nullité sont formulées (enquêté avocat), la nullité est rarement prononcée. De toute façon, en cas de problème, « de manière officieuse, à savoir d'après les discussions entre collègues, il y a une nouvelle intervention dans la même procédure pour autoriser une autre mesure, on voit qu'il n'y a en général pas de difficulté à cet égard » (enquêtés JLD).

> « Des fois j'ai quelques doutes si les faits sont anciens, mais j'autorise quand même pour le moment, aucune demande refusée en un an de fonction. Le parquet procède à un filtrage préalable » (enquêtés JLD).
>
> « La législation autorise toutes ces mesures. Nous, en tant que JLD nous exerçons un contrôle formel (sur les délais par exemple) car il y a beaucoup de conditions légales à vérifier, les régimes juridiques sont très détaillés. Pas d'appréciation substantielle. Sauf en cas de doute, le JLD procède à une appréciation plus substantielle » (enquêtés JLD).
>
> « On n'a pas beaucoup de temps pour répondre une fois qu'on a reçu la demande. Toutefois, on comprend l'importance de l'utilisation de ces mesures pour l'enquête » (enquêtés JLD).

Plus sévère :

> « Il est rare qu'un JLD refuse la prolongation des mesures » (enquêté avocat).
>
> « Le C3N [centre de lutte contre les criminalités numériques] élabore la stratégie de captation des données, le Parquet copie-colle, le JLD copie-colle » (même enquêté).
>
> « Tout le monde navigue à vue », « personne ne comprend sur quoi on statue » (même enquêté).

Dès lors, même si elles sont rarement prononcées, les nullités planent comme une menace, dont se fait l'écho, pour ce qui concerne les données de connexion, le rapport du Sénat précité sur les modalités d'investigation recourant à ces données dans le cadre des enquêtes pénales[42].

III.- Technicité des mesures

37.- Les auteurs sont prolixes sur ce point qui se décline sous trois aspects complémentaires selon les interlocuteurs : la mesure est malaisée à mettre en œuvre, y compris pour les spécialistes (*A*) ; elle est difficile à comprendre et à qualifier pour les profanes (*B*) ; technologie et technique juridique s'entremêlent au point de rendre le travail compliqué, voire de susciter la tentation du contournement (*C*).

[42] Rapport du Sénat n°110, précité, p. 98 et s.

A.- Difficultés techniques pour les spécialistes

38.- Les acteurs techniciens rencontrés livrent de nombreux détails sur les contraintes techniques qu'ils rencontrent. Ainsi, casser un chiffrement est beaucoup plus technique et difficile qu'il n'y paraît (pour des raisons informatiques, parce qu'une application est mal installée, etc.). « Parfois si on n'arrive pas à le faire en interne, il faut contacter le service R& D de la société qui a élaboré le logiciel » (enquêté investigateur spécialisé en NT). De même, redémarrer un ordinateur peut modifier certains fichiers automatiquement, redémarrer un ordinateur chiffré suppose de passer par un support externe pour « déchiffrer le disque à la volée » (même enquêté). Ou encore travailler « en live » (c'est-à-dire sur un ordinateur allumé, par opposition à l'ordinateur dit « *post mortem* » *i.e.* éteint) exige de documenter toutes les opérations effectuées (par exemple : « je vais appuyer sur telle touche » (même enquêté). Le même explique que sur un ordinateur *live*, on récupérera plus d'informations qu'après-coup sur un ordinateur éteint. En ce dernier cas, on saura quelles ont été les pages ouvertes récemment mais pas celles que consultait la personne au moment où elle a été interpellée (même enquêté).

Certes, la technicité fait gagner du temps : ainsi de l'intelligence artificielle, qui permet de faire le script de messages audio. Mais cela demande des outils très puissants (précisément en raison du volume des données) et ne règle pas tout (identification d'une abréviation, d'un accent, etc.) (même enquêté). Et, plus généralement, le temps gagné d'un côté est passé à analyser de l'autre :

> « un disque dur ça peut prendre plusieurs jours, voire plusieurs semaines à traiter, sans compter les assistances, c'est-à-dire guider l'enquêteur comme ça sur des sites pour savoir qui requérir. Ça nous ne le comptons pas comme une affaire » (même enquêté).

B.- Incompréhension pour les profanes

39.- Les magistrats présentent les enquêteurs comme étant plus friands de l'innovation qu'eux (« ils [les enquêteurs] aiment bien l'innovation », dit un enquêté magistrat). « On n'est pas des informaticiens » selon le même enquêté qui évoque, par contraste, des « enquêteurs de haut vol »). En outre, magistrats et enquêteurs n'ont pas à disposition des équipements de même qualité, notamment pour la géolocalisation, ou tout simplement pas le même type de logiciel (enquêté investigateur spécialisé en NT). Globalement avocats et magistrats seraient « mal armés », « peu réceptifs » (enquêté avocat), surtout dans les systèmes de droit civil « où les juridictions ont le pouvoir de dire le droit sans se soucier de convaincre et de susciter l'adhésion, contrairement aux juridictions de *common law* » (même enquêté).

Bien sûr, il est possible de se former mais

> « après comme je le dis ça prend aussi du temps, parce que les formations prennent effectivement du temps et malheureusement pendant ce temps-là nos affaires n'avancent pas, mais on se perfectionne et c'est aussi un moyen de gagner du temps derrière. Et c'est surtout comme je le dis, ma plus-value, en fait, ce que je fais ça s'apprend ; demain je vous donne un ordinateur, je vous montre comment rechercher et vous allez trouver des éléments sans avoir des compétences particulières. Il n'y a rien de "sorcier". A partir du moment où vous avez les outils et qu'on vous a montré comment les utiliser, tout le monde est capable de le faire » (enquêté investigateur spécialisé en NT)

Un autre, qui n'est pas enquêteur, évoque aussi « une formation sur le tas », sachant qu'il est « depuis toujours capable de monter un ordinateur » (enquêté avocat).

« Cela n'est pas facilement accessible, cela demande du temps et de l'énergie ; on comprend au fur et à mesure et donc souvent trop tard. Mais on finit par lire une fadette de manière différente. On a peu de cours à ce sujet. Mais cela change un peu » (autre enquêté avocat).

C.- La tentation du contournement ?

40.- Un enquêteur évoque longuement les obstacles liés à la Convention de Budapest sur la cybercriminalité[43] qui l'empêcherait de faire vraiment du « e-*forensic* », à savoir d'établir des liens de concaténation.

> « Tu lui saisis le téléphone sauf que si je fais votre téléphone, je sais que je passe à côté de 50% de preuves : les 50 qui sont sur votre compte Facebook, qui sont sur votre compte *Snapchat*, qui sont sur votre compte *Messenger*, etc., parce que maintenant l'interconnexion de vos différents comptes réseaux sociaux, tout n'est pas centralisé sur votre téléphone ; eux gardent une partie des données. A partir du moment où on saisit le téléphone, on coupe le fil entre ces données-là, qui sont sur des serveurs dédiés, et les données qui sont sur le téléphone ».
>
> « On me demande de faire l'analyse du téléphone dans un cadre précis : je suis face à un violeur, à un prédateur. Je fais l'analyse du téléphone : techniquement j'ai la possibilité, puisqu'il y a des petits *tokens* qui sont disposés sur le téléphone, d'utiliser un outil en appuyant simplement sur un bouton pour récupérer ces informations-là qui sont sur le serveur dédié mais la convention de Budapest m'en empêche » (enquêté investigateur spécialisé en NT).
>
> « On n'est pas dans ce cadre-là mais c'est simplement avoir la possibilité -je pense que ça nous faciliterait grandement la tâche- dans un cadre légal très précis, loyal : on me demande de faire un téléphone [NB sur la base de 77-1 CPP], le téléphone est à même de pouvoir communiquer avec des serveurs distants, ça serait simplement de dire : voilà je collecte la preuve qui est sur le téléphone mais que je vais également concaténer avec la preuve qui est sur les serveurs dédiés ; je récupère tout ça ; voilà et je fais un *melting pot*. Et je pense que concrètement, ça, j'aimerais bien mais bon ce n'est pas possible » (même enquêté).
>
> « Ce serait pratique par exemple quand l'enquêteur analyse le téléphone d'un utilisateur qui se sert de *WhatsApp* mais qui est souvent hors réseau il pourrait remettre le téléphone sur réseau et en avoir connaissance mais juridiquement il ne le peut pas et ne peut donc intégrer ces informations dans son rapport. Et l'enquêteur doit alors faire une perquisition informatique. Avec assentiment, donc. Vous pouvez refuser, auquel cas le juge de la liberté et de la détention doit être d'accord ; et là il va aller sur votre compte WhatsApp avec votre identifiant, votre mot de passe.
> Il va faire : "archive extraire" ; il va rapatrier les données, les placer sous scellés, en faire une copie : la première, il va la placer sous main de justice pour respecter l'intégrité de la preuve numérique et l'autre, la copie de travail, il va pouvoir

[43] Sur lesquels voir *infra*, Deuxième partie.

travailler sur la copie. Il vous fait signer un papier, le PV de perquisition et de saisie et là la preuve est légale » (même enquêté).

41.- Le même évoque l'existence de plusieurs procédures et la tentation de choisir la plus favorable à l'enquête, plus précisément au travail du technicien :

> « un téléphone d'une personne mise en cause dans le cadre d'une commission rogatoire donc on bosse pour le juge d'instruction, le téléphone est placé sous scellés, on me demande de faire l'analyse du téléphone. Je ne peux pas parce que je ne suis pas expert et je ne suis pas reconnu comme tel et je ne peux pas disposer de l'article 157 CPP.
> La même affaire, les mêmes faits en flagrance ou en préliminaire : le téléphone est placé exactement pareil sous scellés, on nous demande de faire le téléphone. Là je peux faire le téléphone. C'est le procureur qui délivre à l'enquêteur une autorisation de bris de scellés, ce qui me permet de faire l'analyse du téléphone. La seule obligation que j'ai, c'est de respecter l'intégrité de la preuve numérique (donc il ne faut surtout pas que je modifie ou que j'altère la preuve numérique sachant que du numérique c'est de l'immatériel, c'est facilement modifiable, falsifiable ; même simplement le mettre sous tension automatiquement ça va générer une modification de log ou autre).
> Dans la mesure où je n'ai pas la possibilité de le faire en commission rogatoire, on détourne en quelque sorte la loi, en disant ok aux enquêteurs, si tu veux que je fasse le téléphone, avant de le placer sous main de justice où je ne pourrai plus interagir ou sinon je suis obligé de passer par un expert, les sociétés auxquelles vous faisiez référence et tout ça, on va le faire dans le cadre d'une perquisition informatique.
> Là où je fais le téléphone seul dans mon laboratoire puisque j'ai une autorisation de bris de scellés, je le fais seul, une semaine, un mois, 3 mois, 4 mois, 6 mois après, peu importe, là dans le cadre de la perquisition informatique, exactement le même travail, il faut que la personne soit face à moi, elle me donne (alors pas en commission rogatoire) son assentiment (sachant que je peux m'y opposer, je consens expressément à ce que vous fassiez, etc.). Elle signe ce papier-là, elle a conscience que je vais faire une perquisition de son téléphone, je vais extraire des données, je vais interpréter ces données au regard du contexte général de la procédure. Ça c'est une perquisition informatique et ce qui vaut pour le téléphone, on peut le copier également pour la perquisition informatique des données qui sont disposées sur *Snapchat*, sur *Facebook* » (enquêté investigateur spécialisé en NT).

IV.- Dépendance aux opérateurs

42.- S'agissant plus précisément des données de connexion, des acteurs précisent que ce serait une erreur de penser que

> « les GAFA fournissent facilement les données. Il y a certains prestataires qui obligent par exemple : il faut que les faits soient une infraction punie de tant. Il y en a d'autres qui sont hyper protecteurs concernant les données : *Apple* typiquement c'est très compliqué d'avoir des données. A un moment donné même, *Apple* avait mis dans ses clauses d'utilisation générale que, sauf mention contraire dans la réquisition, ils informaient la personne comme quoi la gendarmerie se renseignait sur ses données » (enquêté investigateur spécialisé en NT).

En outre,

> « Par exemple, S*napchat :* si moi j'ai identifié un prédateur et que je fais une réquisition à *Snap* en disant "voilà j'ai identifié telle personne comme un prédateur sexuel qui fait de la corruption de mineurs ou autres", jamais S*napchat* va nous donner tout le contenu des messages. On a l'adresse, IP, purement déclaratif, il habite à tel endroit c'est tout. On sort de notre zone de confort et on sait que les Français pirates utilisent des proxys, des VPN. Donc voilà c'est super compliqué » (enquêté investigateur spécialisé en NT).

Enfin, un enquêté précise que

> « le stockage coûte cher aux entreprises et cela peut être un argument commercial de certaines d'entre elles que de dire qu'elles ne conservent pas de donnée alors qu'en réalité c'est un argument financier » (enquêté spécialisé en NT).

V.- Valeur de la preuve obtenue par une mesure NTIS

43.- Si, on l'a vu, le recours aux mesures NTIS est en lui-même peu discuté, la circonspection s'exprime quant au caractère déterminant de la preuve ainsi obtenue (*A*). En outre, son aspect technique apparaît comme un facteur de complexité quand il s'agit de la discuter judiciairement (*B*).

A.- Un élément de preuve parmi d'autres

44.- La donnée numérique doit toujours être « contextualisée », sinon « on peut lui faire dire tout et son contraire, tout et n'importe quoi » (enquêté investigateur spécialisé en NT) : « on prend trois investigateurs, on leur file chacun le même échantillon ; ils vont -j'espère- forcément trouver la même trace mais l'interprétation de cette trace et ce qu'ils vont en faire je ne suis pas convaincu qu'on aboutisse au même résultat » (même enquêté).

Si elle est très utile, elle est rarement déterminante et ne fait, le cas échéant, que grossir un faisceau d'indices :

> « dans tous les cas, au même titre qu'une enquête classique, un élément tout seul ne vaut rien. Si vous trouvez une adresse IP avec des horodatages et autres, à un moment ou un autre dans l'enquête vous devez vérifier effectivement s'il était bien à cet endroit-là à ce moment-là ; donc ça correspond, ça corrobore : l'heure et la date correspondent. En fait c'est par corrélation. Souvent un élément tout seul peut toujours prêter à interprétation, alors que quand vous avez plein d'éléments qui attestent, qui rentrent dans le même cadre que les autres, ça donne quand même plus de plus de poids à la chose" (enquêté enquêteur spécialiste en NT).

En tout état de cause,

> « en fait aujourd'hui il n'existe pas de méthode miracle, même avec l'arrivée de l'IA. Le problème est qu'aujourd'hui aucune intelligence artificielle, quelle qu'elle soit, ne peut faire le travail complet à notre place. Elle va pouvoir nous aider, ça va être un outil, un super outil à utiliser mais tout ce qui est informatique fonctionne par probabilité en fait. Quand ils vous disent : "ça c'est une image, il semble qu'il y a une plage dessus", c'est : "il semble, mais il n'y a que l'œil humain qui pourra dire c'est bien une plage ou il y a bien un palmier". C'est pareil quand vous faites une recherche sur un ordinateur pour trouver des

> factures, vous faites une recherche avec facture, mais vous trouverez aussi tous les dictionnaires qui contiennent le mot “facture”. Il n’y a que l’œil humain qui peut le dire, qui peut le certifier ; ça reste un bel outil, ça reste quelque chose à prendre en compte aujourd’hui, à commencer à travailler avec mais il faut effectivement toujours une validation humaine derrière » (même enquêté).

B.- Une preuve technique difficile à discuter judiciairement

45.- Étant techniques, les preuves doivent aussi pouvoir être discutées par les avocats sur ce plan-là : « Quelle technique ? Quel protocole ? Quel logiciel ? Quelle version ? Quelle faille connue ? ». L’enquêté avocat qui formule ces questions établit un parallèle avec la maintenance des radars ou l’éthylotest. Et il ajoute : la « discussion est plus compliquée si par exemple pour le déverrouillage d’un code de téléphone on passe par une société étrangère qui sera opaque sur ses méthodes ». Un autre explique qu’on pourrait passer par un expert privé mais qu’alors « il faut avoir les compétences techniques pour le guider » (enquêté avocat).
Certes,

> « dans les dossiers où figurent les PV, ce qui est rare, il est possible de comprendre l’ampleur, de révéler la mécanique et de tirer le fil. Mais dans la plupart des dossiers il n’y a pas cela. On y trouve les réquisitions, les ordonnances, les rapports de synthèse mais pas les PV, on ne voit rien. C’est un capot fermé. Concrètement, ce qui est donné, c’est la sélection de messages, les actes d’investigation réalisés » (enquêté avocat).

Dès lors l’avocat a « une connaissance très partielle » du dossier, et d’autant plus que « la plupart des mesures sont prises à l’insu de la personne » (même enquêté). « La contestation du recours à ces mesures est très compliquée car le contrôle du juge est très formel ; manque de temps et trop grande confiance dans les collègues (même enquêté, qui exprime par conséquent « un doute sur la compréhension des enjeux et par le parquet et par le JLD »).

46.- On comprend dès lors que le rapport d’enquête soit un élément déterminant, ce que confirment ceux qui les rédigent. Ainsi expliquent-ils qu’au fond, ce qui est le plus complexe, c’est moins d’apprendre à se servir d’outils techniques que d’expliquer ce qu’on en tire :

> « La particularité, et l’intérêt pour moi d’être formé, de savoir ce que je fais, c’est quand je vais partir en justice derrière. Parce que je peux être appelé en tant que témoin, je dois être capable d’expliquer ce que je vais faire et pourquoi je l’ai fait, dans quel but et comment je peux affirmer ce que je vais marquer dans mon rapport. Effectivement, moi je fais un rapport à l’issue de mes analyses. J’ai trouvé ça ou autre mais il faut pouvoir l’expliquer parce que si j’arrive en disant au tribunal que j’ai fait comme ça parce que mon logiciel me l’a dit, clairement au niveau crédibilité je ne suis pas bon. Je sais que là c’est le meilleur moyen que les éléments retrouvés ne tiennent pas. Le but c’est vraiment d’avoir une crédibilité aussi derrière en justice en disant : “oui j’ai été formé, je sais ce que je fais, ce que j’ai fait là, je sais ce que c’est ça, ce que ça a entraîné, son matériel ou autre et ce que j’ai trouvé, je peux vous affirmer que c’est bien là parce que... ” et ensuite donner des éléments. Le but est de pouvoir donner des bases à mon travail, pouvoir valoriser mon travail » (enquêté enquêteur spécialiste en NT).

Le rapport d’enquête fait alors le lien entre les spécialistes et les profanes, entre les différentes étapes de la procédure pénale :

> « Et ça c’est un autre problème aujourd’hui dans l’informatique : c’est expliquer et se faire comprendre par des gens qui au final n’y comprennent rien. Il faut de la vulgarisation des termes et des techniques et c’est parfois dans certains

rapports ce qui prend le plus de temps, parce que nous on sait ce qu'on a fait. Je peux l'expliquer en trois lignes, je peux le faire, mais personne ne comprendra. Le problème c'est que c'est pareil quand vous arrivez en justice, si vous défendez quelque chose mais que vous n'utilisez que des termes techniques, les jurés - c'est notamment eux les premiers - vont s'ennuyer et vous allez perdre tout le bénéfice de votre travail. Il faut donc expliquer correctement avec des mots simples les choses et c'est extrêmement compliqué sur certaines affaires, surtout quand vous avez comme aujourd'hui le chiffrement, les fiches effacées, etc... Il y a des termes... Mais ça s'apprend de travailler dessus, mais je sais que pour certains rapports on passe des fois plus de temps à écrire un petit paragraphe qu'à faire une analyse complète parce que je voulais que ce soit compréhensible » (enquêté investigateur en NT).

Le point de vue d'un JLD le confirme :

> « nous n'avons jamais refusé une demande d'autorisation surtout parce que le rapport qui accompagne la demande est bien détaillé et ne laisse aucun doute quant au respect des conditions légales et à la nécessité d'avoir recours à ces techniques ou technologies. Les mesures sont autorisées si le contentieux le permet et si telle est la politique pénale actuelle ».

§4.- Mesure ou démesure

47.- A deux égards au moins les mesures NTIS sont mises à l'épreuve. D'une part, les acteurs soulignent rapidement et spontanément que l'ubiquité des données obtenues par la dématérialisation de l'enquête repousse les limites physiques qui bornent classiquement certaines mesures, ce qui pose problème en matière de coopération internationale (*I*). D'autre part, et plutôt en réponse à nos questions – sauf lorsqu'il s'agit d'avocats –, ils ont des visions différentes de la question de la proportionnalité et de la nécessité des mesures NTIS au regard des droits fondamentaux de la personne poursuivie (*II*).

I.- Ubiquité des données et coopération internationale

48.- Tout d'abord, des acteurs soulignent des difficultés classiques liées à la coopération internationale. Certains pays refusent de coopérer, d'autres qui sont à la pointe sur le plan technologique refusent d'extrader (enquêté magistrat). Avec Europol et les conventions bilatérales qui règlent l'incorporation des éléments de preuve, on a « les outils juridiques pour l'entraide mais la coopération est lente » (même enquêté). En outre, les liens informels jouent un rôle : « On tisse des liens, on se déplace, on peut faire un peu mieux avancer nos enquêtes mais il faut choisir nos enquêtes, il faut arbitrer » (même enquêté) ; on travaille « à travers un collectif informel » (enquêté avocat).

Ensuite, l'existence de paradis fiscaux, le fait que les cryptomonnaies permettent de se passer de banques rendent le travail d'enquête ardu (enquêté magistrat).

Enfin, le « vrai problème de l'international », c'est qu'« on a des lois et des pratiques qui sont totalement différentes » (enquêté enquêteur spécialiste en NT). Le même enquêté donne deux exemples tenant à la diversité tant des législations concernant les incriminations que de la durée de conservation des données.

> « L'exemple avec *Facebook* est flagrant ou avec la plupart des GAFA qui veulent appliquer la loi américaine. Oui mais quand on parle d'infraction française mais que vous ne voulez pas nous donner de réponses, parce qu'aux États-Unis cette infraction n'existe pas. Oui, mais en fait en France elle existe, mais on ne peut pas la traiter parce que notamment pour tout ce qui est droit, on va dire la liberté d'expression aux États-Unis, vous pouvez dire tout ce que vous voulez, insulter qui vous voulez sur internet, il n'y a pas d'infraction. Donc, vous faites une réquisition à *Facebook* pour obtenir des informations sur la personne qui a menacé ou insulté, ils ne vous donneront pas de réponse parce que ce n'est pas une infraction aux États-Unis […]. Pour tout ce qui est conservation des données, vous prenez l'exemple tout bête de la Suède qui n'est pourtant pas un pays très loin : la conservation obligatoire des données est de 0 jour ; aucune durée obligatoire de conservation des données, alors qu'en France c'est un an chez eux c'est 0 jour. Vous faites une réquisition chez eux pour obtenir des informations, vous ne les aurez pas. C'est pour ça que certains fournisseurs d'accès, par exemple *NordVPN*, ne collaborent jamais avec nous, parce qu'ils sont basés dans ce pays-là et donc ils n'ont pas de durée de conservation des données. Donc, vous voulez faire remonter une adresse de quelqu'un qui a fait une bêtise, s'il est passé par le VPN ce n'est pas possible parce qu'ils vous diront qu'ils n'ont pas conservé les données ».

C'est également vrai selon cet enquêté avec le *cloud* :

> « il y a certes la convention de Budapest mais avec le *cloud*, les GAFA elles-mêmes disent qu'elles ne savent pas toujours sur quels serveurs se trouvent les données et celles-ci peuvent être stockées sur des serveurs qui se trouvent dans des pays différents ».

On rencontre les mêmes difficultés pour retracer le parcours d'un e-mail :

> « si vous recevez un mail par *Gmail* par exemple et que vous regardez l'entête de mail (l'entête de mail c'est là où vous avez toutes les informations de la route du mail), tous les mails viennent de *Mountain View*. En réalité, non, ils ne sont pas tous passés par là-bas, ça peut être un serveur à côté. Sauf que dans leur entête de mail systématiquement ça commence par ça » (même enquêté).

49.- Le phénomène est accentué avec le stockage sur des nuages (*clouds*),

> « c'est très compliqué de dire où sont les données. On sait pertinemment que Google a des *data centers* partout dans le monde. Il y a peut-être des données qui sont sur des barges au large de l'Irlande. C'est très compliqué de dire : je vais aller chercher les données qui sont physiquement à tel ou tel endroit. Physiquement les données de votre compte *Google*, je suis incapable de pouvoir dire sur quels *data center*s elles sont : à côté de Paris, sur une barge ; elles sont peut-être en Norvège (l'État norvégien est quasiment le premier fournisseur de *data centers*) » (enquêté enquêteur spécialiste en NT).

Or, selon la législation applicable, les conditions légales diffèrent, notamment en ce qui concerne l'assentiment de la personne. Ainsi, à propos d'un *cloud* examiné une fois l'ordinateur rallumé :

> « c'est le même problème pour le *cloud* où on peut aussi arriver en "*post mortem*" et où on peut retrouver ce qu'on appelle des *tokens*, donc des jetons d'authentification (c'est ce qui évite que vous ayez à taper votre code à chaque fois, ce qui vous permet de vous identifier). Si on a le jeton, on est censé avoir droit d'y accéder, si on ne sait pas où est le serveur, c'est le droit français qui s'applique. Si on est dans le cadre d'une analyse et on nous demande de le faire, on est censé être en droit de le faire. Là où le problème se pose réellement, c'est

quand on a un jeton et qu'on n'a pas besoin de taper l'identifiant. Là on peut accéder normalement comme dans le cas où on ne sait pas où c'est. Par contre, s'il y a besoin de taper les identifiants – par exemple la personne s'est déconnectée de Facebook et je dois taper ses identifiants – là il faut l'accord de la personne, parce que j'ai besoin de ses identifiants, j'ai besoin de ses données personnelles pour y accéder. Ce n'est pas quelque chose qui est accessible directement, j'ai besoin de taper un code. Même si je les obtiens d'une autre voie, à partir du moment où j'ai besoin de les taper manuellement, il me faut l'accord de la personne. Si je n'ai pas besoin de les taper et c'est une authentification automatique, je n'ai pas besoin de l'accord de la personne » (enquêté spécialisé en NT qui se réfère ici à l'article 57 CPP).

II.- Question de la proportionnalité des mesures à l'atteinte aux droits fondamentaux

50.- La question de la proportionnalité des mesures à la gravité de l'atteinte aux droits fondamentaux n'est en général pas abordée d'emblée – sauf par les avocats – et elle suscite des réponses mitigées.

51.- « Le sens de l'histoire, c'est de suivre la CEDH, ce qui est « sympathique comme concept mais parfois un frein aux enquêtes » (enquêté magistrat). « Bien sûr on ne peut pas borner n'importe qui n'importe comment, c'est très intrusif » (enquêté enquêteur spécialiste en NT) ; « ça va dans le bon sens et puis forcément on s'adapte » ; « si je me place en tant que policier, forcément en tant que policier on a toujours l'impression que ça ne va pas assez vite, que tout le monde se met contre nous autres, mais, en réalité, non » ; « Il faut aussi penser aux affaires ou à certains collègues qui veulent peut-être aller trop loin, alors qu'en réalité il n'y aurait pas besoin ; on rentre effectivement dans le domaine de la vie privée » (même enquêté).

52.- Parfois la question de la proportionnalité est envisagée sous le prisme de celle de la nécessité dans le contexte précis de l'affaire :

> « dans une affaire d'écoutes téléphoniques, injecter sur le téléphone un *malware* pour récupérer les données, ça ne pose pas de problème. Mais sur une affaire de vol de voiture, ça a peu d'importance ; il n'y aura pas de gros préjudice, c'est du matériel. Dans une affaire de terrorisme, oui, il va falloir le faire, parce que ça peut permettre d'éviter un attentat. La différence elle est là. Dans des affaires de criminalité organisée, si on sait qu'il y a un risque de passage à l'acte pour un assassinat ou autre, ils vont certainement le mettre en place. Mais si le préjudice n'est que matériel, par exemple des vols de voiture ou des cambriolages, même en bande organisée, l'intérêt est moindre » (enquêté spécialisé en NT).
> « On ne prend pas de bazouka pour tuer une mouche » (enquêté OPJ) ;
> « ce n'est pas au service des urgences que vous allez faire une coronographie » (enquêté magistrat).

53.- Pour le même magistrat, la jurisprudence de la Cour de justice de l'Union européenne donne l'impression de « magistrats qui n'ont jamais été en juridiction » car elle revient à dire : « je ne vais conserver de données que si elles concernent quelqu'un qui va commettre une infraction ! ». Il s'agirait là d'une « inversion du raisonnement qui nous fait tomber dans la prédiction du crime ». Il faut trouver « trouver une troisième voie entre la Chine, État autoritaire, et les Etats-Unis avec le pouvoir des GAFAM ».

54.- Les avocats sont, eux, plus sévères : ils critiquent la tendance du législateur, quand il consacre la mesure, à la circonscrire à des infractions très graves pour ensuite passer du dérogatoire à l'ordinaire, quitte à mettre à mal le droit à la vie privée, les droits de la défense, le secret professionnel ou, encore, à rendre incertaines les modalités et l'effectivité du contrôle de la mesure (procureur, juge d'instruction, juges des libertés et de la détention). Sans surprise, ils estiment que les TSE « portent atteinte aux droits et libertés, aux principes de proportionnalité et de nécessité, ainsi qu'à la CESDH », que les mesures d'investigation se développent au détriment des droits de la défense et, plus précisément, que les TSE posent un problème *in abstracto*, sur le plan des principes (existence) et *in concreto* (par leur application car elles sont très difficiles à comprendre et à discuter), surtout quand l'origine de la preuve est couverte par le secret, et ce d'autant que la jurisprudence a validé le principe de l'utilisation des preuves acquises au moyen de la technique du secret défense (enquêté avocat), un autre évoquant à ce dernier égard une forme de « blanchiment » d'informations obtenues de façon para-judiciaire (autre enquêté avocat). Sur ce dernier point, un enquêté formule la difficulté ainsi :

> « si le renseignement est obtenu par des techniques spécifiques de renseignement et que ça doit rester secret, c'est plus compliqué à mettre en place. C'est forcément plus compliqué de dire comment on l'a obtenu. Mais après c'est la base procédurale aujourd'hui. Dès la moindre technique, vous recevez un appel anonyme qui vous dit "voilà y a quelqu'un qui a fait ça", c'est un renseignement de base déjà. La loi prévoit que, dans un cas comme ça, on ouvre une procédure en préliminaire sur la base de renseignement et on fait les vérifications derrière. Donc transformer un renseignement en procédure ce n'est pas spécialement compliqué. Après, il faut savoir ce qu'on veut bien mettre dans la procédure. Et pour les services de renseignement, c'est souvent ça le problème : qu'est-ce qu'ils peuvent bien mettre dans la procédure ? Ça nous arrive quand vous faites des planques sur des stupéfiants ou autres, on ne veut peut-être pas mettre la photo où on voit la transaction se faire parce qu'ils vont savoir de quel endroit on a surveillé et la fois d'après on ne pourra plus le surveiller du même endroit » (enquêté spécialisé en NT qui établit une analogie avec une information venue d'un pays étranger).

55.- La question de la nécessité est abordée en termes de subsidiarité par un enquêté :

> « [i]l n'y a pas assez de contrôle de subsidiarité. Ce n'est pas facile pour le JLD de contrôler le respect de la subsidiarité. Le JLD n'est pas un juge de l'enquête tel qu'il existe dans d'autres systèmes de justice pénale. Il intervient de manière très ponctuelle au cours de l'enquête, ce qui ne lui permet pas d'exercer un contrôle autre que formel sur la demande d'autorisation des mesures. Malheureusement, le JLD n'a pas les pouvoirs du juge de la mise en état en matière civile. Son contrôle *a posteriori* des actes qu'il autorise est donc très réduit » (enquêtés JLD).

Ainsi l'absence de respect de la nécessité de la mesure n'est-elle pas forcément volontaire : « il peut arriver que les autorités compétentes pour ordonner une mesure n'aient pas conscience de la portée de la mesure décidée » (enquêté avocat).

56.- Un investigateur spécialisé en NT, quant à lui, se place sur le terrain de la loyauté :

> « il y a tout un travail à faire pour assurer que la collecte de la preuve soit loyale. Il y a tout un tas de victimes qui arrivent avec un *screen*. Un *screen*, c'est pas loyal, j'en veux pas. Il y a plein de logiciels, on peut faire son scénario, rien de plus facile. Moi, quand une victime se présente avec des *screens*, on dit à la

victime : 57-1 assentiment ; je préfère aller chercher moi les données, comme ça, ça peut pas être entaché de nullité par rapport à la traçabilité, l'intégrité ».

57.- En tout état de cause, certains acteurs soulignent que ni les justiciables ni les avocats ne sont réellement préoccupés par la façon dont les techniques portent atteinte à la vie privée : « nous avons l'impression que les justiciables saisissent le JLD uniquement lorsque c'est leur liberté individuelle qui est en jeu. Nous avons l'impression que les autres droits ne sont pas si importants pour les justiciables ou aux yeux du public. Par exemple les atteintes à la vie privée sont plus indolores aux yeux du public que celle à la liberté. Les avocats se préoccupent peu des techniques. Dès lors qu'il y a autorisation du JLD, elles sont dotées d'une forme d'autorité » (enquêtés JLD).

Section 3 : Communautés professionnelles

58.- Comme on peut intuitivement le saisir, l'usage des mesures NTIS affecte et parfois transforme les pratiques professionnelles des personnes qui y ont recours, voire donnent de nouveaux contours aux communautés qu'elles forment ou, du moins, un autre regard sur celles-ci. De manière plus précise, le discours des acteurs enquêteurs a fait apparaître une communauté soudée (*§1*) ; dans le domaine de l'enquête et au-delà apparaissent de nouveaux métiers tandis que se précise le rôle du secteur privé (*§2*).

§1.- Une communauté soudée

59.- Autant les acteurs variés que l'on a pu rencontrer ont tous témoigné de l'étanchéité des différentes étapes au cours desquelles interviennent des NTIS, autant, au stade de l'enquête, reviennent les termes ou expressions « entraide » (notamment à l'endroit de ceux qui sont moins bien formés), « communauté », absence de « cloisonnement », « bonnes pratiques ».
Ainsi : « on fait partie d'une communauté. On a toujours eu cette force là et c'est ça que j'adore » (enquêté investigateur spécialisé en NT).

> « Par exemple, moi, j'ai un collègue d'unité de terrain qui me rapporte un fait très particulier au téléphone, il y a un maillage départemental qui fait qu'il n'est jamais seul ; s'il peut répondre au problème, il répond, s'il peut pas, il m'appelle, si moi je ne sais pas quoi répondre, je vois avec le central, je pose la question, je sais pertinemment que dans l'heure quelqu'un là-haut, qui que ce soit, automatiquement va me répondre. Automatiquement on va m'apporter la réponse, voilà, qu'elle soit positive ou négative, c'est un truc de fou, on fait partie vraiment d'une communauté, des passionnés. C'est une des grandes forces. On n'est pas du tout cloisonnés, bien au contraire » (enquêté investigateur spécialisé en NT).

Si l'on peut éviter de se déplacer sur le lieu de la perquisition réelle, on préfère en raison du peu de personnels. Mais s'il le faut, on le fait car parfois les collègues enquêteurs ont très peu de connaissances en informatique.

> « On peut discriminer directement sur place le matériel à amener au commissariat. C'est-à-dire que je vais arriver sur place et dire : alors ça ne sert à rien de le prendre, ce n'est pas un ordinateur, ça n'a pas de support, ou alors on voit qu'il est connecté sur un NAS, un petit serveur à domicile qui existe, et en fait le serveur peut être planqué quelque part derrière une plinthe ou n'importe

quoi, certains sont tout petits. Donc, si je n'étais pas allé avec eux, cet élément je ne l'aurais pas eu » (enquêté investigateur spécialisé en NT).

Et s'il ne peut pas se déplacer, l'investigateur numérique donne aux enquêteurs deux ou trois bonnes pratiques à utiliser : faire une photo de l'ordinateur, de la page, appeler si nécessaire (même enquêté).

La collaboration s'étend aux collègues d'autres services (« on communique tous entre nous, on a un groupe, on est vraiment tous ensemble », enquêté investigateur spécialisé en NT) mais aussi aux collègues étrangers : « moi je suis également sur un groupe *Discord*, parce qu'on utilise les moyens modernes de l'international, avec des experts informatiques ou des experts dans l'investigation informatique dans laquelle nous sommes spécialisés » (même enquêté) ; elle passe par la fréquentation de forums spécialisés (téléphonie, voiture, métiers de la sécurité ou autres), des formations (« souvent assurées par d'anciens collègues policiers ou des membres des forces spéciales de l'armée qui utilisent les techniques sur le terrain », même enquêté), des échanges avec les sociétés privées (représentants ou services *hot line* qui font gagner du temps).

§2.- Nouveaux métiers et nouvelle configuration du secteur privé

I.- Nouveaux métiers

60.- La mise en œuvre des mesures NTIS s'est accompagnée de l'apparition de nouveaux métiers au sein de la police et de la gendarmerie, nés du besoin d'adapter l'enquête pénale aux exigences de la numérisation.

Au croisement des figures de l'enquêteur et de l'expert en informatique, ces nouveaux métiers visent soit à apporter la technicité nécessaire aux enquêtes qui, de plus en plus, investissent (et sont investies par) l'univers ou les supports numériques soit à communiquer ce savoir-faire, ces connaissances techniques aux magistrats qui dirigent l'enquête pénale et ordonnent ou autorisent la mise en œuvre des mesures NTIS.

61.- La première catégorie se compose des experts en informatique qui travaillent aux côtés des enquêteurs de la police nationale et de la gendarmerie (*A*) ; la seconde, des référents en matière de cybercriminalité qui assurent le lien entre l'action de la police judiciaire et celle du Parquet dans les affaires de cybercriminalité (*B*).

A.- Les experts en informatique : une fonction en appui des missions de police judiciaire

62.- La diffusion du numérique dans la vie de tout un chacun, notamment par la généralisation des connexions internet et des *smartphones*, a rendu l'investigation numérique incontournable dans le cadre de l'enquête pénale. Tant la gendarmerie que la police ont vite ressenti le besoin de disposer de leurs propres spécialistes en la matière afin de mener les enquêtes sur des supports numériques en totale autonomie par rapport aux experts en informatique du secteur privé. Pionnière et à l'avant-garde de la lutte contre la cybercriminalité[44], la gendarmerie a saisi la problématique posée par celle-ci ainsi que par la numérisation de l'enquête pénale dans sa globalité en mettant l'accent sur la formation de ses propres enquêteurs spécialisés dans les technologies numériques, connus sous l'acronyme NTECH (enquêteurs nouvelles technologies) (*1*). La police nationale a suivi le mouvement avec la création des Investigateurs en

[44] BARLATIER Jérôme, « Le renseignement criminel au service de la lutte contre la cybercriminalité : l'exemple français de la gendarmerie nationale », *Rivista di criminologia, vittimologia e sicurezza*, Vol. XVI – Numero unico – janvier-décembre 2022, p. 95 et s.

Cybercriminalité (*2*). Or, malgré leur importance pour l'enquête pénale, aucune définition précise du statut de ces professionnels ni des opérations de criminalistique ou d'appui et de conseil auxquelles ils procèdent ne figure explicitement dans le code de procédure pénale[45]. Contraints d'agir non seulement dans l'ombre mais aussi à travers la figure de l'OPJ, ces spécialistes restent discrets tout au long de la procédure.

1) Les spécialistes de la technologie numérique de la gendarmerie : constater sans agir

63.- Première force de l'ordre à s'être adaptée aux spécificités de la lutte contre la cybercriminalité, la gendarmerie dispose de ses propres spécialistes dans le domaine des technologies numériques. Il s'agit d'un ensemble de gendarmes dotés de compétences plus ou moins poussées en matière informatique leur permettant de rechercher, saisir et exploiter les preuves numériques ainsi que d'enquêter en matière de cybercriminalité ou en utilisant les mesures d'enquête fondées sur les nouvelles technologies. Si les gendarmes NTECH se trouvent au sommet de la hiérarchie et des compétences en la matière, ils sont assistés dans leurs fonctions par les enquêteurs sur Internet, les C-NTECH ainsi que les P-NTECH.

64.- A la fois enquêteurs et informaticiens, les gendarmes NTECH sont des enquêteurs spécialisés dans les technologies numériques et affectés au niveau départemental[46]. Environ 300 pour l'ensemble du territoire national, ils exercent tant les fonctions d'OPJ que celles d'analyste forensique. Selon leur affectation, ils peuvent intervenir dans le cadre de l'enquête pénale soit en qualité d'OPJ soit en qualité d'analyste. En tant qu'enquêteurs cyber, ils mènent des investigations complexes impliquant l'utilisation des technologies numériques ou nécessitant la mise en œuvre des mesures fondées sur de telles technologies. En tant qu'analystes forensiques, les gendarmes NTECH ne participent pas à l'enquête pénale en qualité d'OPJ, mais en tant que « personne qualifiée » au sens de l'article 60 alinéa 1er du code de procédure pénale[47]. Sous ce statut, les gendarmes NTECH assurent une mission de criminalistique appliquée et non pas de police judiciaire. Habilités pour effectuer des actes d'enquête sur des sites Internet ou des examens techniques sur des supports numériques, les gendarmes NTECH secondent leurs collègues qui enquêtent sur une affaire en comblant le manque de moyens et de technicité au sein des équipes d'enquête. Ils peuvent alors effectuer des analyses sur différents supports tels qu'une unité centrale, un ordinateur portable ou un *smartphone* à l'aide de matériels et logiciels spécifiques à cette fin. En tant qu'assistants techniques des enquêteurs, les NTECH assument le rôle d'un expert en criminalistique numérique. Ils effectuent des constats sur la base de leurs analyses techniques qu'ils soumettent par la suite aux enquêteurs de l'affaire sans pour autant enquêter eux-mêmes. Ce sont « des serruriers qui n'ouvrent les portes qu'à la demande de leurs collègues » (enquêté investigateur spécialisé en NT).

Toutefois, en pratique, la séparation est sinon contredite, à tout le moins nuancée : « Pour être un bon NTECH, il faut surtout être un bon enquêteur judiciaire » (enquêté investigateur spécialisé en NT). L'expérience antérieure d'enquêteur lui sert même quand il exerce en tant qu'analyste forensique puisqu'elle lui permet de mieux appréhender les enjeux de l'enquête et d'orienter celle-ci en suggérant souvent à ses collègues la marche à suivre. Par exemple, le gendarme NTECH pourra indiquer aux enquêteurs quel site internet il faut viser dans leurs

[45] Cf. DAOUST François, *Sur les traces de la police technique et scientifique*, Paris, PUF, 2020, p. 99.
[46] https://www.gendarmerie.interieur.gouv.fr/gendinfo/dossiers/la-police-judiciaire/ntech-les-enqueteurs-specialises-dans-les-technologies-numeriques
[47] Voir également l'article D7 du CPP.

réquisitions ou à quel fournisseur d'accès il faut adresser leurs réquisitions relatives aux données informatiques.

Pour assurer cette assistance technique, les gendarmes NTECH reçoivent une formation universitaire d'une durée d'environ un an dispensée par l'université de Troyes et le centre national de formation de la police judiciaire, appuyé par le pôle judiciaire de la gendarmerie nationale, sous la forme d'une licence professionnelle alternant des périodes d'enseignement en présentiel et des périodes en unité. Uniquement ouverte aux OPJ, la qualification de NTECH est délivrée à l'issue de cette formation, qui fournit des compétences plus généralistes et plus complètes que des formations ciblées du secteur privé.

65.- Dans leur mission d'OPJ, les NTECH sont assistés par des enquêteurs sur Internet, qui cherchent à détecter la commission d'infractions en ligne et à interpeller les auteurs d'infractions cyber par le biais des données recueillies lors des dépôts de plainte, des analyses de supports, de l'étude des réseaux sociaux, de la recherche d'images pédophiles ou de publications faisant l'apologie du terrorisme sur Internet. Titulaires d'une formation moins spécialisée que celle des NTECH, les enquêteurs sur Internet sont néanmoins capables non seulement de fournir une expertise de base en matière informatique, mais également de mener des enquêtes sous pseudonyme ainsi que des recherches en sources ouvertes.

66.- Compte tenu de l'importance des connaissances techniques pour les besoins de l'enquête pénale, la gendarmerie a également mis en place au sein des brigades des « Correspondants en technologies numériques » (C-NTECH)[48]. Leur mission est de fournir une expertise technique de base au sein des unités de proximité afin d'alléger la charge de travail des NTECH et ainsi leur permettre de se concentrer sur les missions techniques les plus compliquées. A cette fin, les C-NTECH procèdent aux saisies et aux placements sous scellés lors des perquisitions, sont habilités à réaliser des analyses simples sur des téléphones[49] ou à vérifier les données accessibles d'un ordinateur et, de manière générale, préparent l'intervention du NTECH. Contrairement aux NTECH, les C-NTECH n'ont pas le statut d'OPJ et sont formés pendant cinq jours par les NTECH au niveau régional.

67.- Le premier maillon de la chaîne des gendarmes spécialisés dans les nouvelles technologies est composé des P-NTECH, à savoir les primo-intervenants en nouvelles technologies numériques[50]. Se trouvant au sein de chaque brigade, les P-NTECH se limitent à une intervention au tout début de l'enquête pénale. Ainsi, ils sont habilités à recueillir les plaintes des particuliers victimes d'infractions et à effectuer des opérations de préservation et de saisie de preuves. Dotés d'une formation de base dispensée soit à distance soit au sein des écoles de la gendarmerie[51], les P-NTECH ont appris à connaître les principales infractions en matière cyber et les actions de prévention, à faire une réquisition à un opérateur Internet et à interpréter son résultat ou encore à détecter les supports numériques. Loin d'être des experts en la matière, les P-NTECH ont des connaissances de base en matière de cybercriminalité et d'environnement numérique ainsi qu'à propos des outils mis à leur disposition.

---

[48] https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2022/les-cntech-premiers-maillons-de-la-chaine-cyber

[49] Comme par exemple, l'extraction des SMS.

[50] https://www.gendarmerie.interieur.gouv.fr/gendinfo/dossiers/la-menace-cyber/des-technicites-alliees-a-l-investigation

[51] Depuis 2014, la formation P-NTECH est dispensée au sein de l'École des officiers de la gendarmerie nationale (EOGN) et des écoles des sous-officiers (ESOG).

68.- La masse des données à laquelle le travail des enquêteurs et des NTECH de tous niveaux permet d'avoir accès au cours d'une enquête pénale, comme les données de connexion ou les données de contenu (contenu des communications trouvées dans le téléphone portable par exemple), fait l'objet d'un traitement par les analystes criminels de la gendarmerie connus sous la dénomination d'ANACRIM (analystes en recherche criminelle)[52]. OPJ spécialisés dans l'analyse criminelle et l'usage des logiciels appropriés, les analystes d'ANACRIM effectuent un traitement et une analyse de ces données afin de créer des relations entre les différents types de données (par exemple : localisation, personnes, contenu). Opérant sur la base de la même logique que les *data scientists*, les analystes criminels deviennent de plus en plus indispensables au regard de la dataisation de l'enquête pénale contemporaine (voir *infra*, partie 3). Après une formation technique d'un an, les enquêteurs qui le souhaitent peuvent devenir des analystes criminels. Ils n'ont pas le double statut des gendarmes NTECH, puisque les analystes criminels restent toujours des enquêteurs.

S'expliquant par la place centrale de la gendarmerie dans le cadre de la lutte contre la cybercriminalité, cette pléthore de métiers et cette variété des fonctions ne se retrouvent pas au sein de la police nationale.

2) Les spécialistes de la technologie numérique de la police nationale : investiguer sans enquêter

69.- Même si elle est moins fournie que la gendarmerie en termes d'outils, de ressources et d'effectifs, la police nationale dispose également de ses propres spécialistes en technologies numériques. Il s'agit des Investigateurs en Cybercriminalité (ICC)[53] appartenant à la Cellule technique d'assistance de la police nationale, rattachée à la sûreté territoriale. Les Investigateurs en Cybercriminalité travaillent dans tous les commissariats et les services des directions départementales où ils apportent une assistance technique.

Contrairement aux NTECH qui sont leur équivalent au sein de la gendarmerie, les Investigateurs en Cybercriminalité ne sont pas des OPJ. Néanmoins, le fait de l'avoir été auparavant les aide beaucoup dans leurs missions, comme c'est le cas s'agissant des NTECH. Dans le cadre de l'enquête pénale, les Investigateurs en Cybercriminalité ont une double mission : d'une part, l'assistance technique au cours de l'enquête pénale et, d'autre part, la formation des enquêteurs.

70.- En effet, ils offrent une assistance technique aux enquêteurs de la police en analysant les ordinateurs, les portables ainsi que tout autre support informatique. Ces analyses font l'objet d'un rapport qui est par la suite transmis à l'enquêteur. Les investigateurs se limitent alors à un rôle d'assistance qui peut parfois comprendre l'orientation de l'enquêteur et la mise en évidence d'un faisceau d'indices mais il revient « à l'enquêteur parfois d'aller faire le lien » (enquêté investigateur spécialisé en NT), les Investigateurs en Cybercriminalité ne faisant que des constats qu'ils communiquent ensuite aux enquêteurs. Ce rôle d'appui ne leur donne pas une visibilité dans le cadre de l'enquête pénale surtout pour les magistrats impliqués, comme le procureur de la République ou le juge d'instruction. Toutefois, cela n'empêche pas le parquet de solliciter expressément leur intervention dans certaines affaires en raison de leurs compétences techniques. Si cette sollicitation donne une certaine crédibilité à leur travail, ils

---

[52] https://www.gendarmerie.interieur.gouv.fr/gendinfo/dossiers/la-police-judiciaire/analystes-en-recherche-criminelle-schematiser-une-procedure-judiciaire-complexe

[53] https://www.devenirpolicier.fr/metiers/enqueter/policier-investigateur-en-cybercriminalite

n'ont aucun retour de la part des magistrats du parquet ni sur l'issue des affaires ni sur la qualité de leur travail[54].

71.- Outre leur expertise informatique pendant l'enquête pénale, les Investigateurs en Cybercriminalité s'occupent de la formation des enquêteurs de la police judiciaire en matière informatique et criminalistique. Ces derniers n'étant pas spécialisés, ils interviennent dans tout type d'affaires et ont besoin de connaissances de base afin de comprendre les enjeux de la mise en œuvre des mesures NTIS, en particulier les perquisitions de téléphones portables ainsi que l'extraction des données d'unités centrales et de disques durs.

Les Investigateurs en Cybercriminalité sont formés pendant huit semaines par l'Office central de la sous-direction en charge de la lutte contre la cybercriminalité. Par la suite, plusieurs formations notamment sur les différents logiciels utilisés par la police peuvent être dispensées par des sociétés privées spécialisées dans la lutte contre la cybercriminalité qui commercialisent ces logiciels.

La nécessité de disposer de compétences en matière de nouvelles technologies et de criminalistique numérique concerne non seulement les acteurs de l'enquête pénale au sein de la police ou la gendarmerie mais aussi les magistrats qui dirigent ou contrôlent ces enquêtes et qui ont besoin *a minima* de comprendre les enjeux techniques posés par la mise en œuvre des mesures NTIS ainsi que par la transformation de l'enquête pénale au contact de l'environnement numérique.

B.- Les référents cyber auprès des magistrats : une fonction de communication des enjeux techniques

72.- Les référents en matière de cybercriminalité auprès des juridictions ont pour mission de faire le lien entre les magistrats intervenant dans l'enquête pénale et les enquêteurs dès lors que l'enquête implique le recours aux mesures NTIS et, par extension, des compétences en informatique ou en criminalistique numérique.

Sans être institutionnalisée, cette mission avait été conduite, de façon expérimentale, il y a cinq ans environ, par un officier de police détaché au parquet du Tribunal judiciaire de Paris. Chargé d'assurer une meilleure communication des enjeux de l'enquête pénale portant sur des affaires de cybercriminalité ou comportant des aspects numériques, il lui revenait également d'intervenir de manière ponctuelle afin d'expliquer aux magistrats du parquet ou aux juges d'instruction les techniques spéciales d'enquête mises en œuvre dans une affaire donnée ainsi que les points techniques des rapports rédigés par les Investigateurs en Cybercriminalité de la police nationale sur leurs activités dans le même contexte.

Se rapprochant de la figure du magistrat de liaison du point de vue de son rôle, le référent cyber auprès des juridictions assure une meilleure compréhension des techniques spéciales d'enquête par les magistrats dont la plupart ignore le fonctionnement technique des mesures NTIS en général. Certes, la création de pôles d'instruction spécialisés ainsi que l'émergence des assistants spécialisés qui travaillent au sein des juridictions ont réduit l'impact et l'importance des policiers référents cyber. Toutefois, les problèmes de compréhension des mesures NTIS et du déroulement de l'enquête pénale au sein de l'environnement numérique persistent parmi les magistrats qui n'interviennent que ponctuellement dans ce contexte, comme c'est le cas tout

[54] Voir *supra*, n° 33.

spécialement des juges des libertés et de la détention, mais aussi des magistrats des juridictions de jugement.

II.- Rôle du secteur privé

73.- Même s'il n'explose pas, le secteur privé joue un rôle croissant, certaines entreprises s'étant spécialisées dans les techniques numériques au service des États, des entreprises et des populations mais surtout dans les enquêtes au service de l'État, principalement du ministère de la Justice, sur réquisitions judiciaires (*via* les frais de justice), et du ministère de l'Intérieur. Ces entreprises interviennent sur réquisition du juge d'instruction ou du procureur à la demande d'un OPJ dans le cadre d'une enquête. L'entreprise interrogée travaille en *Open source* et stocke ses données en France ou en Europe pour garantir la souveraineté numérique. Elle revendique se situer dans le cadre légal :

> « on prend en compte la jurisprudence et la loi. On s'inscrit dans la loi. Ainsi la reconnaissance faciale est exclue de notre champ. On est accompagné par des conseils.
> La jurisprudence sur la conservation des données conduira à faire évoluer les solutions mais pour l'instant on n'est pas trop impacté car cette jurisprudence concerne davantage la mécanique de l'enquête que notre travail » (enquêté spécialiste des NT dans une entreprise privée).

Le développement du recours au secteur privé dans ce domaine est justifié ainsi :

> « [e]nquêter, ce n'est pas faire du développement informatique. Le coût est très élevé (par exemple la PNIJ coûte beaucoup plus cher que ce qui avait été prévu). Trop cher, trop compliqué, trop lourd. Pour l'État c'est moins cher d'acheter du service. C'est le même topo que pour les bracelets électroniques. L'objectif c'est d'accélérer le travail d'enquête, non de le faire (cela reste du régalien). Cela permet à l'enquête de se concentrer sur l'analyse » (même enquêté).

En pratique, en matière de géolocalisation, il s'agira de récupérer la donnée et de la rendre intelligible aux enquêteurs « en temps réel par une remontée de points qui permet aux enquêteurs de savoir où sont les téléphones » (même enquêté). Mais le secteur privé intervient aussi pour créer des logiciels de traitement des fadettes, former des enquêteurs, élaborer des solutions servant à certaines enquêtes administratives (ici l'État ne veut pas externaliser et l'entreprise vend une licence). Le secteur privé est aussi sollicité, sous réquisitions également, pour faire de l'investigation numérique, c'est-à-dire extraire des données et éventuellement les analyser.

De l'avis du secteur privé comme des services d'enquête, la collaboration est bonne : « l'expérience utilisateur » est utile pour faire évoluer l'outil, de façon « quasi individuelle auprès des policiers et gendarmes » (enquêté spécialiste des NT dans une entreprise privée). « Le ministère de la Justice paie mais reste très lointain. Pas de contrat, pas de cahier des charges » (même enquêté).

Un enquêteur spécialisé dans les NT confirme ce point : il est « facile de contacter le service après-vente car ce service est inclus dans l'abonnement annuel (abonnement car recherche permanente en la matière ». Sur l'*Open source*, il précise :

> « [a]lors oui, il y a soit les boîtes privées soit effectivement des sociétés des logiciels *Open Source* qu'on retrouve. On peut utiliser de l'*Open source* après être sûr qu'effectivement il n'y a pas de risque… Tous les logiciels qu'on utilise sont vérifiés et on s'assure qu'il n'y a pas de problème derrière. Effectivement

> on peut utiliser de l'*Open source* aussi parce que l'*Open source* est ouvert à tous donc on ne peut pas, nous, rester fermés. Il faut juste les vérifier, il faut les tester avant. Mais effectivement sur l'*Open source* on le peut aussi. Après, les boîtes privées souvent c'est des boîtes qui ont des contrats avec l'État, avec lesquelles on va travailler et qui développent spécifiquement (des logiciels) pour le *forensic* au niveau international, pour aussi avoir une garantie. Effectivement, c'est des contrats avec des États, c'est vraiment des sociétés, on travaille avec les mêmes entreprises qu'à peu près tous les pays du monde » (enquêté investigateur spécialisé dans les NT).

Mais les policiers et gendarmes développent aussi des logiciels :

> « [i]l y a des policiers qui peuvent le faire ou des gendarmes. On a pas mal de logiciels comme ça. Parfois ces policiers ou gendarmes ont développé ces logiciels pour eux, pour travailler et puis ils se rendent compte que finalement c'est pas mal et ils le partagent avec la communauté. Après il y a des policiers qui font ça, qui développent des logiciels après, par exemple : *Whisper*, un logiciel qui traite l'audio, là c'est la société *OpenAI*, la même société que *ChatGPT*, il a développé pour l'audio et après il l'a partagé et après, effectivement, il y a des experts informatiques ou des gens comme ça qui partagent leur logiciel » (même enquêté).

La concurrence entre entreprises a des effets induits sur l'enquête : « Effectivement, certaines d'entre elles sont en concurrence. Donc la moindre information est confidentielle. Même nous des fois, quand on travaille avec différentes sociétés on a la difficulté d'obtenir certaines informations parce que les sociétés sont un peu réticentes, elles ont peur qu'il y ait une fuite au niveau de la société concurrente avec laquelle on travaille aussi » (même enquêté).

* *
*

74.- En conclusion de cette plongée dans les usages, nous pouvons faire observer que d'eux-mêmes les acteurs ne proposent pas vraiment d'élément de réforme pour améliorer le système.

A notre demande toutefois ils ont pu évoquer :

- l'intérêt d'associer les professionnels spécialisés à l'élaboration des textes ;
- la confection de guides qui soient des applications pratiques et non une paraphrase ou une exégèse des textes (ce que sont souvent les circulaires), autrement dit des guides à usage des professionnels et qui partent d'exemples du terrain (même si les technologies évoluent très rapidement) ;
- des formations transversales et continues sur les TSE ;
- un référent « cyber » dans chaque tribunal qui permette de faire le lien entre les parquetiers, les juges d'instruction et les affaires et d'expliquer les rapports et les techniques qui avaient été utilisées ;

- une meilleure motivation des actes demandant une NTIS ou la refusant.

Nous ajouterions volontiers :

- des données et analyses statistiques sur la place des mesures et l'évolution de leur emploi.

Cartographie des acteurs du recueil et de l'administration du renseignement et de la preuve numériques

Réalisée par

Antonin Guillard
Doctorant au Centre de droit pénal et de criminologie

Sophie Sontag-Koenig
Maîtresse de conférences à l'Université Paris Nanterre

Conçue de manière dynamique et dotée de liens hypertextes, la cartographie est accessible en ligne (lien ci-dessous).

Sa version imprimée est également livrée avec le rapport.

Enfin, une note explicative présente l'ambition et la méthodologie (*infra*).

Lien vers la cartographie en ligne[55]

https://miro.com/welcomeonboard/T3AwZllmeUNjYUNPdE5qVXY0WE96bHRLaFRGZTJjNHBUVFA5UEM5SFNNZDhPY25UN0VVY3RIalF1RmZlRXFQcnwzNDU4NzY0NTU3NjM5MjkwMTI3fDI=?share_link_id=44640732862

Note explicative :

I.- Présentation de la cartographie

75.- Finalité. La cartographie a pour finalité de présenter les différents acteurs impliqués dans le recueil et dans l'administration du renseignement et de la preuve numériques. Elle met en carte le processus d'orientation, de collecte, d'analyse et de diffusion des informations obtenues par les services de renseignement et de police judiciaire.
Sa structure repose sur une double séparation du temps et des fondements : d'une part, une division temporelle (bien que la circulation et les interactions entre ces deux sphères – renseignement et procédure pénale – ne soient pas à sens unique) entre la phase de prévention des atteintes aux intérêts fondamentaux de la Nation et celle de recherche des infractions pénales ; d'autre part, une distinction matérielle entre les dispositions du code de la sécurité

[55] *Mode d'emploi* : Pour accéder à la cartographie dynamique, il faut cliquer sur le lien qui ouvre le site de l'application MIRO, puis renseigner un nom et une adresse mail, puis définir un mot de passe, un code est envoyé à l'adresse mail qu'il faut renseigner ; une fois ce code renseigné, la carte peut être consultée.

intérieure et du code de la défense relatives au renseignement et celles du code de procédure pénale applicables à l'enquête, à l'instruction et au jugement des infractions. Les différentes rubriques qui composent les deux parties de la carte peuvent être comprises séparément mais une lecture complète suppose de commencer par la partie située en haut à gauche.

76.- Le renseignement. La partie gauche de la carte montre les mécanismes propres au renseignement alors que la partie droite explique ceux qui concernent la procédure pénale.
- ***L'encadré numéro 1*** présente les acteurs cadres chargés de conduire et d'encadrer la politique publique de renseignement. Ils ne sont pas directement impliqués dans le recours aux techniques de recueil de renseignement mais ils exercent une influence sur les services qui les mettent en œuvre.
- ***L'encadré numéro 2*** expose la procédure relative aux techniques de recueil de renseignement prévue par le livre VIII du code de la sécurité intérieure. Elle se subdivise en trois phases relatives à la demande de l'acte, à son exécution et au traitement des informations collectées.
- ***L'encadré numéro 3*** vise les services compétents pour initier et exécuter cette procédure. Les finalités poursuivies par les différents services de renseignement sont précisées. Les services spécialisés de renseignement, aussi appelés services du premier cercle, participent à la défense et à la promotion de tous les intérêts fondamentaux de la Nation alors que les autres services de renseignement, aussi appelés services du second cercle, n'agissent que dans la poursuite de certaines finalités. Cependant, la carte ne fournit pas de liste des techniques de recueil de renseignement susceptibles d'être utilisées par les différents services de renseignement sur le fondement des finalités relevant de leur compétence.
- Le dernier encadré de la partie gauche de la carte porte le ***numéro 7*** car il est commun à la procédure pénale. Il décrit en effet les organismes sollicités en application des deux procédures afin de recueillir, d'analyser ou de conserver des données. Les règles prévues par les deux cadres juridiques ne sont pas identiques mais les acteurs requis sont proches. Il est préférable d'examiner la fonction des opérateurs de communications électroniques et d'autres prestataires après avoir étudié le déroulement du recueil et de l'administration de la preuve numérique.

77.- La procédure pénale. En miroir des trois encadrés spécifiques au renseignement, la partie droite de la carte vise les acteurs cadres de la procédure pénale, la procédure relative aux actes d'investigation et les services de police judiciaire.
- **L'*encadré numéro 4*** décrit ainsi les institutions qui guident l'exercice de la procédure pénale. Il comprend peu d'éléments car la séparation des pouvoirs restreint fortement l'immixtion de l'exécutif et du parlement dans les affaires judiciaires. La situation tranche avec celle du renseignement (***voir encadré 1***) qui constitue un outil du pouvoir exécutif soumis à un contrôle parlementaire. La rubrique comprend néanmoins la mention de quelques acteurs nationaux et internationaux qui peuvent jouer un rôle dans la formation et dans l'application des normes.
- **L'*encadré numéro 5*** propose une synthèse de la procédure relative aux actes d'investigation permettant d'obtenir et d'analyser des preuves numériques. Sa présentation est bien plus complexe que la procédure prévue en matière de renseignement car chaque acte connaît des particularités notoires. La carte retient en conséquence les règles communes aux différents actes d'investigation exposées en trois temps. La phase d'autorisation de l'acte, celle de son exécution et le traitement réservé aux preuves obtenues. La rubrique met aussi en avant les magistrats et les juridictions qui jouent le rôle le plus important dans la supervision de ces étapes.
- Dans la même optique, ***l'encadré numéro 6*** vise les services de police judiciaire les plus actifs dans le recueil et l'administration de la preuve numérique. Certains d'entre eux sont aussi visibles dans ***l'encadré numéro 3*** relatif aux services de renseignement car ils disposent d'une compétence mixte.

- Au niveau inférieur, ***l'encadré numéro 7*** désigne donc (*supra*) les organismes sollicités en application de la procédure pénale en lien avec ceux qui participent à l'exécution des techniques de recueil de renseignement. Ce n'est qu'à l'issue de la lecture des 6 premières rubriques qu'il est intéressant de se plonger dans l'encadré numéro 7. Il montre à quel point l'obtention et le traitement des données numériques est dépendant d'acteurs publics et privés extérieurs à la procédure pénale et au renseignement.

78.- Les interconnexions du renseignement et de la procédure pénale. La séparation entre la partie gauche et la partie droite de la carte n'est pas seulement atténuée par ***l'encadré numéro 7***. Elle est aussi nuancée par les liens qui existent entre les deux domaines particulièrement sous l'angle des échanges d'informations. Ces liens apparaissent sur la carte et sont figurés par les différents traits qui traversent la frontière entre les matières, entre les deux sphères. La procédure pénale peut être destinataire de données collectées grâce à des techniques de recueil de renseignement et le renseignement peut être destinataire d'éléments recueillis au cours de l'enquête ou de l'instruction.

II.- Méthodologie de confection de la cartographie

79.- L'élaboration de cette cartographie a impliqué des prises de position méthodologiques de la part de ses auteurs. Ces choix ont pu conduire à focaliser la représentation graphique sur certains points plus que sur d'autres.

80.- S'agissant de la partie de la cartographie présentant les rapports entre acteurs de la procédure pénale, il a été fait le choix d'axer la présentation sur les services ou magistrats dotés d'un rôle spécifique dans le cadre de la recherche de la preuve numérique. De même, plutôt que d'exposer de façon détaillée tous les actes de procédure pénale, le choix a été fait de présenter synthétiquement les opérations, suivant les trois temps décrits plus haut. En effet, comme spécifié dans la cartographie, les règles applicables aux actes d'investigation sont bien plus variables que celles qui encadrent les techniques de renseignement. Les acteurs impliqués n'étant alors pas nécessairement spécialisés dans la conduite des procédures d'investigation en vue du recueil de la preuve numérique, il a donc été fait le choix de spécifier les services qui détiennent une compétence spécifique (sections spéciales J1, J2, J3 du parquet par exemple).
A l'inverse, la partie inférieure de la cartographie, relative aux organismes sollicités en application du droit du renseignement et de la procédure pénale, nécessitait davantage d'explications rédigées pour clarifier leurs rôles respectifs, ce qui a justifié des encadrés plus détaillés.

81.- Par ailleurs, le choix du positionnement de certains acteurs dans **l'*encadré 4*** aurait également pu justifier un placement plus à la marge mais de ce fait transversal, eu égard au rôles pluriels et périphériques qu'ils jouent dans l'accès à la preuve obtenue par les nouvelles technologies d'investigation et de surveillance.

82.- L'indication de la Direction des affaires criminelles et des grâces (DACG) renvoie au rôle de cette direction dans l'élaboration des normes en matière pénale. Elle établit et conduit notamment les politiques publiques en matière pénale. En son sein, le pôle d'évaluation des politiques pénales travaille spécifiquement à l'analyse de données statistiques du ministère de la justice, permettant de répondre ainsi aux demandes du garde des Sceaux ou de son cabinet lorsqu'ils travaillent sur des projets de texte portés par le gouvernement ou sur une action visant un domaine spécifique.

83.- La Commission nationale de l'informatique et des libertés (CNIL) peut être impliquée à plusieurs égards dans le processus. Autorité administrative indépendante créée par la loi Informatique et Libertés de 1978, elle détient plusieurs missions élargies par la loi pour une république numérique du 7 octobre 2016. Elle a notamment le rôle de conduire une réflexion sur les enjeux éthiques et les questions de société soulevées par l'évolution des technologies numériques. Mis en lien avec le sujet de la présente étude, on peut donc souligner le rôle de la CNIL pour initier la tenue de débats publics sur des sujets tels que le recours accru à l'intelligence artificielle. Plus spécifiquement, la régulation à laquelle cette autorité indépendante contribue en matière de données personnelles s'opère par différents instruments : avis sur des projets de loi ou de décret, autorisation pour les traitements les plus sensibles, recommandations, cadre juridique simplifiant les formalités préalables, réponse à des demandes de conseils. Ainsi, elle s'est par exemple prononcée le 8 décembre 2022 sur le projet de loi relatif aux Jeux olympiques et paralympiques de 2024 qui présente des enjeux forts en matière de protection des données personnelles et de vie privée, en particulier en ce qui concerne la possibilité de mettre en œuvre, à titre expérimental, des dispositifs de vidéoprotection et des drones afin de détecter et de signaler en temps réel des événements prédéterminés susceptibles de menacer la sécurité des personnes.

84.- Par ailleurs, le rôle de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) nécessite également quelques précisions. L'ANSSI est une agence interministérielle, créée par le décret n° 2009-834 du 7 juillet 2009. Elle constitue un service du Premier ministre et est placée sous l'autorité du secrétaire général de la défense et de la sécurité nationale. L'ANSSI se positionne comme l'autorité nationale en matière de cybersécurité et est à ce titre dotée de plusieurs missions visant à « *comprendre, prévenir et répondre au risque cyber* ». Dans ce cadre, ses fonctions d'accompagnement peuvent être soulignées. Cet accompagnement s'adresse notamment au gouvernement dans le cadre du déploiement d'une politique publique en matière de cybersécurité ou vise encore à contribuer au développement d'une doctrine française de cybersécurité et à la conception des dispositifs normatifs et réglementaires aux niveaux national et européen. En outre, son action tend également au développement d'un écosystème de prestataires de produits et de services de confiance dans le domaine de la cybersécurité. En lien avec la présente étude, le rôle de l'ANSSI peut notamment être souligné pour sa contribution à l'utilisation de certains dispositifs de recueil de la preuve numérique ; par exemple, dans le cadre de la mise en œuvre de l'article 706-102-1 CPP (***voir encadrés 5 et 7***), relatif à la captation à distance de données informatiques par les enquêteurs, dans le cadre d'une information judiciaire en matière de criminalité et de délinquance organisées et sur autorisation du juge d'instruction. Cette captation ne peut en effet être effectuée que *via* des dispositifs techniques autorisés conformément à l'article R. 226-3 du code pénal et mis en place dans ce cadre, c'est-à-dire par des dispositifs soumis à une autorisation, après avis d'une commission consultative composée notamment du directeur général de l'Agence nationale de la sécurité des systèmes d'information ou son représentant, président (art. R. 226-2 CP).

85.- Enfin, dans un souci de clarté de présentation, le choix a été fait de centrer la présente cartographie sur le système français, et ce faisant de mentionner uniquement la présence des instances EUROPOL (officie européen de police) et EUROJUST (Agence de l'Union européenne pour la coopération judiciaire en matière pénale) sans détailler davantage leurs actions. Pour autant, la démarche ici entreprise mériterait d'être poursuivie et dupliquée à l'échelle européenne pour envisager les interactions et la coopération entre les services d'enquête transfrontaliers. Cette coopération se trouve désormais renforcée grâce à plusieurs outils mis en place par le deuxième Protocole additionnel à la Convention sur la cybercriminalité, adopté par le Conseil des Ministres du Conseil de l'Europe le 17 novembre

2021, et relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE n° 224). Ce texte vise notamment à apporter des réponses aux défis tenant au stockage externalisé des données informatiques nécessaires aux fins d'une enquête pénale. La coopération est en outre plus encore appelée à se déployer dans l'espace de liberté, de sécurité et de justice de l'Union européenne, par l'intermédiaire en particulier du paquet *e-evidence* composé du règlement (UE) 2023/1543 du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale et de la Directive (UE) 2023/1544 du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales.

Deuxième partie : Normes

86.- Ancrées sur les nouvelles technologies, et surtout sur le numérique, et exigeant un niveau de technicité relativement élevé pour leur maniement, les mesures NTIS résultent d'un processus normatif qui explique les traits de leur consécration juridique. Souvent éclipsée au profit d'une mise en lumière de leur caractère technique et technologique, l'analyse normative de ces mesures oblige à se pencher non seulement sur les textes afin d'étudier le régime des mesures (*Section 2*), mais également sur leur histoire, et plus précisément leur généalogie afin de comprendre leurs mutations, leurs différences et les distinctions opérées par le législateur au moment de leur insertion dans le droit positif (*Section 1*). Véritable pivot autour duquel s'articulent les usages des mesures NTIS et les perspectives qu'ils impliquent pour l'ensemble de la procédure pénale, l'étude des normes relatives aux mesures NTIS dévoile une certaine façon de légiférer : plus technique[56] mais moins juridique, plus pratique mais moins théorisée, plus pointue mais moins inclusive.

Section 1 : Généalogie des mesures NTIS

87.- La généalogie des mesures d'investigation et de surveillance fondées sur les nouvelles technologies (mesures NTIS) révèle combien leur apparition (*§1*) comme leur évolution (*§2*) se sont réalisées de manière pour ainsi dire réactive au rythme de l'essor des technologies numériques perçues et conçues à la fois comme menace contre laquelle il fallait lutter et outil qu'il fallait absolument intégrer à la procédure pénale. Cette forme de spontanéité donne ainsi à la construction d'ensemble un caractère apparemment[57] improvisé et désordonné, relevant tantôt du réflexe législatif presque machinal ou intempestif tantôt de la tentative partielle ou inaboutie d'esquisser un cadre.

§1.- L'apparition des mesures NTIS

88.- La reconstruction historique de l'apparition des mesures NTIS est susceptible de mettre en échec tant la prétention à la nouveauté des mesures NTIS que leur caractère spécial. Si leur nouveauté est liée au fait qu'elles sont fondées sur celle des technologies elles-mêmes, il n'en demeure pas moins que certaines mesures sont relativement anciennes puisqu'elles ont été conçues et appliquées d'abord en dehors du numérique, contrairement à d'autres qui sont « nées » dans le monde numérique (*I*). Si l'expression « autres techniques spéciales d'enquête » employé par le Code de procédure pénale implique une distinction entre spécial et général dans

[56] Quoique la dimension technique des questions puisse échapper au législateur sans que cela ne l'empêche de légiférer alors qu'il ignore les modalités pratiques de réalisation de la mesure envisagée (et donc sans pouvoir pleinement mesurer l'intensité de l'atteinte aux droits fondamentaux ni la suffisance des garde-fous) ; en ce sens, à propos de l'activation à distance d'un appareil électronique, DELAGE Pierre-Jérôme, « À propos de quelques évolutions de la procédure pénale issues de la loi "Justice" du 20 novembre 2023 », *RSC*, n° 3, 2024, p. 638-639.
[57] Insistant au contraire sur le caractère « réfléchi » du processus : VERGES Étienne, « La procédure pénale technicienne (ou l'asphyxie procédurale), Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice », *RSC* 2019 p. 667.

ce contexte, la généalogie des mesures NTIS montre qu'elles sont nées presque toutes de la pratique, ce qui unifie en quelque sorte leurs histoires respectives (*II*).

I.- La distinction entre ancien et nouveau

89.- L'histoire de l'insertion en droit français des mesures d'investigation et de surveillance fondées sur les nouvelles technologies explique leur éclatement, difficilement compréhensible de prime abord, entre la catégorie des techniques spéciales d'enquête et une catégorie résiduelle, les « autres mesures d'enquête » pouvant y être assimilées sans l'être formellement. En effet, dans l'obligation de mettre le cadre juridique français en conformité avec les exigences de la lutte contre la cybercriminalité, le législateur français a choisi, d'une part, d'adapter les mesures d'enquête et d'investigation existantes à la technologie numérique du moment et, d'autre part, d'adopter au fur et à mesure de l'avancement technologique des mesures d'enquête fondées sur de nouvelles technologies et techniques[58].

La distinction entre anciennes mesures d'investigation et de surveillance adaptées au numérique et nouvelles mesures conçues spécialement pour le numérique est sous-jacente dans le Code de procédure pénale lorsque le texte fait référence aux « *autres techniques spéciales d'enquête* »[59] laissant ainsi entendre qu'il y aurait plusieurs types de techniques de cette sorte[60]. Elle devient plus claire grâce la reconstitution de l'apparition de chaque mesure dans le Code de procédure pénale.

90.- Les mesures d'investigation ordinaires ou « classiques » adaptées au numérique ont un champ d'application plus étendu et leur mise en œuvre est accompagnée de garanties élémentaires. Il s'agit des mesures d'enquête comme la conservation rapide de données informatiques stockées[61], la réquisition de documents (ou injonction de produire) ainsi que l'injonction de donner un mot de passe[62], la perquisition et la saisie de données informatiques stockées[63], les interceptions de correspondances émises par la voie des communications électroniques[64] et l'infiltration numérique[65]. A l'inverse, les mesures « nouvelles » sont fondées non sur une mesure d'enquête préexistante mais sur l'évolution des nouvelles techniques et technologies et s'insèrent dans le Code de procédure pénale au moment où ces techniques et technologies ont déjà été utilisées dans le domaine du renseignement ou de la police administrative. Considérées en principe comme plus attentatoires aux droits et libertés, leur champ d'application est limité aux infractions les plus graves et leur utilisation est entourée de davantage de garanties. Il s'agit des mesures comme l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant

[58] Voir BRIGANT Jean-Marie, « Mesures d'investigation face au défi numérique en droit français », *in*, FRANSSEN Vanessa et FLORE Daniel (dir.), *Société numérique et droit pénal*, Bruxelles, Bruylant, 2019, p. 217 et s.
[59] Articles 706-95-11 et s. du CPP.
[60] Voir PARIZOT Raphaële, « Les (autres) techniques spéciales d'enquête, une non-catégorie juridique », *in* PELLE Sébastien (dir.), *Quelles mutations pour la justice pénale du XXIe siècle*, Paris, Dalloz, 2020, p. 72 et s.
[61] Article 60-2 du CPP.
[62] Articles 60-1, 77-1-1 et 99-3 du CPP.
[63] Article 57-1 du CPP.
[64] Articles 100 à 100-8 du CPP.
[65] Article 706-35-1 du CPP.

informatique[66], les sonorisations et fixations d'images de certains lieux ou véhicules[67], la captation des données informatiques[68], la géolocalisation[69] et l'*IMSI-catcher*[70].

91.- L'événement marquant qui a obligé le législateur français à une telle approche progressive et en même temps disparate a sans aucun doute été l'adoption de la Convention du Conseil de l'Europe sur la cybercriminalité. Signée à Budapest le 23 novembre 2001 et ratifiée par 76 États, dont les États-Unis, ce texte constitue le premier instrument contraignant en la matière. Même si cette convention n'a été ratifiée par la France que le 1er mai 2006, son influence sur le droit français a été déterminante depuis sa signature. En effet, dès ce moment-là les interventions du législateur se sont multipliées afin non seulement de conformer, le cas échéant par anticipation, le droit français aux exigences de la Convention[71], mais également et surtout en vue de suivre le rythme des évolutions technologiques et de garantir l'effectivité des poursuites pénales[72]. Parce que la cybercriminalité induit, par hypothèse, la dématérialisation et la déterritorialisation de l'infraction, elle interroge le type de réponse pénale à apporter en posant le choix entre une réponse pénale spécifique propre à une nouvelle forme de délinquance et une réponse pénale classique face à de nouvelles modalités d'une délinquance classique[73]. Aussi bien, l'impact de la Convention de Budapest sur la procédure pénale française est déterminé par la perception que le législateur français s'est faite du cyberespace comme nouveau cadre de la criminalité.

92.- Nombreuses sont les lois qui ont ainsi été adoptées, à un rythme plus que soutenu, visant à assurer la conformité de la procédure pénale française aux nouvelles exigences que l'environnement numérique a imposées à l'enquête. Il s'agit, en particulier, de la *loi relative à la sécurité quotidienne*[74], de la *loi pour la sécurité intérieure*[75], de la *loi portant adaptation de la justice aux évolutions de la criminalité* dite Perben 2[76], de la *loi pour la confiance dans l'économie numérique*[77], de la *loi relative à la prévention de la délinquance*[78], de la *loi relative à la géolocalisation*[79], de la *loi renforçant les dispositions relatives à la lutte contre le terrorisme*[80], de la *loi renforçant la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale*[81], de la *loi de programmation de 2018-2022 et de réforme pour la justice*[82] ainsi que de la *loi d'orientation et de programmation du ministère de la justice 2023-2027*[83]. Elles ont soit adapté les mesures d'investigation et de surveillance classiques à l'environnement numérique soit adopté de

---

[66] Articles 706-95 à 706-95-3 du CPP.
[67] Articles 706-96 à 706-98 du CPP.
[68] Article 706-102-1 du CPP.
[69] Article 230-32 du CPP.
[70] Article 706-95-20 du CPP.
[71] L'article 14§1 de la Convention de Budapest prévoit que chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.
[72] BRIGANT, *op.cit.*, p. 219.
[73] STASIAK Frédéric, « Avant-propos », *in* FRANSSEN Vanessa et FLORE Daniel (dir.), *Société numérique et droit pénal*, Bruxelles, Bruylant, 2019, p.7.
[74] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.
[75] Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.
[76] Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.
[77] Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
[78] Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance.
[79] Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation.
[80] Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.
[81] 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.
[82] Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.
[83] Loi n° 2023-1059 du 20 novembre 2023 d'orientation et de programmation du ministère de la justice 2023-2027.

nouvelles mesures de surveillance et d'investigation. Hétérogènes tant par leur objet que leurs finalités, ces lois ont en commun d'avoir été adoptées après la signature de la Convention de Budapest par la France[84]. Pourtant, elles s'inscrivent davantage dans une démarche de mise à disposition des enquêteurs de mesures d'investigation fondées sur les nouvelles technologies plutôt que de mise en œuvre des dispositions conventionnelles : les références au texte ou aux objectifs de ladite Convention sont loin d'être systématiques dans les travaux préparatoires[85]. Cette genèse des mesures NTIS s'apparente ainsi à un *patchwork* législatif dépourvu de cohérence interne et de considérations systémiques. Cela résulte en partie de la particularité de leur consécration en droit positif qui s'opère généralement à la faveur d'une validation des pratiques.

II.- De la pratique à la loi

93.- Consacrées par le législateur au fil de l'eau, les mesures NTIS ont toutes en commun d'avoir été utilisées en pratique avant d'être introduites dans le droit positif[86]. Leur intégration *ex pos*t est due soit à la pression exercée par la jurisprudence nationale ou européenne, exigeant que des mesures d'investigation et de surveillance aussi intrusives soient exhaustivement réglementées, soit à l'initiative du législateur français, éventuellement « pressé » par les professionnels intéressés[87], choisissant de reconnaître et « sécuriser » les besoins ou possibilités nouveaux issus des évolutions technologiques dans le domaine du numérique et éprouvés par la pratique. Quatre exemples témoignent de cette dynamique.

94.- Tout d'abord, l'exemple des écoutes est bien connu et illustre de manière paradigmatique la pression des Cours : dans le silence total de la loi, l'interception de correspondances, notamment sous la forme d'écoutes téléphoniques[88], était largement pratiquée bien avant l'entrée en vigueur de la loi de 1991, comme l'illustre le fait qu'une commission d'étude de la question des écoutes téléphoniques, présidée par le Premier Président de la Cour de cassation, ait été créée en 1982[89]. En l'absence de tout cadre législatif exprès, la Cour de cassation[90] considérait que le juge d'instruction se trouvait habilité, par l'article 81 du Code de procédure pénale[91], à procéder à tout acte d'information jugé par lui utile à la manifestation de la vérité. L'article 151 du code de procédure pénale[92] lui permettait également de déléguer ces actes par

---

[84] La Convention de Budapest a été signée par la France le 23 novembre 2001.

[85] Comme c'est le cas par exemple des travaux préparatoires à la loi du 18 mars 2003. Voir *infra, §2, I.*

[86] Un parallèle fructueux pourrait être fait avec la façon dont l'expertise par analyse des empreintes génétiques a été introduite en droit français par l'article 28 de la *loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs*. De façon générale, la pratique a précédé la loi, ainsi du recueil d'éléments s'étant détachés naturellement du corps de l'intéressé ou encore de la recherche en parentèle.

[87] En ce sens, à propos de la loi de 2016 (n° 2016-731), à propos du gouvernement « plus à l'écoute des praticiens que des justiciables », VERGES Etienne, « La procédure pénale à son point d'équilibre (À propos de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale) », *RSC* 2016, p. 551.

[88] Les « écoutes téléphoniques » traditionnelles ne constituent pas les seules mesures susceptibles d'entrer dans le champ plus vaste du droit positif actuel.

[89] Commission nationale de contrôle des interceptions de sécurité, premier rapport d'activité 1991-1992, annexes, 1993, La Documentation française. Le premier rapport de la Commission nationale de contrôle des interceptions de sécurité compte 5 691 interceptions judiciaires réalisées en 1991.

[90] Crim. 9 oct. 1980, no 80-93.140 ; Crim. 13 juin 1989 (*Derrien*), *Bull. crim.*, n° 254.

[91] Article 81 du Code de procédure pénale : « Le juge d'instruction procède, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité. Il instruit à charge et à décharge (...) ».

[92] Article 151 Code de procédure pénale : « Le juge d'instruction peut requérir par commission rogatoire tout juge de son tribunal, tout juge d'instruction ou tout officier de police judiciaire, qui en avise dans ce cas le procureur

commission rogatoire. Les seules conditions requises pour pouvoir procéder à une telle mesure étaient : l'existence d'un fait dont le juge d'instruction est saisi[93] ; l'absence d'artifice et de stratagème[94] ; une personne concernée, qui pouvait être un témoin[95], toute personne intéressée sur qui ne pèsent pas des indices[96], ou l'inculpé[97]. Si, dans un premier temps, la chambre criminelle de la Cour de cassation ne s'est pas prononcée expressément sur l'incompatibilité du régime des écoutes avec l'article 8 de la CESDH[98], par un arrêt du 24 novembre 1989, l'Assemblée plénière de la Cour de cassation a reconnu pour la première fois que l'écoute et l'enregistrement des propos constituaient des cas légaux d'ingérence d'une autorité publique dans la vie privée au sens de l'article 8 de la CESDH et que le fait de procéder à l'écoute et à l'enregistrement relevait de la compétence exclusive du juge d'instruction[99]. Le scepticisme, voire l'hostilité, d'une partie de la doctrine à l'égard de la légalité de ces mesures[100] trouvèrent cependant écho dans deux arrêts rendus par la CEDH le 24 avril 1990. La Cour condamna la France[101] pour violation de l'article 8 de la Convention, qui protège le droit à la vie privée et au secret des correspondances, auquel il ne peut être porté atteinte que par une loi et pour des motifs de sécurité publique. La Cour considéra que les écoutes téléphoniques telles que mises en œuvre par la pratique judiciaire ne répondaient pas aux exigences minimales, en particulier de prévision légale[102], de l'article 8 CESDH[103]. Une loi fixant les modalités et les limites des écoutes téléphoniques s'avéra donc nécessaire[104]. L'arrêt de la CEDH fut suivi par de nombreux arrêts rendus par la Chambre criminelle, qui, dans une tentative d'alignement avec la jurisprudence européenne, exigèrent une nouvelle condition pour la régularité des écoutes téléphoniques, à savoir que l'infraction en cause « constitue, soit un crime, soit un délit portant gravement atteinte à l'ordre public »[105], cette atteinte grave devant être déduite par le juge des « éléments de l'espèce »[106]. Un peu plus d'un an après la condamnation de la France par la

---

de la République, de procéder aux actes d'information qu'il estime nécessaires dans les lieux où chacun d'eux est territorialement compétent (...) ».

[93] Crim. 23 juill. 1985, *Bull. crim.*, n° 275.

[94] Crim. 12 juin 1952, *JCP* 1952.II.7241, note Brouchot.

[95] Crim. 23 avr. 1981, *Bull. crim.*, n° 117.

[96] Crim. 26 nov. 1990, *Bull. crim.*, n° 401.

[97] Crim. 9 oct. 1980, *Bull. crim.*, n° 255.

[98] Crim. 24 avr. 1984, *D.* 1986.

[99] Cass., Ass. Plén., 24 nov. 1989 n° 89-84.439.

[100] En ce sens, CHAMBON Pierre, « De la légalité des écoutes téléphoniques concernant un inculpé, ordonnées par le juge d'instruction », *JCP*, 1981. I. 3029.

[101] CEDH, 24 avril 1990, *Kruslin et époux Huvig c. France*, nos 11801/85 et 11105/84.

[102] « [L]e système n'offre pas pour le moment des sauvegardes adéquates contre divers abus à redouter. Par exemple, rien ne définit les catégories de personnes susceptibles d'être mises sous écoute judiciaire, ni la nature des infractions pouvant y donner lieu; rien n'astreint le juge à fixer une limite à la durée de l'exécution de la mesure; rien non plus ne précise les conditions d'établissement des procès-verbaux de synthèse consignant les conversations interceptées, ni les précautions à prendre pour communiquer intacts et complets les enregistrements réalisés, aux fins de contrôle éventuel par le juge - qui ne peut guère se rendre sur place pour vérifier le nombre et la longueur des bandes magnétiques originales - et par la défense, ni les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction desdites bandes, notamment après non-lieu ou relaxe. Les renseignements donnés par le Gouvernement sur ces différents points révèlent au mieux l'existence d'une pratique, dépourvue de force contraignante en l'absence de texte ou de jurisprudence », point 34 de l'arrêt.

[103] « En résumé, le droit français, écrit et non écrit, n'indique pas avec assez de clarté l'étendue et les modalités d'exercice du pouvoir d'appréciation des autorités dans le domaine considéré. Il en allait encore davantage ainsi à l'époque des faits des deux causes, de sorte que les requérants n'ont pas joui du degré minimal de protection voulu par la prééminence du droit dans une société démocratique. La Cour considère qu'il y a donc eu violation de l'article 8 de la Convention ». CEDH, 24 avril 1990, *Huvig c. France*, n° 11105/84, §.50.

[104] KOERING-JOULIN Renée, « De l'art de faire l'économie d'une loi », *D.* 1990. Chron. 187 ; PRADEL Jean, « Écoutes téléphoniques et Convention européenne des droits de l'homme, (à propos de Cass., Ass. plén., 24 novembre 1989, *affaire Baribeau* », *D.* 1990.34), *Recueil Dalloz*, 1990, Chronique, p. 15-20.

[105] Crim. 15 mai 1990, n° 90-80.827.

[106] Crim. 26 nov. 1990, *Bull. crim.*, n° 401; 19 mars 1991, *D.* 1991. IR.142.

CEDH, la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques [107] entra en vigueur. D'après les travaux préparatoires, il s'agissait de donner un cadre juridique rénové à une technique ancienne, « l'écoute téléphonique », discutée de longue date[108], en définissant le régime applicable, procédant ce faisant à la mise en conformité du droit français avec les exigences européennes.

95.- Par la suite, l'article 81 du CPP a servi de fondement à la pratique de la géolocalisation avant que cette mesure ne soit prévue par la loi. Il doit être noté que le défaut de base juridique n'a pas empêché le recours à la captation des données par les services de renseignement ou à l'infiltration numérique par les services de renseignement ou par les enquêteurs bien avant la codification de ces mesures. En effet, l'émergence du cyberespace en tant que nouvel espace de commission des infractions, que ce soit par le biais des réseaux sociaux ou du *dark web*, a rendu indispensable l'infiltration « à distance » afin que les autorités puissent lutter efficacement contre ces formes de criminalité. Compte tenu de l'efficacité de cette mesure dans ce contexte, son insertion en droit positif a été motivée non seulement par le besoin d'assurer la protection des personnes concernées mais également par le souci de pouvoir intégrer en toute légalité les éléments de preuve qu'elle permettait de recueillir dans la procédure pénale[109].

96.- La pratique a été aussi le fondement des réquisitions de données informatiques. En effet, le premier pouvoir de réquisition, prévu explicitement dans le Code de procédure pénale en 1985 [110] lorsqu'ont été introduits les articles 60 et 77-1, respectivement pour l'enquête de flagrance et pour l'enquête préliminaire, ne concernait que des constatations ou des examens techniques ou scientifiques. Or, cette procédure n'a pas été considérée comme la source de compétence des officiers de police judiciaire permettant de requérir des données détenues par des entités privées[111]. Aussi ces dernières faisait-elles l'objet de « *réquisitions de service* » ou

---

[107] *Loi 91-646 du 10 juillet 1991 relative au secret des correspondance émises par la voie des communications électroniques*.

[108] Rapport de M. Rudloff, Doc. Sénat, n° 403 p. 5.

[109] En effet, selon Myriam Quéméner, il apparaissait « fondamental que les services d'enquête aient les compétences techniques et les moyens juridiques pour récupérer ces indices afin qu'ils puissent être utilisés dans les procédures judiciaires ». Voir QUEMENER Myriam, « Les techniques spéciales d'enquête », *Répertoire de droit pénal et de procédure pénale Dalloz*.

[110] Loi n° 85-1407 du 30 décembre 1985 portant diverses dispositions de procédure pénale et de droit pénal, JORF, 31 décembre 1985, p.15505 ; Voir LASSALLE Maxime, « La mue des réquisitions, signe avant-coureur d'une transformation plus large ? », *AJ Pénal*, 2023, n°11, p. 491.

[111] C'était le cas en particulier pour les données bancaires. La Cour de cassation, suivant la cour d'appel de Grenoble (possibilité pour la police judiciaire d'obtenir d'une banque, dans le cadre d'une enquête préliminaire, des relevés de compte sans avoir à respecter la procédure de l'article 77-1 du Code de procédure pénale ; cour d'appel de Grenoble 7 juillet 2000, *D.* 2001, p. 1128 ; Redon Michel, « Article 77-1 du Code de procédure pénale : un salutaire rappel des principes », *D.* 2001, p. 1128) a ainsi affirmé que « *la police judiciaire peut également, selon une jurisprudence constante, dans le cadre de ses enquêtes, solliciter et obtenir d'un établissement bancaire des relevés de compte, sans que puisse être opposé le secret bancaire* » (Crim., 24 octobre 2001, n°00-86.440). L'article 77-1 n'avait pas vocation à créer un pouvoir de réquisitions de document mais à créer un pouvoir de nomination d'expert dans le cadre d'une enquête préliminaire ou de flagrance (Crim., 14 sept. 2005, 05-84.021 ; Voir aussi Crim., 19 mars 2014 n°10-88725 et 13-88616.) Cette interprétation est confirmée par les travaux préparatoires de la loi de 1985. Robert Badinter, alors garde des Sceaux, avait affirmé qu'il s'agissait « *d'éviter l'ouverture d'informations judiciaires lorsque celles-ci ne sont pas indispensables : tout le monde en convient, dans cette perspective, des examens techniques ou scientifiques pourront désormais être effectués au stade de l'enquête, sous le contrôle du parquet* » (J.O. Sénat, Séance du 23 octobre 1985, p. 2393. Cité par Fauchon Pierre, *Rapport n°486* (97-98), Commission des lois, « Alternative aux poursuites, renfort de l'efficacité de la procédure pénale et délégation aux greffiers des attributions dévolues par la loi aux greffiers en chef », article 7.). Le rapport du Sénat souligne de même la nécessité de ne plus avoir à ouvrir une information judiciaire pour des actes d'enquête relativement simples (*Rapport fait au nom de la commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale sur le projet de loi, adopté par l'Assemblée*

de réquisitions « *aux fins de fournir un service* »[112], soit des réquisitions dénuées de tout formalisme et relevant de la simple pratique[113].

97.- Enfin, la nécessité de « sécuriser » les procédures judiciaires semble avoir également motivé l'encadrement législatif de la mesure de fixation d'images. Utilisée par les services de police depuis les années 1980 sans être régie par un texte spécifique, cette mesure relevait jusqu'à la loi du 9 mars 2004 de la notion de pratique policière régulièrement utilisée pour décrire certaines mesures effectuées par les enquêteurs qui ne sont pas encadrées par le droit[114]. Même si cette catégorie assez vague n'est pas censée inclure d'opérations attentatoires aux droits des personnes, lors des discussions au sein de la Commission des lois du Sénat portant sur ce texte, des parlementaires ont considéré que, puisque la technique existait déjà, il valait mieux la réglementer que l'ignorer[115], traduisant ainsi la vision selon laquelle une pratique, potentiellement ou manifestement illicite, devrait plutôt être admise et encadrée qu'ignorée ou interdite[116].

98.- Le passage d'une pratique des services de police et de renseignement à une technique d'enquête réglementée a le mérite d'encadrer *a posteriori* dans le droit positif une technique spéciale d'enquête dont les points problématiques ont déjà été relevés par la jurisprudence, par les acteurs de la procédure pénale, par la doctrine, voire par des rapports des organes chargés de veiller sur leur application à titre expérimental[117]. La consécration législative qui en sanctionne la légitimité vient clarifier les conditions de mise en œuvre de la mesure et assurer, théoriquement, le respect des droits fondamentaux. Toutefois, cela n'empêche pas que l'adaptation des mesures d'investigation et de surveillances ordinaires à l'environnement numérique et aux exigences de la lutte contre la cybercriminalité puisse être aussi source d'imprécisions ou d'incohérence, dues au fait que l'adaptation en question n'a pas pris en compte l'ensemble des implications que la dématérialisation dans la recherche de la preuve pourrait avoir sur la procédure pénale.

Nationale, relatif à la simplification des procédures et à l'exécution des décisions pénales, par JOLIBOIS Charles, Annexe au procès-verbal de la séance du 16 octobre 1985, p. 24.)

[112] REDON Michel, « Article 77-1 du Code de procédure pénale : un salutaire rappel des principes », *op.cit.*

[113] En parlant de « *salutaire rappel des principes* », un magistrat commentant cet arrêt avait conclu que « *si l'enquête préliminaire doit obéir à des règles protectrices des droits individuels* », elle *« ne peut pas non plus être entravée par davantage d'obstacles supplémentaires* » (REDON Michel, « Article 77-1 du Code de procédure pénale : un salutaire rappel des principes », *op.cit.*). Or, il est permis de s'interroger sur lesdits obstacles supplémentaires à défaut d'en identifier d'autres. L'autorisation du procureur de la République était limitée aux réquisitions visant à des constatations ou à des examens techniques ou scientifiques, elle n'était pas nécessaire pour toutes les autres formes de réquisition qui ne bénéficiaient donc d'aucune protection (Crim., 8 novembre 2005, n°05-84822**,** parmi les documents collectés, il y avait des relevés bancaires).

[114] Voir, MERMOZ Vincent, *Les indices en procédure pénale*, Thèse soutenue à l'Université Paris-Saclay (Sceaux), 2019, p. 34.

[115] Sénat, Commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, examen du rapport de M. François Zocchetto sur le projet de loi n° 314 portant adaptation de la justice aux évolutions de la criminalité, mercredi 24 septembre 2003. V. http:// www.senat.fr/commission/loi/lois030927.html#toc2

[116] Selon Jean PRADEL, il était plus judicieux de fonder juridiquement les techniques spéciales d'enquête pour protéger le mis en cause et les tiers, éviter des atteintes au principe de loyauté de la preuve ou au contradictoire et contrôler l'action de la police. Voir PRADEL Jean, « De l'enquête pénale proactive : suggestions pour un statut légal », *Dalloz*, 1998, p. 57.

[117] A propos de l'articulation et des liens entre techniques d'enquête pénale et techniques de renseignement, voir GUILLARD Antonin, « Sonorisation et fixation d'images au croisement de la procédure pénale et du renseignement », *AJ Pénal*, n° 11, 2023, p. 484 et s.

§2.- L'évolution des mesures NTIS

99.- L'étude de l'évolution des mesures NTIS dévoile deux mouvements parallèles qui, tous deux, témoignent du développement de techniques intrusives au moyen d'une politique des petits pas, dépourvue de vision d'ensemble, visant surtout à accroître le pouvoir des enquêteurs par le recours à une ou à la technique[118] : d'une part, l'adaptation des mesures d'investigation « classiques » au numérique (*I*) et, d'autre part, l'extension progressive mais continue de la portée des mesures NTIS consacrées par le législateur (*II*).

I. - Du tangible au cybermonde : l'adaptation heurtée des outils de l'enquête

100.- Les mesures NTIS fondées sur des mesures d'investigation ordinaires ne sont pas en soi des opérations *sui generis*, mais bien plutôt des applications particulières à l'environnement numérique de mesures d'investigation et de surveillance portant sur des objets ou des documents[119]. Tel est notamment le cas des perquisitions et des saisies informatiques ainsi que des réquisitions informatiques. Si les notions d'objet et de document peuvent, en raison de leur caractère général, s'adapter aux évolutions techniques et ainsi englober les données informatiques[120], le législateur français a opté pour une référence explicite aux données informatiques sous l'influence de la Convention sur la cybercriminalité. Ce souci de précision, qui tranche avec la tendance contraire consistant à exploiter la généralité et le caractère compréhensif de dispositions existantes, favorise la spécification du champ numérique et pose la question de son autonomie ou singularité à raison de sa nature ainsi que du régime devant en découler.

101.- Le lien avec la Convention sur la cybercriminalité est plus clair s'agissant des mesures NTIS fondées sur des mesures d'investigation et de surveillance ordinaires, même si dans la plupart des cas il n'apparaît que de manière discrète dans les travaux législatifs. A cet égard, l'étude des travaux préparatoires de la loi du 18 mars 2003 pour la sécurité intérieure permet d'établir que le législateur français a voulu prendre acte des dispositions de la Convention sur la cybercriminalité de Budapest du 21 novembre 2001 consacrant en son article 19 la notion de « perquisition informatique ». Au moment de la discussion de la loi, cette convention était signée mais pas encore ratifiée par la France[121]. Au contraire, les travaux préparatoires relatifs

---

[118] Voir en ce sens, VERGES Étienne, « La procédure pénale technicienne (ou l'asphyxie procédurale), Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice », *RSC* 2019 p. 667.

[119] Voir en ce sens, BRIGANT Jean-Marie, *op.cit.*, p. 220-221.

[120] Voir, à titre d'exemple, Crim., 8 août 2007, n° 07-84.252, *Bull. crim.*, 2007, n° 188 ; *Procédures* 2007, comm. 264, obs. J. BUISSON ; *Droit pénal*, 2007, chr. 6, obs. A. LEPAGE ; Crim., 17 décembre 2002, n° 02-83.679, *Bull. crim.*, 2002, n° 231.

[121] *Rapport n° 508 enregistré à la Présidence de l'Assemblée nationale le 18 déc. 2002 fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi, adopté par le Sénat après déclaration d'urgence, pour la sécurité intérieure* : « Article additionnel après l'article 8 (art. 57-1 [nouveau] du Code de procédure pénale). La Commission a été saisie d'un amendement du rapporteur autorisant les officiers de police judiciaire à procéder à des perquisitions informatiques et à étendre celles-ci aux données et systèmes accessibles depuis le système initial. Tout en déclarant partager l'objectif poursuivi par l'amendement du rapporteur, M. Xavier de Roux s'est interrogé sur le sort distinct fait aux systèmes informatiques situés en dehors du territoire national, dont la perquisition requiert le consentement préalable de l'intéressé. Le rapporteur ayant précisé qu'il s'agissait, par cette précision, de se conformer à la Convention du Conseil de l'Europe sur la cybercriminalité, que la France avait signée mais pas encore ratifiée, M. Xavier de Roux a fait part de sa préférence pour une rédaction plus générale qui mentionnerait simplement les conditions d'accès

à la conservation rapide des données de connexion, mesure issue directement de la Convention sur la cybercriminalité et introduite également par la loi du 18 mars 2003[122], ne contiennent aucune référence à cette Convention[123].

102.- L'ambiguïté entourant le lien entre la Convention sur la cybercriminalité et les mesures NTIS fondées sur des mesures d'investigation ordinaires retentit également sur les textes législatifs relatifs à ces mesures. L'exemple des perquisitions et des saisies informatiques ainsi que celui des réquisitions de données illustrent le manque de précision du droit positif qui est dû à une approche fragmentée de la réforme des mesures d'investigation, qui ne tient pas compte de la systématique à laquelle prétend le code de procédure pénale.

103.- En premier lieu, l'application des perquisitions et des saisies aux données informatiques a été réalisée sans que le législateur français ne définisse au préalable cette dernière notion en droit interne. L'expression de données informatiques figure au premier alinéa de l'article 56 CPP depuis 2004[124] alors que la mesure a été appliquée à ce type de données depuis 2003[125]. Toutefois, pour la définition des données informatiques, il faut se référer à celle inscrite dans la Convention de Budapest, à savoir : « *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* »[126]. S'agissant des perquisitions, l'imprécision du texte permet l'extension de la mesure de perquisition à tout appareil se servant de l'informatique ou contenant des applications informatiques. Faute de prévisions législatives, l'exploitation pendant la garde à vue du téléphone portable de son possesseur a été considérée par la jurisprudence comme une mesure « assimilable à une perquisition »[127]. Toutefois, l'imprécision du texte est susceptible de poser des difficultés de mise en œuvre. Au sens strict, la notion de « perquisitions informatiques » renvoie uniquement à des perquisitions (« classiques ») appliquées au matériel informatique. Toutefois, la spécificité de la perquisition informatique réside dans le fait que l'on doit distinguer le contenant, qui est le disque dur ou tout support numérique, voire un simple code d'accès, du « contenu » qu'il renferme, c'est-à-dire des fichiers. Ainsi, toute appréhension de données informatiques dans le cadre de la recherche des preuves par les enquêteurs n'est pas une « perquisition informatique » au sens des articles 56, 57-1, 76, alinéa 3, et 97, alinéa 1, du CPP. Cette spécificité pose de nouvelles questions juridiques et pratiques. En effet, l'accès distant « manifeste un début de dématérialisation »[128] et en cela change la physionomie de la perquisition. Ces perquisitions se singularisent par leur objet même, l'« informatique », empreint d'immatérialité, de volatilité, alors que les règles processuelles et l'esprit des perquisitions « classiques » se sont bâtis autour « *du tangible, du temps et de l'espace* »[129]. Si

---

prévues par les engagements internationaux en vigueur. Le rapporteur s'étant rallié à cette rédaction, la Commission a adopté l'amendement ainsi rectifié (amendement n° 67) ».

[122] L'article 18 de la *loi n° 2003-239 du 18 mars 2003* a inséré la mesure de la conservation rapide des données informatiques stockées en droit français par la création de l'article 60-1 du CPP.

[123] La seule référence à la Convention sur la cybercriminalité se fait à l'amendement n° 67 portant sur les perquisitions informatiques.

[124] Par l'article 44 de la *loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*.

[125] En vertu de la *loi du 18 mars 2003 pour la sécurité intérieure*.

[126] Article 1er b, de la Convention sur la cybercriminalité.

[127] Crim. 12 janv. 2021, n° 20-84.045, *D.* 2021. 82; *AJ pénal* 2021. 214, obs. E. Clément ; *Dalloz IP/IT* 2021. 294, obs. O. de Maison Rouge ; *RSC* 2021. 128, obs. R. Parizot.

[128] DECIMA Olivier, « Du piratage informatique aux perquisitions et saisies numériques ? », *AJ Pénal* 2017 p. 315.

[129] BELLOIR Philippe, « Perquisition et saisie en matière de lutte contre la cybercriminalité », *RLDI* 2010/60, p. 71.

la distinction entre perquisition informatique et perquisition « numérique »[130] – cette dernière s'effectuant à distance sans aucun contact physique avec l'objet de la perquisition – découle des cas de figure prévus par l'article 57-1 du CPP, le législateur n'a pas envisagé les conséquences qu'elle pouvait avoir sur l'application de cette mesure d'investigation. Il en est ainsi à propos des saisies de données informatiques lesquelles peuvent également s'opérer de deux manières alternatives, à savoir : par la saisie de l'objet matériel au sein duquel se trouvent les données informatiques ou par la réalisation d'une copie de ces données[131].

104.- En deuxième lieu, cette distinction entre ce que recouvre une mesure d'investigation dans sa forme ordinaire et son nouveau champ d'application à la suite de son adaptation, par la loi, au numérique s'observe également dans le cas des réquisitions de données. Les textes prévoient deux types de réquisition : d'une part, les réquisitions télématiques ou informatiques de l'article 60-2 du CPP, qui permettent d'accéder à des bases de données publiques ou privées contenant des informations utiles à la manifestation de la vérité se trouvant dans des systèmes informatiques ou traitements de données nominatives[132] ; d'autre part, les réquisitions de documents par lesquelles le législateur a reconnu aux enquêteurs « un pouvoir de réquisition de portée générale, au-delà des spécificités liées aux systèmes informatiques »[133] avec la création des articles 60-1 et 77-1-1 du Code de procédure pénale[134]. Les deux textes et les deux types de réquisition (réquisitions télématiques et réquisitions de documents) coexistent sans que leurs rôles respectifs ne soient clairement dessinés. On peut penser que les réquisitions télématiques sont plus « technologiques » mais il est difficile de circonscrire quel est leur champ d'application réel.

105.- En dernier lieu, dans le domaine des réquisitions, au sein duquel s'insère la conservation rapide des données informatiques stockées, les dispositions du Code de procédure pénale restent relativement floues quant à la définition du champ d'application de cette mesure. L'alinéa 2 de l'article 60-2 du CPP ne précise pas explicitement le(s) type(s) de données concernées par la réquisition relative à la conservation rapide des données informatiques. La différence entre les termes utilisés dans la Convention sur la cybercriminalité et ceux du Code de procédure pénale, à savoir « *données électroniques spécifiées, y compris celles relatives au trafic* »[135], d'une part, et « *contenu des informations consultées* », d'autre part, laisse penser que le champ d'application du Code de procédure pénale est plus étroit que celui de la Convention. En effet, la notion de « contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs » utilisée dans l'article 60-2 al. 2 du CPP semble – c'est une tautologie –, se référer uniquement aux données relatives au contenu. Pourtant, une circulaire du 2 décembre 2016 précise que les articles 60-2 al. 2, 77-1-2 al. 2 et 99-4 al. 2 du CPP ne visent pas « le contenu des correspondances échangées ». Elle indique ensuite que les articles 60-1, 77-1-1, 99-3 et 60-2 al. 1er (qui consacrent les pouvoirs de réquisition et de mise à disposition de données informatiques) ne distinguent ni les catégories de données numériques, de type

---

[130] Voir DECIMA, *op. cit.*, p. 315.
[131] Articles 56 al. 5 et 97 al. 3 du CPP.
[132] Il s'agissait « d'obtenir dans des délais rapides des informations contenues dans des systèmes informatiques » : ESTROSI, Christian, *Rapport fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi, adopté par le Sénat après déclaration d'urgence (n°381), pour la sécurité intérieure*, enregistré à la Présidence de l'Assemblée nationale le 18 décembre 2002, p. 67.
[133] WARSMANN Jean-Luc, *Rapport fait au nom de la Commission des lois sur le projet de loi (n°784) portant adaptation de la justice aux évolutions de la criminalité*, déposé le 20 mai 2003, art. 28.
[134] *Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.*
[135] Article 16§1 de la Convention.

« contenu » ou « contenant », ni leur localisation[136]. Or, le partage entre, d'une part, la conservation rapide désignée dans le CPP par la possibilité de « préserver » le contenu des informations consultées et, d'autre part, les réquisitions et mises à disposition de données informatiques stockées se perd ensuite là où la circulaire ne distingue plus et vise de manière générale et indifféremment tous ces textes comme fondement permettant d'obtenir les facturations détaillées des communications, la localisation d'un téléphone, les données stockées en nuage, les données publiées via des réseaux sociaux, voire les données de connexion en général[137]. De surcroît, dans le Rapport d'évaluation de la Convention sur la cybercriminalité, il est mentionné que la conservation rapide des données informatiques stockées en droit français s'applique à toutes les données[138]. A défaut d'une interprétation jurisprudentielle claire, un certain doute persiste que les entretiens n'ont pas permis de dissiper car l'injonction de conservation rapide des données informatiques (comprise comme la mesure visée par l'alinéa 2 de l'art. 60-2 du CPP) est en réalité très peu utilisée par les enquêteurs. Cela dit, il pourrait en être autrement à l'avenir compte tenu de la jurisprudence de la CJUE aboutissant à valoriser l'usage de ce mode de conservation en tant que mesure compensatoire à l'impossibilité juridique de recourir à la conservation généralisée et indifférenciée aux fins de criminalité grave ou à l'impraticabilité opérationnelle de recourir à la conservation ciblée[139].

106.- Ces difficultés persistent en droit positif bien que la quasi-totalité des mesures NTIS aient subi plusieurs modifications législatives depuis leur première apparition en droit français. En effet, la généalogie des mesures montre que les différentes réformes ont poursuivi comme objectif principal l'extension de leur champ d'application au regard soit des infractions concernées soit du type d'enquête pénale dans le cadre duquel elles peuvent être autorisées.

II.- De l'exceptionnel au droit commun

107.- L'interception des correspondances offre un poste d'observation privilégié et illustre l'expansion continue du champ d'application de mesures d'abord étroitement réglementées. Ainsi, l'interception des correspondances émises par la voie des communications électroniques, introduite par la loi du 10 juillet 1991 dans le cadre de l'instruction pour des infractions punies d'une peine égale ou supérieure à trois ans d'emprisonnement[140], a été admise en 2004 dans le cadre de l'enquête préliminaire ou de l'enquête de flagrance en matière de lutte contre la criminalité organisée et moyennant l'autorisation du juge des libertés et de la détention[141]. Si la loi du 23 mars 2019[142] a porté de deux à trois ans le quantum de la peine d'emprisonnement exigé pour qu'une telle interception ait lieu en matière délictuelle, la mesure est applicable pour

---

[136] *Circulaire du 2 décembre 2016 de présentation des dispositions de la loi n° 2016-73 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relative au renforcement du dispositif en matière de lutte contre la délinquance et la criminalité organisée*, p. 17.
[137] *Idem*, p. 24.
[138] Comité de la Convention sur la cybercriminalité (T-CY), Rapport d'évaluation, Mise en œuvre des dispositions de la Convention de Budapest en matière de préservation des données, Strasbourg, 25 janvier 2013, (2012) 10 REV, p. 28.
[139] Voir *infra*, Troisième partie, étant noté cependant que la compréhension étendue par la chambre criminelle de la notion de conservation rapide tempère cette perspective.
[140] Article 2 de la *loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques*.
[141] *Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité*.
[142] *Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*.

l'ensemble des crimes[143]. De plus, l'article 100 du CPP[144], tel que modifié par la loi de 2019, admet la possibilité d'autoriser l'interception de la ligne de la victime à la demande de celle-ci en cas de délit puni d'une peine d'emprisonnement commis par la voie des communications électroniques.

108.- Dans le même sens d'une expansion continue – non plus du domaine mais des modalités de mise en œuvre –, s'agissant des perquisitions, la loi du 13 novembre 2014[145] a introduit un deuxième alinéa à l'article 57-1 du CPP ajoutant aux côtés de la perquisition informatique effectuée sur place, c'est-à-dire sur un système informatique trouvé sur les lieux de la perquisition, la possibilité d'une perquisition informatique effectuée à distance en utilisant le système informatique des enquêteurs dans le but d'accéder à des données stockées dans un autre système informatique.
En matière de réquisitions, le législateur a ajouté en 2004[146] aux réquisitions télématiques ou informatiques introduites l'année d'avant[147] les réquisitions de documents prévues par les articles 60-1 et 77-1-1 du CPP.
Tel est encore le cas de l'infiltration numérique. Créée par l'article 17 de la *loi n° 2007-297*, l'enquête sous pseudonyme, dite infiltration numérique ou encore « cyberpatrouille », a été prévue d'abord pour les jeux en ligne, puis pour la contrefaçon par l'administration des douanes et ensuite pour la criminalité financière depuis la *loi du 6 décembre 2013*[148]. Elle a connu un élargissement progressif de son champ d'application jusqu'à devenir une procédure de droit commun avec la *loi n°2019-22 du 23 mars 2019*[149].

109.- Ce mouvement d'une procédure conçue initialement comme exceptionnelle (ou limitée) vers une procédure de droit commun par le biais de la généralisation de l'application de la mesure NTIS s'observe également à propos de l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique, ainsi que s'agissant des « autres techniques spéciales d'enquête » prévues aux articles 706-95-11 et suivants du CPP. Introduit par la *loi n° 2016-731 du 3 juin 2016*[150], l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique était initialement prévu uniquement pour la criminalité organisée. Toutefois, son champ d'application a été étendu aux crimes par la *loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*[151]. Pareille extension a été réalisée à propos du champ d'application de la fixation d'images et de la sonorisation de certains lieux ou véhicules. Introduite par la *loi du 9 mars 2004* uniquement dans le cadre de l'instruction pour des infractions relevant de la criminalité et de la délinquance organisées, la mesure a été par la suite autorisée – tout comme la captation des données

---

[143] Article 100 al. 1er CPP.
[144] Article 100 dernier alinéa : « En cas de délit puni d'une peine d'emprisonnement commis par la voie des communications électroniques sur la ligne de la victime, l'interception peut également être autorisée, selon les mêmes modalités, si elle intervient sur cette ligne à la demande de la victime ».
[145] *Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.*
[146] *Loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.*
[147] Par l'article 18 de la *loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.*
[148] *Loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière.*
[149] Article 45 et 109-XIII de la loi.
[150] *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.*
[151] Cet élargissement a par ailleurs répondu à certaines interrogations formulées à la suite de la rédaction initiale de 2016 quant aux choix des infractions concernées. Il semblait surprenant que des infractions graves telles que le meurtre soient exclues du champ d'application de cette mesure tandis que celle-ci avait un potentiel élevé de contribuer à la recherche de la vérité en la matière.

informatiques[152] – dans celui de l'enquête par la loi du 3 juin 2016[153] avant d'être étendue à tous les crimes par la *loi du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*. Toutefois, cette dernière extension à tous les crimes a été déclarée contraire à la Constitution[154], ce qui a obligé le législateur à limiter le recours à cette mesure uniquement au cadre de l'enquête et de l'instruction pour les infractions énumérées par les articles 706-73 et 706-73-1 du CPP. Le même mouvement d'extension s'observe en outre à propos des acteurs de la procédure pénale et plus précisément à propos du pouvoir de recourir à ces mesures[155]. Tel est le cas du pouvoir de prendre des réquisitions, prévu à l'article 60-1 du CPP. Initialement dévolu aux seuls OPJ, ce pouvoir a été par la suite élargi aux APJ[156] ainsi qu'aux assistants d'enquête[157].

Section 2 : Régimes des mesures NTIS

110.- La construction du régime juridique des mesures NTIS est le fruit de réformes nombreuses dévoilant un intérêt manifeste du législateur pour ces mesures mais une attention inégale aux effets systémiques de ses interventions répétées par lesquelles il paraît plutôt courir après les pratiques et les techniques, lorsqu'il n'est pas astreint de légiférer pour répondre aux contraintes européennes ou nationales.

Issues de la pratique et consacrés dans le droit positif par différentes lois, les mesures NTIS n'ont pas fait l'objet d'une consécration systémique ou coordonnée au sein de la procédure pénale française. Au contraire, chaque intervention du législateur pour valider une mesure déjà employée en pratique a eu un caractère ponctuel et aucune n'a procédé d'une vision d'ensemble, à la notable exception près de l'introduction en droit français des (autres) « techniques spéciales d'enquête », effectuée par le biais d'une même loi et gouvernées par les mêmes règles[158]. Le régime commun des « techniques spéciales d'enquête » contraste avec la consécration disparate des autres mesures NTIS que le législateur s'est contenté d'insérer dans les cadres juridiques préexistants, sans pour autant les articuler entre elles. Tel est notamment le cas des mesures NTIS fondées sur des mesures d'investigation et de surveillance ordinaires, comme les perquisitions et les saisies informatiques qui s'insèrent dans la catégorie des perquisitions et des saisies classiques, ou des réquisitions de données informatiques, y compris la conservation rapide des données de connexion, qui relèvent de la catégorie des réquisitions judiciaires, ou bien encore des infiltrations numériques qui complètent la catégorie des infiltrations classiques, ou bien enfin l'interception des correspondances émises par la voie des communications électroniques qui enrichit l'ancienne catégorie des écoutes téléphoniques. Si ce choix assure une certaine uniformité de leur régime juridique dans la mesure où elles s'insèrent toutes dans des cadres juridiques disposant déjà de leurs propres règles, acteurs et mécanismes de contrôle, cette uniformité n'est qu'apparente. Par-delà l'existence de traits communs, la consécration des

---

[152] Initialement cantonnée à l'instruction préparatoire, la mesure a été étendue à l'enquête par la *loi n°2016-731 du 3 juin 2016*.

[153] *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*.

[154] Cons. const., 21 mars 2019, n°2019-778 DC, sp. point 165.

[155] Voir en ce sens, VERGÈS Étienne, « La procédure pénale technicienne (ou l'asphyxie procédurale), Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice », *RSC* 2019 p. 667.

[156] Article 47 de la loi 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

[157] Article 18 de la loi 2023-22 du 24 janvier 2023 d'orientation et de programmation du ministère de l'intérieur.

[158] *Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice*. Les mesures faisant partie de ces « techniques spéciales d'enquête » se trouvent dans le Chapitre II du Titre XXV du Livre 4 du Code de procédure pénale.

mesures NTIS en droit positif présente aussi d'importantes différences de sorte que le singulier doit céder la place au pluriel : ce sont plusieurs régimes qui coexistent et non un seul pour l'ensemble des mesures NTIS.
Fondées sur une règle assez classique et simple selon laquelle « *plus un acte d'investigation est intrusif dans les droits et libertés fondamentaux, plus il doit bénéficier d'un régime protecteur »*[159], ces différences révèlent une hiérarchisation implicite des mesures NTIS selon la gravité de l'atteinte aux droits et libertés des personnes concernées. Toutefois, à défaut d'une conceptualisation claire des critères du caractère intrusif des actes d'investigation, cette gradation manque de rigueur, ce qui aboutit à la relativisation de la règle qui la sous-tend.

111.- La distinction entre anciennes mesures adaptées au numérique et nouvelles mesures d'emblée numériques sans aucun lien avec une mesure préexistante non-virtuelle se dilue au sein de trois régimes juridiques dont les différences reflètent l'ampleur de l'impact du caractère numérique sur la physionomie de la mesure. Ainsi, les anciennes mesures dont la portée est seulement étendue par l'avènement de la technologie numérique continuent à relever du régime juridique ordinaire de droit commun (*§1*). En revanche, les mesures, anciennes ou nouvelles, dont les effets sont substantiellement renforcés par la technologie numérique, font l'objet d'un régime spécifique, notamment quant aux garanties prévues, distinct du régime de droit commun au sein duquel elles s'insèrent (*§2*). Différemment encore, les nouvelles mesures entièrement pensées et construites dans le monde numérique et informatique sont soumises à un régime dérogatoire par rapport au régime de droit commun (*§3*).

§1.- Le régime ordinaire des mesures NTIS

112.- Le régime ordinaire des mesures NTIS est le régime juridique de la procédure de droit commun applicable à toutes les infractions. La mesure NTIS fondée sur une mesure d'investigation existante s'insère dans cette procédure et obéit aux mêmes règles relatives à la portée, à l'encadrement, aux conditions ainsi qu'au contrôle de sa mise en œuvre que celles qui s'appliquent à la mesure « d'origine ». Aucune déviation, ni exception à des règles applicables dans chaque cadre procédural (enquête de flagrance, enquête préliminaire, instruction) n'est consacrée par le législateur au regard de la mesure NTIS. Cette assimilation entre anciennes mesures d'investigation et nouvelles mesures NTIS semble se justifier par la moindre intensité de l'atteinte à la vie privée caractérisant tant les anciennes que les nouvelles mesures.

113.- Tel paraît être le cas s'agissant des perquisitions, des saisies et des réquisitions judiciaires. Fondées sur des mesures d'investigation existantes[160], ces trois mesures NTIS sont considérées par le législateur comme portant une atteinte aux droits et libertés de gravité équivalente ou égale aux perquisitions, saisies et réquisitions classiques. Aucun besoin donc de prévoir un cadre juridique distinct, notamment par le renforcement du contrôle de leur mise en œuvre ou la restriction de leur portée. Dans les cas précis de ces trois mesures NTIS, les nouvelles technologies semblent ne pas avoir d'effet sur l'appréciation de la gravité de l'atteinte aux droits et libertés, et notamment sur le droit au respect à la vie privée. Si un tel constat est certes justifié par le fait que, d'une part, ces trois mesures impliquent une ingérence dans la vie privée en temps différé et que, d'autre part, certaines d'entre elles ne présentent pas de caractère secret tandis que d'autres n'ont pas de caractère coercitif, il n'en demeure pas moins que le législateur

[159] AUROY Benoît, « La preuve numérique en procédure pénale : un système à (re)construire », *Dalloz*, n° 14, 2023, p. 700.
[160] Voir *supra*, Section précédente sur la généalogie des mesures.

ne paraît pas avoir pris la mesure du potentiel amplificateur recelé par les nouvelles technologies, susceptibles d'accentuer l'atteinte à la vie privée sous l'effet de l'expansion de la portée matérielle de la mesure classique. Un tel risque concerne surtout les perquisitions et, par extension, les saisies informatiques.

114.- Le régime des perquisitions informatiques suit celui des perquisitions « classiques » régies par le cadre procédural prévu aux articles 56 et s. du CPP pour l'enquête de flagrance, à l'article 76 du CPP pour l'enquête préliminaire et aux articles 94 et s. du CPP pour l'instruction et 706-88 et s. du CPP en matière de criminalité organisée. Il en est également ainsi concernant les saisies informatiques qui peuvent porter soit sur le support physique des données informatiques nécessaires à la manifestation de la vérité soit sur une copie réalisée en présence des personnes qui assistent à la perquisition[161]. Mises en œuvre en connaissance de la personne concernée, les perquisitions informatiques sont requises au regard des mêmes infractions que les perquisitions « classiques » soit par le procureur de la République soit par le juge d'instruction, selon la procédure, et elles sont opérées par un OPJ, ou, sous la responsabilité de ce dernier, un APJ, en présence de la personne au domicile de laquelle la perquisition a lieu ou de son représentant, voire de deux témoins choisis par l'OPJ. Elles constituent une mesure non coercitive dans le cadre de l'enquête préliminaire, puisqu'elles ne peuvent en principe être effectuées sans l'assentiment exprès de la personne chez laquelle l'opération a lieu, assentiment qui doit faire l'objet d'une déclaration écrite de la main de l'intéressé. Néanmoins, si les nécessités de l'enquête l'exigent et pour les infractions punies d'au moins trois ans d'emprisonnement, le JLD peut autoriser qu'une perquisition soit réalisée sans l'assentiment de la personne. Les perquisitions ne peuvent avoir lieu qu'entre 6h00 et 21h00 sauf exception, en matière de criminalité organisée notamment.

115.- Cette assimilation des perquisitions informatiques aux perquisitions « classiques » pourrait s'avérer problématique dans la mesure où elle permet la réalisation de deux actes d'investigation numérique sans qu'ils soient encadrés par des garanties adéquates. En effet, l'article 57-1 du CPP autorise les enquêteurs à accéder, au cours d'une perquisition domiciliaire, à des données informatiques stockées dans un système présent sur place ou accessibles depuis ce système sans aucune condition supplémentaire autre que celles prévues pour les perquisitions « classiques ».
Autrement dit, en assimilant l'environnement numérique à l'environnement réel, la loi autorise l'extension de la perquisition dans le premier à partir du moment où elle peut être menée sans discontinuité. Ainsi sont susceptibles d'être consultées par les enquêteurs les données informatiques stockées non seulement dans tout support informatique, à savoir, ordinateur, clé USB, disque dur trouvé sur les lieux physiques de la perquisition mais également dans un *cloud* accessible depuis un ou plusieurs de ces supports informatiques. Tant que l'accès à l'espace numérique est libre, c'est-à-dire qu'il peut s'effectuer sans mot de passe, la poursuite de la perquisition au sein de celui-ci ne connaît pas de limites. De surcroît, l'article 57-1 du CPP autorise également aux mêmes conditions que celles requises pour les perquisitions physiques une perquisition informatique à distance consistant en l'accès à un système informatique par le biais d'un autre système qui se trouve dans les locaux des enquêteurs. La consultation des données stockées dans les supports informatiques se trouvant sur les lieux de la perquisition devient encore plus facile, la seule limite restant le verrouillage de l'accès par un mot de passe. Or, étant donné que la masse des données à laquelle il est possible d'accéder lors d'une perquisition informatique peut être plus volumineuse que celle qui est accessible en vertu de mesures NTIS considérées comme plus intrusives et donc soumises à des conditions plus

[161] Voir article 56 al. 5 CPP.

strictes, comme l'interception des correspondances émises par la voie des communications électroniques ou l'*IMSI-catcher*, le régime des perquisitions informatiques peut paraître insuffisant au regard de l'ingérence dans le droit à la vie privée qu'elles impliquent.
Le choix du législateur d'assimiler les deux mesures d'investigation, la « classique » et la « numérique » ou « informatique », en prévoyant pour la seconde les mêmes garanties que pour la première, peut être discuté et mérite examen, tout comme le *continuum* entre le monde physique et le monde numérique sur lequel ce choix repose : le profit tiré de ce que ce dernier n'a ni frontières ni limites physiques[162] se solde par un coût insuffisamment considéré pour les droits et libertés en cause.

116.- Contrairement à la réglementation des perquisitions informatiques, un tel coût a pour partie déterminé la définition des conditions du recours aux réquisitions judiciaires aux fins de mise à disposition de données informatiques. Ces réquisitions suivent le régime des réquisitions judiciaires ordinaires des articles 60-1 du CPP pour l'enquête de flagrance, 77-1-1 du CPP pour l'enquête préliminaire et 99-3 du CPP pour l'instruction uniquement lorsqu'elles portent sur des données issues d'un système informatique ou d'un traitement de données nominatives, comme les comptes bancaires[163]. Dans ces cas, les réquisitions sont autorisées au cours des investigations pour toute infraction par le procureur de la République dans le cadre de l'enquête et par le juge d'instruction dans le cadre de l'instruction. Même si elles sont secrètes, l'absence de caractère coercitif[164] tempère sûrement l'atteinte à la vie privée ainsi qu'aux droits de la défense des personnes concernées par les données en question. Toutefois, l'élément décisif justifiant leur assimilation aux réquisitions ordinaires est le type de données concernées. Dès lors qu'elles portent sur des données de connexion, ces réquisitions font l'objet d'un régime spécifique caractérisé par des garanties et des conditions plus strictes.

§2.- Le régime spécifique des mesures NTIS

117.- A propos de certaines mesures NTIS, le législateur a prévu un régime juridique différent du régime ordinaire afin de prendre en compte le caractère spécifique qui les distingue des autres mesures NTIS, y compris celles qui relèvent des procédures dérogatoires. Véritable catégorie intermédiaire entre le régime procédural de droit commun et celui d'exception, ce régime spécifique relève de la procédure de droit commun mais prévoit des garanties renforcées pour la mise en œuvre des mesures en question. Tel est le cas de la géolocalisation[165], des réquisitions de données informatiques stockées[166] ainsi que de la conservation rapide des données informatiques[167], étant souligné que la distinction entre ces deux derniers types de

---

[162] Or, de telles limites existent dans le monde physique et sont également établies par la délimitation de la perquisition au domicile de la personne concernée ainsi que par la définition de ce que l'on entend par domicile, terme qui malgré son extension par la jurisprudence, connaît des limites également physiques (par exemple, s'il peut inclure un espace annexe, il ne saurait inclure le domicile d'une autre personne).
[163] Article 60-1 CPP.
[164] Les articles 60-1 al. 2, 77-1-1 al. 2, 99-3 al. 2 CPP punissent le refus de répondre à ces réquisitions d'une amende de 3750 euros sans pour autant imposer l'exécution des réquisitions. Si les mêmes dispositions prévoient que seule l'existence d'un motif légitime peut justifier le refus de réponse, elles ne donnent pourtant aucune précision supplémentaire sur la nature de ce motif légitime dont l'appréciation est laissée au juge.
[165] Article 230-32 CPP.
[166] Articles 60-1 al. 1er, 60-2 al. 1er, 77-1-1, 77-1-2 al. 1er et 99-3 al. 1er CPP.
[167] Articles 60-1-2, 60-2 al. 2, 77-1-2 al. 2, 99-4 al. 2 CPP.

mesures n'est pas clairement arrêtée[168]. Ces mesures sont considérées comme portant une atteinte grave aux droits et libertés, et notamment au droit à la vie privée, de sorte que leur insertion dans les cadres procéduraux existants est accompagnée de conditions supplémentaires comme l'exigence d'un seuil de gravité pour les infractions concernées, d'une limitation dans le temps, d'un contrôle par un magistrat du siège, et dont la méconnaissance peut entraîner la nullité de l'acte d'investigation en question.

118.- L'hétérogénéité des mesures NTIS dont il est ici question interroge quant à l'usage de la gravité de l'atteinte aux droits et libertés comme critère d'établissement du régime juridique qui les gouverne. En effet, ce régime s'applique à la fois à des mesures NTIS fondées sur une mesure « classique », comme c'est le cas des réquisitions des données informatiques, à des mesures nouvelles sans aucun ancrage dans une mesure d'investigation préexistante, comme la géolocalisation ou la conservation rapide des données informatiques (entendue ici dans son sens « originel » de mode de préservation), ainsi qu'à des mesures NTIS consistant en une ingérence dans la vie privée non seulement en différé, comme la conservation rapide ou les réquisitions, mais aussi en temps réel, comme la géolocalisation. La *ratio legis* d'un encadrement renforcé de leur mise en œuvre doit alors être recherchée en examinant non seulement leur nature mais également leur objet : appliquées de manière clandestine à l'insu de la personne concernée, ces mesures NTIS permettent aux enquêteurs d'accéder aux données de connexion[169]. L'accès à ces données, surtout lorsqu'il se fait en masse comme c'est le cas en matière de conservation rapide ou en général de réquisitions des données de connexion[170], est susceptible de porter une grave atteinte au droit à la vie privée. Tel est également le cas en matière de géolocalisation qui, même si elle est dépourvue de cet effet de massification des données, engendre une ingérence significative dans la vie privée des individus dans la mesure où elle permet une observation relativement approfondie de leur conduite, qui peut en plus être réalisée en temps réel[171]. Contrairement aux mesures NTIS relevant du régime ordinaire, dans toutes ces hypothèses les nouvelles technologies aggravent l'atteinte aux droits et libertés, ce qui oblige le législateur, sous le poids de contraintes européennes ou constitutionnelles, à restreindre la portée de la géolocalisation, des réquisitions de données informatiques stockées ainsi que de la conservation rapide (au sens de préservation) des données informatiques et à renforcer le contrôle judiciaire de leur application. Toutefois, ce choix lui-même est susceptible de poser question dans la mesure où il traduit plutôt la mise en conformité du droit positif aux contraintes européennes et constitutionnelles qu'une approche systémique et une vue d'ensemble des mesures NTIS portant sur les données personnelles[172], et notamment sur les données de connexion.

119.- En effet, l'approche graduelle du législateur français renvoie inévitablement à la jurisprudence des deux cours européennes qui ont développé des vues comparables s'agissant

---

[168] Les réquisitions de données informatiques stockées pouvant tenir lieu d'injonction de conservation rapide, au sens de la convention de Budapest, selon la jurisprudence de la chambre criminelle (cf. Crim. 12 juillet 2022, n° 21-83.710).

[169] Toutefois, l'accès aux données de localisation n'est plus permis lorsque la géolocalisation se fait par le biais des réquisitions de ces données auprès des opérateurs de téléphonie. Voir, Crim., 27 février 2024, n° 23-81.061.

[170] Depuis les arrêts du 12 juillet 2022 de la Chambre criminelle Cour de cassation sur les données de connexion, la distinction entre réquisitions de conservation et réquisitions d'accès aux données informatiques, pourtant présente dans le code de procédure pénale, semble s'estomper, puisque la réquisition d'accès aux données vaut aussi réquisition de conservation. Voir Crim., 12 juillet 2022, n° 21-83.710, §. 32 et s. Voir également la note explicative (p. 6) accompagnant cette jurisprudence qui renvoie au rapport explicatif de la Convention de Budapest pour considérer que l'injonction de conservation rapide peut résulter d'une injonction de produire.

[171] Voir en ce sens, CEDH, 2 septembre 2010, *Uzun c. Allemagne*, n° 35623/05, §. 80.

[172] Dans le même sens, MORNET Alice, « Vers un droit commun de la preuve numérique ? », *Lexbase*, 8 mars 2023.

de la géolocalisation ou des réquisitions de données de connexion, et surtout de leur conservation rapide[173].

120.- Cette approche est manifeste dans le cas de la géolocalisation puisque le Code de procédure pénale prévoit désormais deux – en réalité trois compte tenu de la jurisprudence récente tirant les conséquences des contraintes issues du droit de l'Union[174] – procédés de géolocalisation, mis en œuvre selon des conditions différentes.

121.- Premièrement, les articles 230-32 et suivants du CPP établissent les conditions du recours à la géolocalisation en temps réel effectuée par tout moyen technique. Cette mesure est autorisée dans le cadre de l'enquête par le procureur pour huit jours consécutifs (quinze en matière de criminalité organisée et de procédures de recherches de personnes disparues ou en fuite), puis éventuellement renouvelée par le JLD pour une durée d'un mois renouvelable, et dans le cadre de l'instruction par le juge d'instruction[175]. En cas de risque imminent de dépérissement des preuves ou d'atteinte grave aux personnes ou aux biens, elle peut exceptionnellement être mise en place par un OPJ pour 24 heures, qui en informe immédiatement le procureur de la République lequel décide de la poursuite ou non de l'opération[176]. Le procureur de la République ou le juge d'instruction peuvent autoriser l'introduction dans certains lieux privés destinés ou utilisés à l'entrepôt de véhicules, fonds, valeurs, marchandises ou matériel ou dans un véhicule aux fins de mise en place du dispositif de géolocalisation, y compris en dehors des heures de perquisitions légales[177]. S'agissant d'autres lieux privés, l'opération n'est possible que pour rechercher les causes de la mort ou de la disparition d'une personne ou encore un individu en fuite et lorsque l'enquête ou l'instruction est relative à un crime ou à un délit puni d'au moins cinq ans d'emprisonnement, tandis que s'agissant d'un lieu d'habitation, l'autorisation est délivrée par le JLD dans le cadre de l'enquête ou le juge d'instruction dans le cadre de l'instruction[178]. La mesure ne peut être appliquée que dans le cadre d'investigations concernant des infractions punies d'au moins trois ans d'emprisonnement, la recherche des causes de la mort ou de la disparition, ainsi que la recherche d'une personne en fuite[179]. La durée totale de l'opération de géolocalisation ne peut pas excéder un an (deux ans en matière de criminalité organisée ou grave[180]).

---

[173] Voir CJUE, 8 avril 2014, *Digital Rights Ireland*, C-293/12 et C-594/12 ; CJUE, 21 décembre 2016, *Tele2-Sverige*, C-203/15 ; CJUE, 2 octobre 2018, *Ministerio Fiscal*, C-207/16 ; CJUE, 6 octobre 2020, *La Quadrature du Net*, C-511/18 ; CJUE, 2 mars 2021, *Prokuratuur*, C-746/18 ; CJUE, 5 avril 2022, *Garda Siochàna*, C-140/20 ; CJUE, 20 septembre 2022, *Spacenet*, C-793/19 ; CJUE, 7 septembre 2023, A.G., C-162/22 ; CEDH, 15 février 2024, *Škoberne c. Slovénie*, n° 19920/20.

[174] *Infra*, à propos de l'arrêt de la chambre criminelle 27 février 2024, n° 23-81.061. Sur l'éclatement des régimes de la géolocalisation selon que le droit de l'Union est applicable (cas de la géolocalisation en temps réel d'un téléphone) ou non (cas de la géolocalisation de véhicule par pose de balise), voir notamment CHAUVELOT Aurore, « La mesure de suivi en temps réel d'un véhicule automobile par pose d'une balise de géolocalisation ne mobilise pas les opérateurs de service de communication électronique au sens du droit de l'Union », *RSC*, 2024, p. 412 et s. qui souligne combien « l'égale protection des droits fondamentaux s'accommode mal de la coexistence de régimes différenciés selon les modalités techniques de mise en œuvre de la géolocalisation. Qu'elle fonctionne grâce à une balise fixée à cette fin ou procède de réquisitions à l'équipementier ou à l'opérateur lorsque le véhicule dispose d'un système de navigation intégrant l'accès à un service de communications électroniques ouvert au public, il en résulte le même suivi du déplacement d'une personne via le véhicule qu'elle utilise ».

[175] Article 230-33 CPP.

[176] Article 230-35 CPP.

[177] Article 230-34 CPP.

[178] Article 230-34 CPP.

[179] Article 230-32 et 706-1-3 CPP.

[180] Il s'agit des infractions prévues aux articles 706-73 ou 706-73-1 du CPP.

122.- Si le Code de procédure pénale ne distingue pas la géolocalisation en temps réel selon le moyen technique utilisé, tel n'est pas le cas de la jurisprudence. En effet, pour mettre en œuvre la géolocalisation de l'article 230-32 CPP, deux moyens peuvent être utilisés : la pose de balises et le suivi en temps réel d'un dispositif de téléphonie mobile[181]. Si le premier s'effectue par les enquêteurs eux-mêmes, le second requiert les services d'un fournisseur de téléphonie à qui les enquêteurs demandent un suivi en temps réel, lequel comprend l'accès aux données de localisation. Or, une géolocalisation qui s'effectue par le biais de réquisitions des données de localisation à un opérateur de téléphonie entre bien dans le champ d'application du droit de l'Union, ce que la chambre criminelle n'a pas manqué de rappeler dans un arrêt du 27 février 2024, dans lequel elle a appliqué à la géolocalisation par suivi en temps réel d'un dispositif de téléphonie mobile sa jurisprudence précédente relative aux conditions d'accès aux données de connexion[182]. Elle a alors constaté l'incompatibilité avec le droit de l'Union tirée du pouvoir reconnu au procureur de la République d'autoriser les réquisitions de données de localisation, ce pouvoir ne pouvant être le fait que d'une juridiction ou d'une autorité administrative indépendante[183].

123.- Deuxièmement, les articles 230-34-1 et 230-36 du CPP restreignent les conditions de mise en œuvre de la géolocalisation lorsque cette technique s'effectue par l'activation à distance d'un appareil électronique, à l'insu ou sans le consentement de son propriétaire ou de son possesseur afin de procéder à sa localisation en temps réel. Considérée comme plus intrusive que la géolocalisation par balise posée[184] et plus attentatoire que la géolocalisation par bornage du téléphone mobile[185], cette mesure non seulement a une portée plus restreinte que celle de l'article 230-33 du CPP dans la mesure où elle ne peut s'appliquer que lorsque les nécessités de l'enquête ou de l'instruction relative à un crime ou à un délit puni d'au moins cinq ans d'emprisonnement l'exigent, mais, en outre, n'est autorisée que par un magistrat du siège, à savoir le JLD ou le juge d'instruction.

124.- Dans le même sens, l'article 60-1-2 du CPP renforce les garanties relatives aux réquisitions adressées aux opérateurs de communications électroniques lorsqu'elles portent sur des données de connexion, à savoir des données techniques relatives à l'identification ou au recensement des numéros d'abonnement ou de connexion à des services de communications électroniques d'une personne désignée, à la localisation d'équipements terminaux, à la liste des numéros appelés ou appelants, à la durée et à la date des communications. Même si elle ne concerne pas le contenu des communications ou des navigations numériques, l'exploitation de ce type de données fournit néanmoins des informations sur la vie des personnes concernées susceptibles d'être exploitées par les enquêteurs. Ce risque accru pour le droit au respect à la

---

[181] Rapport n° 284 (2013-2014) de M. Jean-Pierre SUEUR, fait au nom de la commission des lois, déposé le 15 janvier 2014, p. 21.
[182] Crim. 27 février 2024, n° 23-81.061.
[183] CJUE, 2 mars 2021, *Prokuratuur*, aff. C-746/18, pt. 51 et s.
[184] Voir en ce sens, CANAYER Agnès, VERIEN Dominique, *Rapport du Sénat sur le projet de loi d'orientation et de programmation du ministère de la justice 2023-2027 (procédure accélérée) et sur le projet de loi organique relatif à l'ouverture, la modernisation et la responsabilité du corps judiciaire (procédure accélérée), n° 660, 31 mai 2023*, p. 107.
[185] A propos de l'absence d'information sur le procédé technique utilisé en l'espèce, et les enjeux subséquents quant à la possibilité d'apprécier l'intensité de l'atteinte aux droits fondamentaux, DELAGE, Pierre-Jérôme, « À propos de quelques évolutions de la procédure pénale issues de la loi "Justice" du 20 novembre 2023 », *op.cit*. Voir aussi CHAUVELOT Aurore, « La mesure de suivi en temps réel d'un véhicule automobile par pose d'une balise de géolocalisation ne mobilise pas les opérateurs de service de communication électronique au sens du droit de l'Union », *op.cit.* qui souligne combien l'arrêt illustre « la difficulté de mesurer au plus juste l'atteinte que tel outil d'enquête porte à la vie privée ».

vie privée a contraint le législateur français[186] à restreindre la portée de ces réquisitions aux procédures portant sur des crimes ou des délits punis d'au moins trois ans d'emprisonnement ou sur des délits punis d'un an d'emprisonnement lorsqu'ils sont commis par l'utilisation d'un réseau de communications électroniques. Les réquisitions de données de connexion sont également autorisées lorsqu'elles concernent le terminal de la victime d'un délit puni d'emprisonnement et interviennent à sa demande ainsi que lorsqu'elles tendent à retrouver une personne disparue ou à retracer le parcours d'une personne condamnée pour crimes sériels ou soupçonnée de tels faits. Intervenue après la décision du Conseil constitutionnel qui avait considéré que le fait que des données de connexion pouvaient être requises pour toute infraction, sans limite de temps ni justification fondée sur l'urgence, portait une atteinte disproportionnée au droit au respect à la vie privée[187], cette réforme s'inscrit dans la continuité de la jurisprudence européenne, tout spécialement celle de la CJUE, qui a posé de nouvelles règles dans le domaine de la conservation et de l'accès aux données de connexion dans le cadre des procédures pénales[188]. Néanmoins, les exigences du contrôle judiciaire de ces réquisitions spécifiques sont les mêmes que celles relatives aux réquisitions de données issues d'un système informatique ou d'un traitement de données nominatives. En effet, les réquisitions de données de connexion s'effectuent sous le contrôle du procureur dans le cadre de l'enquête préliminaire et du juge d'instruction dans le cadre de l'instruction, mais elles peuvent aussi être formulées uniquement par l'OPJ ou l'APJ, sous le contrôle du premier, dans le cadre de l'enquête de flagrance. L'absence de contrôle judiciaire dans ce dernier cadre d'enquête s'explique par les caractéristiques de l'enquête de flagrance, en particulier l'urgence et la limitation dans le temps, qui ne rendent pas disproportionnée l'atteinte au droit à la vie privée du fait des réquisitions portant sur les données de connexion[189]. Pourtant, c'est bien la question du contrôle judiciaire qui a obligé le législateur français à modifier le régime juridique de la conservation rapide des données de connexion, qui consiste à demander à un opérateur de conserver en urgence à partir d'un instant « t » des données qu'il stocke.

125.- Depuis 2014, par une suite d'arrêts retentissants[190], la CJUE a restreint les possibilités de conservation et d'accès aux données de connexion au nom d'une interprétation des exceptions au principe de la confidentialité des communications[191] conforme, selon elle, aux droits au

---

[186] *Loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire*.

[187] Cons. Const., décision du 3 décembre 2021, n° 2021-952 QPC.

[188] *Infra*.

[189] La CJUE réserve également le cas de l'urgence « dûment justifié » mais à la condition que le contrôle qui n'a pu être, comme elle l'exige, préalable ait lieu dans de « brefs délais », cf. notamment CJUE (grande chambre), 6 octobre 2020, *La Quadrature du Net*, aff. jtes C-511/18, C-512/18 et C-520/18, point 189.

[190] CJUE (grande chambre), 8 avril 2014, *Digital Rights Ireland*, aff. jtes C-293/12 et C-594/12 ; CJUE (grande chambre), 21 décembre 2016, *Tele2 Sverige*, aff. C-203/15 ; CJUE (grande chambre), 2 octobre 2018, *Ministerio Fiscal*, aff. C-207/16 ; CJUE (grande chambre), 6 octobre 2020, *La Quadrature du Net*, précité ; CJUE (grande chambre), 2 mars 2021, *Prokuratuur*, aff. C-746/18 ; CJUE (grande chambre), 5 avril 2022, *Garda Siochàna*, aff. C-140/20 ; CJUE (grande chambre), 20 septembre 2022, *Spacenet*, aff. C-793/19; CJUE, 17 novembre 2022, *Spetisalizirana prokuratura*, aff. C-350/21; CJUE, 7 septembre 2023, *A.G.*, aff. C-162/22.

[191] Telles que prévues par l'article 15§1 de la *Directive 2002/58/CE, dite Vie privée et communications électroniques*, selon lequel : « Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises

respect de la vie privée, à la protection des données à caractère personnel et à la liberté d'expression. Cette jurisprudence, qui a bouleversé le travail des enquêteurs en réservant le recours à la conservation généralisée et indifférenciée des données de connexion aux seules fins de sauvegarde de la sécurité nationale des États membres, a également posé des conditions strictes au recours à la mesure de conservation rapide des données informatiques stockées. Qu'elle résulte de la transposition de la Convention de Budapest en tant que mesure de « préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs »[192] ou qu'elle soit inférée du pouvoir de réquisition de données informatiques stockées[193], ce que le CPP prévoit pour l'ensemble des cadres d'enquête, la conservation rapide des données de connexion ne devrait être autorisée, selon la CJUE, qu'aux fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale et à la condition d'être décidée pour une durée déterminée par une autorité compétente dont la décision est soumise à un contrôle juridictionnel ou à tout le moins indépendant et effectif[194]. Or le respect des conditions relatives à la conservation constitue à son tour la condition *sine qua non* de l'accès aux données conservées. Selon la CJUE, la légalité et la motivation de l'accès doivent faire l'objet d'un contrôle préalable par une juridiction ou par une entité administrative indépendante et ne peuvent être justifiées que par les mêmes finalités que celles qui ont justifié la conservation, à savoir la lutte contre la criminalité grave et la sauvegarde de la sécurité nationale[195].

126.- Afin de mettre le droit français en conformité avec ces exigences relatives tant à la portée de la mesure qu'à son contrôle juridictionnel, la loi du 2 mars 2022 a restreint le domaine de la conservation rapide (*lato sensu*) lorsqu'elle porte sur les données de connexion. Dans un tel cas, la mesure n'est plus applicable à toute infraction mais seulement aux crimes ou délits punis d'au moins trois ans d'emprisonnement ainsi qu'aux délits punis d'au moins un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques[196]. La mise en conformité législative est cependant partielle dans la mesure où elle n'a pas été l'occasion de revoir la question du contrôle de l'autorisation de l'accès aux données ainsi conservées. Pourtant, la CJUE avait insisté sur le fait que l'accès des autorités nationales compétentes aux données conservées devrait être subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, susceptible d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité grave, et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel[197]. Constatant la contrariété de l'œuvre législative inachevée, la chambre criminelle s'est chargée de poursuivre, à sa manière [198] et depuis sa position, l'entreprise de mise en conformité des dispositions procédurales françaises. Elle a considéré que les articles 60-1, 60-2, 77-1-1 et 77-1-2 du CPP sont contraires au droit de l'Union en ce qu'ils ne prévoient pas un tel contrôle[199].

---

dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne ».

[192] Alinéas 2 des articles 60-2, 77-1-2 et 99-4 CPP.

[193] Art. 60-1, 60-2, 77-1-1 et 77-1-2 CPP.

[194] CJUE 6 oct. 2020, *La Quadrature du Net*, précité, points 163-167.

[195] *Ibid.*, pt. 146-151.

[196] Article 60-1-2 CPP.

[197] Voir notamment, CJUE, 20 septembre 2022, *Spacenet AG*, aff. C-793/19 et 794/19, pt. 72 ; CJUE, 5 avril 2022, *Commissioner of Garda Siochana*, aff. C-140/20, pt. 58 ; CJUE, 2 mars 2021, *Prokuratuur*, aff. C-746/18, pt. 51.

[198] *Infra*, Troisième partie.

[199] Crim. 12 juillet 2022, n° 21-83.710, §. 42.

Quoi qu'il en soit, s'insérant dans la catégorie des réquisitions des données informatiques, la conservation rapide ne présente pas un caractère coercitif dans la mesure où les personnes visées par ces réquisitions ne peuvent être obligées de fournir la prestation demandée. Certes la sanction du refus de se conformer aux réquisitions[200] peut avoir un effet persuasif mais en aucun cas la loi ne prévoit un moyen quelconque de coercition directe.

Malgré la restriction des conditions et l'imposition d'un certain seuil de gravité de l'infraction, les mesures soumises à un régime spécifique restent applicables à un très grand nombre d'infractions pénales susceptibles de faire l'objet d'une enquête ou d'une instruction. Or tel n'est pas le cas des mesures qui relèvent d'un régime dérogatoire.

§3.- Le régime dérogatoire des mesures NTIS

127.- Le régime dérogatoire auquel sont soumises certaines mesures NTIS correspond au régime dérogatoire des procédures pénales prévues au Livre IV du Code de procédure pénale. S'appliquant uniquement dans ce cadre procédural, le recours aux mesures NTIS en question est encadré dans le temps, se fait sous le contrôle d'un magistrat du siège et n'est prévu que pour les infractions les plus graves. Le caractère exceptionnel du recours à ces mesures NTIS est justifié par la gravité de l'atteinte à la vie privée que leur utilisation est susceptible de provoquer dans la mesure où la plupart d'entre elles se déploient de manière clandestine et réalisent une intrusion en temps réel dans la vie privée des personnes concernées. C'est surtout le cumul de ces conditions qui les différencie des autres mesures NTIS relevant du régime ordinaire ou spécifique. Tel est le cas des mesures NTIS regroupées au sein de l'ensemble des « autres techniques spéciales d'enquête » de la section 6 du Titre XXV relatif à la procédure applicable à la criminalité et à la délinquance organisées, comme le recueil des données techniques de connexion[201] (qui permettent d'identifier la source de la connexion ou celles qui sont relatives aux équipements terminaux utilisés), les interceptions de correspondances émises par la voie des communications électroniques[202], les sonorisations et fixations d'images de certains lieux ou véhicules[203], la captation des données informatiques[204], ainsi que de l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique[205], même si cette mesure ne figure pas dans la section 6[206]. A l'exception de cette mesure qui s'applique à tout crime[207], toutes les autres mesures NTIS ne s'appliquent qu'à la criminalité et délinquance organisées, aux actes de terrorisme, aux crimes et à certains délits[208] portant atteinte aux intérêts fondamentaux de la Nation prévus au titre Ier du livre IV du Code pénal et à certains délits graves comme

[200] Les articles 60-1 al. 2, 60-2 al. 4, 77-1-1 al. 2, 77-1-2 al. 4, 99-3 al. 2 et 99-4 al. 4 CPP punissent le refus de répondre à ces réquisitions d'une amende de 3750 euros. Si les mêmes dispositions prévoient que seule l'existence d'un motif légitime peut justifier le refus de réponse, elles ne donnent pourtant aucune précision supplémentaire sur la nature de ce motif légitime dont l'appréciation est laissée au juge.
[201] Article 706-95-20 CPP.
[202] Article 706-95 CPP.
[203] Article 706-96 CPP.
[204] Article 706-102-1 CPP.
[205] Article 706-95-1 CPP.
[206] Il s'agit d'une mesure faisant partie des techniques spéciales d'enquête, mais pas des « autres techniques spéciales d'enquête », titre de la Section 6. Voir PARIZOT Raphaële, « Les (autres) techniques spéciales d'enquête, une non-catégorie juridique », *in* PELLÉ Sébastien (dir.), *Quelles mutations pour la justice pénale du XXIe siècle*, Paris, Dalloz, 2020, p. 78 et s.
[207] Article 706-95-1 CPP.
[208] Art. 411-5, 411-7 et 411-8 ; art. 412-2, al. 1 et 2 ; art. 413-1 et art. 413-13, al. 3 du Code pénal.

l'importation, l'exportation, le transit, le transport, la détention, la vente, l'acquisition ou l'échange d'un bien culturel[209], ainsi que le blanchiment et le recel portant sur la plupart de ces infractions [210]. Visant, pour la plupart, des infractions punies d'une peine d'emprisonnement de sept ans au moins, cette liste est fondée sur le critère de gravité de l'infraction supposée autoriser le recours aux mesures NTIS réalisant une entorse sérieuse au droit à la vie privée. Toutefois, ce constat est tempéré par la présence, au sein de cette même liste, d'infractions punies de sanctions dont le quantum est situé en dessous du seuil de sept ans d'emprisonnement, à savoir cinq ans, trois ans ou même six mois d'emprisonnement[211], ce qui implique le risque non seulement de brouillage entre procédure dérogatoire et procédure de droit commun, mais également de relativisation de la notion d'infraction grave comme critère pour l'application de ces mesures NTIS. Or, cette notion est au cœur de la jurisprudence des deux cours européennes à propos des données de connexion et de la mise en œuvre des mesures de surveillance non seulement dans le domaine pénal mais aussi dans celui du renseignement[212].

128.- Si le critère de la gravité de l'infraction ne suffit pas à lui seul pour distinguer les différents régimes juridiques applicables, il n'en est pas ainsi en ce qui concerne le contrôle judiciaire et la durée des mesures NTIS. En renforçant ces deux conditions, le législateur français marque une différence entre le régime juridique dérogatoire et les régimes juridiques de droit commun des mesures NTIS. Tout d'abord, la mise en œuvre des mesures NTIS susvisées est soumise au contrôle d'un magistrat du siège, à savoir le JLD ou le juge d'instruction selon le cadre dans lequel la mesure NTIS est déployée, et non pas à des magistrats du parquet, ce qui renforce les exigences d'indépendance et d'impartialité et est supposé assurer la conformité du droit français avec le droit de l'UE en la matière[213]. Compte tenu du caractère clandestin de la plupart des mesures en question, qui sont mises en œuvre à l'insu de la personne concernée[214], le contrôle *a priori* acquiert une importance fondamentale car c'est la seule manière de s'assurer de la légalité et de la proportionnalité de l'application de ces mesures [215]. Il est alors indispensable de confier ce contrôle à un magistrat du siège. Toutefois, les entretiens menés ont montré que le contrôle réalisé aux fins d'autorisation des mesures NTIS, notamment par le JLD, est largement formel[216], pratique qui va à l'encontre d'une jurisprudence qui insiste de plus en plus sur le caractère substantiel d'un tel contrôle[217].

---

[209] Article 322-3-2 du code pénal.
[210] Voir articles 706-73, 706-73-1 et 706-74 CPP.
[211] Voir respectivement à titre d'exemple, les articles 222-52, 222-59, 412-8, 413-2, 413-11, 413-13, 413-14, 413-5, 413-6, 322-6-1, ainsi que 413-7 du Code pénal.
[212] Voir à titre d'exemple, CJUE, 2 mars 2021, *Prokuratuur*, aff. C-746/18, points 27-45 ; CEDH, 25 mai 2021, *Centrum för Rättvisa c. Suède*, n° 35252/08, § 284 et s. ; CEDH, 15 février 2024, *Škoberne c. Slovénie*, n° 19920/20, § 125 et s.
[213] Voir en ce sens, CJUE, 2 mars 2021, *Prokuratuur*, aff. C-746/18, points 46-59.
[214] En effet, à l'exception des perquisitions et des saisies qui sont notifiées aux personnes visées et nécessitent leur assentiment, les autres mesures NTIS revêtent un caractère secret et leur mise en œuvre se fait à l'insu des intéressés.
[215] En l'absence de toute notification l'intéressé ne peut exercer un recours contre l'ordonnance autorisant la mise en œuvre de la mesure.
[216] Voir *supra*, partie 1.
[217] Par l'arrêt du 23 novembre 2016, n° 15-83.649, la chambre criminelle insistait sur le caractère substantiel de la motivation de l'autorisation d'une perquisition délivrée par un JLD, exigeant que cette motivation s'effectue par référence non pas à la requête présentée par le procureur de la République, mais aux éléments de fait et de droit justifiant la nécessité de l'acte d'enquête en question. Dans le même sens, la chambre criminelle exige dans l'arrêt du 1er octobre 2024 (n° 24-80.363) que l'autorisation de géolocalisation émise par le Procureur de la République soit motivée par référence aux éléments de fait et de droit justifiant la nécessité la mesure. Voir SCHERER Théo, « Viser n'est pas motiver, tant pour le procureur que pour le JLD », *Dalloz actualité*, 9 octobre 2024.

129.- Ensuite, en guise de garantie supplémentaire, l'utilisation des mesures NTIS qui consistent en une ingérence en temps réel dans la vie privée des personnes concernées est limitée dans le temps. Tel est le cas de l'interception des correspondances émises par la voie des communications électroniques qui est autorisée pour une durée d'un mois, renouvelable une fois[218], dans le cadre des enquêtes préliminaire et de flagrance et pour une durée de quatre mois, renouvelable sans pouvoir excéder un an ou, s'il s'agit d'une infraction visée aux art. 706-73 et 706-73-1 du CPP, deux ans. En cas d'information pour recherche des causes de la mort ou d'une disparition, la durée est de deux mois, renouvelable[219]. Le recueil des données techniques de connexion au moyen d'une antenne-relais mobile factice (*IMSI-catcher*) est autorisé dans le cadre de l'enquête pour un mois renouvelable une fois s'agissant de l'accès aux données de connexion[220] et pour 48 heures, délai renouvelable une fois en ce qui concerne l'interception des télécommunications[221]. Dans le cadre de l'instruction, cette durée s'élève à une période de quatre mois, renouvelable cinq fois pour l'accès aux données de connexion[222], mais elle reste toujours limitée à 48 heures renouvelables une fois pour l'interception des télécommunications[223]. Les mêmes délais, à savoir un mois renouvelable une fois dans le cadre de l'enquête et quatre mois renouvelables cinq fois dans le cadre de l'instruction, sont également prévus pour la sonorisation et la fixation d'images de certains lieux ou véhicules[224], tandis que la captation des données informatiques peut être autorisée pour une durée d'un mois renouvelable une fois dans le cadre de l'enquête[225] et de quatre mois renouvelables dans la limite de deux ans dans le cadre de l'instruction[226].

Dans tous les cas, l'exécution de ces mesures NTIS s'effectue après ordonnance écrite et motivée soit du JLD soit du juge d'instruction, laquelle est cependant insusceptible de recours. Toutefois, comme tout acte de procédure, cette ordonnance peut faire l'objet d'une requête en annulation.

* *
*

Conclusion

130.- Malgré une certaine rationalité due au fait que les mesures NTIS s'insèrent dans des cadres procéduraux préexistants, les différents critères pris en compte pour distinguer les différents régimes ne permettent pas d'envisager une systématique rigoureuse des mesures NTIS. Certes, la construction du régime juridique de chaque mesure NTIS semble être fondée sur la gravité de l'atteinte que son utilisation est susceptible d'avoir sur les droits et libertés. Une certaine hiérarchisation émerge alors selon cette approche graduelle que l'on retrouve en

[218] Article 706-95 CPP.
[219] Article 80-4, al. 1er CPP.
[220] Article 706-95-16, al. 1er CPP.
[221] Article 706- 95-20, al. 2 CPP.
[222] Article 706-95-16, al. 2 CPP.
[223] Article 706-95- 20, al. 2 CPP.
[224] Article 706-95-16, al. 1 et 2 CPP.
[225] Article 706-95-16, al. 1er CPP.
[226] Article 706-95-16, al. 2 CPP.

pratique puisque les mesures NTIS les plus utilisées sont celles qui sont les plus « faciles » à mettre en œuvre, du point de vue des conditions juridiques et de la technicité requises. Toutefois, l'impact sur les droits et libertés, et notamment sur le droit au respect à la vie privée, n'a pas toujours été mesuré correctement à propos de chaque mesure NTIS, et notamment s'agissant de celles qui correspondent aux mesures « classiques » ou qui n'impliquent pas une surveillance en temps réel des personnes concernées. Considérées comme moins attentatoires, elles peuvent néanmoins porter une atteinte grave à la vie privée. Le cas de la perquisition informatique est emblématique à cet égard. Alors qu'elle permet l'accès aux données non seulement de connexion mais aussi de contenu, ses conditions d'application sont moins strictes que celles des réquisitions visant uniquement les données de connexion. Or, l'appréciation de l'intensité de l'intrusion dans la vie privée effectuée à l'aune plutôt des moyens utilisés (accès en temps réel ou différé) et moins des résultats obtenus (catégorie des données auxquelles l'accès a été donné) ne parvient pas à saisir de manière globale les risques de la « numérisation » des actes d'investigation pour les droits et libertés des personnes concernées. L'absence d'une définition claire de la notion d'« infraction grave » émousse encore davantage les distinctions entre les différents régimes des mesures NTIS, les privant ainsi de la cohérence et de l'articulation internes souhaitables.

131.- Le régime des mesures NTIS recèle des enjeux non seulement technologiques ou techniques mais aussi juridiques mettant à l'épreuve les principes de la procédure pénale. Les évolutions technologiques créent de nouvelles techniques d'investigation et de surveillance qui permettent de contourner les limites matérielles de la procédure pénale et d'étendre la portée de l'action des enquêteurs. Or, si elle facilite le travail des enquêteurs, l'extension du champ de la recherche de la preuve pénale au-delà des frontières nationales ou physiques les confronte à de nouveaux obstacles propres à l'environnement numérique, surtout si l'on envisage ce dernier dans la perspective plus vaste des changements profonds qui affectent l'enquête pénale.

Troisième partie : Perspectives

132.- Tant les pratiques des acteurs que leur encadrement juridique montrent combien les technologies d'investigation et de surveillance se présentent à la fois comme des moteurs et des révélateurs des transformations de l'enquête pénale : tandis qu'elles conduisent à l'adaptation des pratiques des enquêteurs, elles mettent tout autant en lumière une perturbation des principes de l'enquête.
Or, les unes et les autres gagnent à être replacés dans un contexte plus large de déstabilisation d'un certain nombre de repères essentiels à la construction et à l'application des règles de procédure pénale (*section 1*). Seul cet effort de contextualisation permet, en effet, d'apercevoir les frémissements ou fragments d'une reconfiguration de l'enquête pénale (*section 2*).

Section 1 : Déstabilisation des repères de la procédure pénale

133.- Au cœur des mesures d'enquête étudiées, figurent les technologies numériques, dénominateur commun à toutes. Or, la déstabilisation observée des repères de la procédure pénale peut être ramenée à un processus : la « dataisation » ou, pour reprendre les mots du Conseil d'État utilisés voici dix ans déjà[227], « la mise en données » du monde (*§1*). Cette lame de fond se produit à la faveur d'un autre processus qu'elle alimente en retour : la transnationalisation ou, empruntant là encore la formule au Conseil d'État, la « mise en réseaux du monde »[228] (*§2*). Se nourrissant l'un l'autre, ces deux processus convergent, concourant à la mise sous surveillance du monde, à la faveur d'un processus de « sécurisation »[229] (*§3*).

§1.- La « dataisation » ou la mise en données du monde

134.- « Dataisation », tentative d'une version française du terme anglo-saxon de « *datafication* », ou mise en données, pour rappeler le caractère construit de la donnée[230] : les termes ne sont pas encore fixés et cela signale déjà combien le processus reste largement à penser, ce qui suppose de le décrire (*I*) et de le nommer (*II*).

---

[227] Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, La documentation française, p. 9.
[228] *Ibid*.
[229] Le terme est ici choisi faute de mieux et vise à souligner la montée en puissance du concept et des enjeux de sécurité. Il est préféré à celui de « sécuritisation » qui, bien que lié et également utile à la compréhension du processus dit ici de sécurisation, relève d'autres questionnements, engage des controverses propres et repose sur des instruments singuliers ; pour une entrée en matière, cf. Esprit de justice, « Qu'est-ce que la sécuritisation ? », 3 mars 2021 (https://www.radiofrance.fr/franceculture/podcasts/esprit-de-justice/qu-est-ce-que-la-securitisation-6478211) où le concept est présenté comme « l'ensemble des processus à travers lesquels un enjeu social, public, est élevé au rang d'enjeu de sécurité », comme « la transformation fonctionnelle d'un problème en enjeu de sécurité », alors que ce problème « aurait pu être traité dans d'autres termes mais [en choisissant] de le présenter comme un enjeu de sécurité, [cela] entraîn[e] une grammaire et des pratiques tout à fait singulières.
[230] CATTARUZZA Amaël, « XXI. Prolégomènes à une stratégie critique de la donnée », Jean Baechler éd., *Guerre et Technique*, Hermann, 2017, pp. 309-322.

I.- Décrire la bascule numérique

135.- Comme l'indiquait déjà le Conseil d'État en 2014, dans son rapport précité sur le « numérique et les droits fondamentaux » : « [l]e numérique ne se réduit pas à internet, mais forme un système d'innovations techniques dont internet permet la mise en réseau ; le numérique n'est pas qu'un système d'innovations techniques, mais aussi un ensemble de transformations sociales et économiques, les trois dimensions s'alimentant l'une l'autre. Par la formule « le numérique », on désignera donc dans cette étude non seulement le phénomène technique, mais l'ensemble de ces mutations »[231].
Prolongeant ces indications, il apparaît que le moment numérique dans lequel nous nous trouvons a provoqué une bascule dont nous peinons à prendre la mesure et à saisir le sens, la signification comme la direction dans laquelle il emporte nos sociétés.

A.- Le moment numérique

136.- Le travail de dévoilement doit encore être mené ou approfondi dans le prolongement des études qui s'emploient notamment à discuter les métaphores permettant de saisir au mieux ce qui se joue, en particulier la nature révolutionnaire ou non du processus, les éléments de rupture ou de continuité ou encore les glissements d'un paradigme ou modèle à un autre ou à d'autres, en particulier s'agissant de la question centrale pour notre recherche, à savoir celle des contours, formes et modalités de la (mise sous) surveillance à partir de laquelle paraît s'édifier un modèle mondialisé d'organisation politique, économique et sociale.
137.- A cet égard, la première partie de l'ouvrage de Bernard Harcourt *La société d'exposition*[232] est certainement précieuse, là où sont discutées les métaphores récurrentes dans le débat public, médiatique ou académique, du « *Big Brother* » de Georges Orwell, de l'État de surveillance ou du « Panoptique » de Jeremy Bentham.
Tandis que, selon l'auteur, la première ne permet pas de saisir la particularité contemporaine d'une surveillance désirée ou qui, plus exactement se nourrit du désir et non, comme dans *1984*, de la haine et de l'élimination du désir, la deuxième fait l'impasse sur la surveillance privée, celle des GAFAM et autres opérateurs économiques avec lesquels les pouvoirs publics doivent composer. Quant à la troisième, elle bute sur l'intériorisation de la surveillance qui, essentielle au pouvoir panoptique, ne se vérifierait pas : la surveillance est tantôt ignorée, tantôt objet d'une indifférence radicale manifestée par des pratiques et relations d'exposition.
L'analyse proposée par Bernard Harcourt, inscrite dans le prolongement des travaux de Foucault sur le biopouvoir et le dépassement de la surveillance comme modèle des rapports de pouvoir au profit de la sécurité, étroitement liée au paradigme néolibéral, au sens, non d'un retrait de l'État et du « laisser-faire » mais d'un nouveau type d'interventionnisme promouvant la concurrence et l'individu-entreprise[233], peut aider à saisir la puissance des transformations en cours sur les grands repères qui structurent et informent le droit et la pensée juridique, en particulier les politiques criminelles[234].

---

[231] *Le numérique et les droits fondamentaux*, *op. cit.*, p. 9.
[232] HARCOURT Bernard, *La société d'exposition, Désir et désobéissance à l'ère numérique*, Seuil, 2020.
[233] Voir notamment, VERLENGIA Carolina, « Les origines d'un projet critique et la question du néolibéralisme : Foucault, une philosophie aux frontières » », *Astérion* [En ligne], 20, 2019, mis en ligne le 09 juillet 2019 – consulté le 19 juillet 2024.
[234] « La discipline est centripète : elle se concentre sur les cas de trouble mineur et cherche à en éradiquer la moindre occurrence. La sécurité, au contraire, est centrifuge : elle tolère les déviances mineures et cherche à optimiser, à minimiser ou maximiser, au lieu d'éliminer [Sécurité, territoire et population, Cours au Collège de France (1977-1978), éd. Michel Senellart, Paris, Gallimard/Éditions du Seuil, 2004, p. 46]. Et bien sûr, les deux diffèrent énormément du modèle juridique de la souveraineté, la forme du droit, qui opère une distinction binaire

L'auteur propose, quant à lui, de considérer que « nous sommes au-delà du modèle sécuritaire dans une sorte de transparence numérique et d'omniscience gratuite qui (…) façonne notre identité numérique »[235]. Même si « notre existence numérique est traversée par une logique et des pratiques néolibérales, nous sommes bien loin de la forme de pouvoir sécuritaire imaginée par Foucault à la fin des années 1970. La transparence recherchée par *Facebook*, *Google* et la *NSA* est absolue. L'idée n'est pas seulement d'optimiser cette connaissance en fonction des coûts, mais de parvenir à *tout* savoir ». Car « les données sont devenues une ressource brute gratuite, alors que cette ressource est une mine d'or »[236].

B.- La source numérique : la donnée

138.- C'est dire, et nous reprendrons cette hypothèse plus loin, combien ce nouvel objet – la donnée numérique – s'impose comme objet de recherche transverse ou transdisciplinaire au-delà du droit mais aussi comme un objet de recherche central pour les juristes.
Dans ce cadre-là, scruter les métaphores ou expressions employées pour figurer ou approcher la question sous-jacente et fondamentale de la nature des données apparaît également fertile. Qu'il s'agisse des « visions physiocratiques »[237] au moyen desquelles les données « sont parfois présentées comme un aliment ou des fleurs à récolter (semées par les usagers eux-mêmes, au hasard de leurs déplacements, et laissées en friche ou alors échangées contre des services fournis par les entreprises privées et qui dès lors n'appartiennent plus aux individus) », ou des « visions plus industrialistes »[238] dans lesquelles les données « seraient comme un minerai précieux à extraire de sa gangue rocheuse. Il importe d'avoir des outils de forage qui savent détecter ce qui est important et faire des tris qui permettent de ne retenir que ce qui a de la valeur. Au milieu de la masse de données qui circulent et qui sont hétérogènes, faiblement corrélées, il va falloir capter, intercepter et faire remonter celles qui correspondent à un certain profil, afin que, de leur mise en relation, émerge une information, qui doit aussi être affinée, taillée, un peu comme des diamants. Ainsi, l'analyse déboucherait non seulement sur une information de qualité, mais également une information utile dans le processus de décision politique »[239]. Point commun remarquable de ces deux métaphores, « l'idée que les données dites brutes n'appartiennent à personne »[240].
139.- Cette construction est aujourd'hui très largement battue en brèche comme en témoigne l'émergence du droit des données au sein duquel le droit des données personnelles s'emploie notamment à « attacher » la donnée à la personne[241].

---

entre le permis et l'interdit, et qui pénalise ce dernier [*Ibid.*, p. 7] », Bernard Harcourt, *La société d'exposition*, *op. cit*.

[235] « Pour dire les choses plus simplement, notre ère numérique est certainement néolibérale, mais pas strictement sécuritaire », *ibid*.

[236] *Ibid*.

[237] BIGO Didier et BONELLI Laurent, « "Nous ne sommes pas un Big Brother !" », *Cultures & Conflits*, 114-115, 2019, 199-226, sp. §11.

[238] BIGO Didier et BONELLI Laurent, « "Nous ne sommes pas un Big Brother !" », *op.cit*.

[239] *Ibid*.

[240] *Ibid*.

[241] L'idée qu'existent des données brutes reste néanmoins présente, comme le montre encore très récemment l'argumentaire présenté par le gouvernement français devant la Cour européenne des droits de l'homme dans l'affaire *EncroChat* (*A.L. et E.J. c. France*, 17 octobre 2024, précité) qui avançait que « la France s'est bornée à transmettre des données brutes (…) ces données ne sont devenues "personnelles" que grâce aux investigations menées par les enquêteurs britanniques » (§90). Argument que la Cour a cependant balayé soulignant que, de manière générale, « une donnée a un caractère "personnel" dès lors qu'elle se rapporte à une personne identifiée ou identifiable (…) peu important qu'elle soit conservée sous une forme codée intelligible uniquement à l'aide de l'informatique et ne pouvant être interprétée que par un nombre restreint de personnes » (§103) et, en particulier dans cette affaire, que « [l]a circonstance que les utilisateurs d'*EncroChat* localisés au Royaume-Uni n'ont été

C'est tout le sens du combat d'Edward Snowden, retracé dans le film documentaire *Citizen four*, réalisé par Laura Poitras, sorti en 2014. Comme il l'indique d'une formule lumineuse « *Metadata in aggregate is content. It tells a story about you which is made up of facts, but is not necessarily true* »[242].
Toutefois, si la donnée n'est pas cette *res nullius*, le problème de l'identification de l'instrument ou de la technique juridique le ou la mieux à même d'aménager un encadrement adéquat, moyennant en particulier une protection effective des droits fondamentaux susceptibles d'être enfreints, reste entier. Le rapport précité du Conseil d'État de 2014 l'illustrait parfaitement à propos de l'opposition entre les tenants d'une approche en termes de propriété et les partisans d'une approche fondée sur l'autodétermination informationnelle[243]. Il optait clairement en faveur de la seconde en préconisant d'écarter l'introduction d'une logique patrimoniale dans la protection des données personnelles et d'envisager celle-ci comme un droit à l'autodétermination informationnelle[244].

C.- Des ressources numériques pour la procédure pénale

140.- Apparemment éloignée des enjeux de l'enquête pénale, cette toile de fond est en réalité décisive s'agissant de l'encadrement juridique des données personnelles, lequel joue un rôle déterminant dans la reconfiguration de la procédure pénale (*infra*). Car il en va de la construction de la notion de « donnée » en « ressource » pour la procédure pénale. Les recherches réalisées sur le renseignement à la suite notamment des scandales et controverses ayant suivi les révélations d'Edward Snowden ont montré combien les données sont des constructions à la fois politiques et professionnelles[245], ce qui n'est pas sans incidence sur l'élaboration de leur régime juridique.

141.- Cette co-construction politique, professionnelle et juridique peut être approchée dans le champ de l'enquête et de la procédure pénale au travers du cas symptomatique du statut procédural du téléphone portable. Cet exemple permet également d'illustrer l'apport des analyses plus amples – philosophiques ou de science politique – sur le moment numérique. Ainsi Bernard Harcourt mobilise-t-il la figure du *Doppelgänger* (le double ou le sosie imaginaire, ici numérique) pour signifier le déploiement d'une nouvelle rationalité de « la similitude, de la correspondance, qui ne tient pas compte des liens de causalité ». Cette logique d'adéquation ou de correspondance parfaite au niveau individuel alimente la tentation prédictive à des fins commerciales comme de contrôle social (dans le prolongement des

---

identifiés qu'après l'exécution de la DEE [décision d'enquête européenne] n'ôte rien au caractère personnel des données transmises et n'affranchit pas la France de son obligation de respecter les droits des personnes concernées » (*ibid.*).

[242] « Les métadonnées agrégées, c'est du contenu. Elles racontent à propos de vous une histoire qui est faite de faits mais qui n'est pas nécessairement vraie », traduction libre.

[243] Opposition reprise, mais dépassée et actualisée par Bernard Harcourt dans la postface de l'édition française à *La société d'exposition* (*op.cit.*) car il s'agirait plutôt, selon lui, de faire feu de tout bois : tant de la privatisation qui confie aux sujets numériques (individuels) le bénéfice et le contrôle des flux d'information, que de la création d'un espace commun (collectif) et de nouvelles réglementations démocratiques (collectives). *Adde* : MASSON F., « Quel "modèle propriétaire" pour les données personnelles ? », *RTDCiv*. 2022, p. 777 et s.

[244] Cf. p. 264 et s ; « Proposition n° 1 : Concevoir le droit à la protection des données personnelles comme un droit à "l'autodétermination informationnelle", c'est-à-dire le droit de l'individu de décider de la communication et de l'utilisation de ses données à caractère personnel », p. 269.

[245] Notamment, les programmes de recherche coordonnés par Didier Bigo : Projet ANR « UTIC » (Les usages des technologies liées à l'interception des communications téléphoniques et Internet par les services de police et de renseignement et par leurs prestataires privés: la France dans son environnement européen) ; Projet ANR « GUARDINT » (Contrôle des services de renseignement: surveiller ceux qui nous surveillent – GUARDINT).

logiques et méthodes actuarielles). Or, cette figure du *Doppelgänger* ne pourrait-elle pas également marquer le passage qu'implique l'idée d'une « existence numérique », d'une « vie numérique » en introduisant celle selon laquelle le numérique n'est pas seulement le reflet de l'analogique mais son prolongement, son extension, préfigurant le rêve transhumaniste de l'humain augmenté ? Plus qu'une projection du corps dans l'espace virtuel, certains objets connectés, et en particulier le téléphone portable, correspondraient alors une « augmentation » de la personne[246].

Cette interrogation a pénétré l'enquête pénale et atteint le juge pénal amené à dire ce qu'est (ou plutôt ce que n'est pas) un téléphone portable[247] dans ce cadre. Elle apparaît ainsi au regard d'actes d'enquête innomés, révélés par la pratique policière et qu'il revient par conséquent au juge de qualifier pour déterminer le régime juridique qui lui est applicable.

C'est ainsi que la chambre criminelle de la Cour de cassation a été amenée à dire si un *smartphone* (un téléphone intelligent, augmenté donc par la mise en réseau et les services qu'il peut en conséquence rendre) est, selon les termes d'une autrice, « une part de soi »[248]. La réponse négative permet d'écarter le bénéfice du droit de ne pas s'auto-incriminer et de constater la conventionnalité de l'incrimination du refus de remettre le code de déverrouillage du téléphone, compris (à certaines conditions[249]) comme la convention secrète de déchiffrement d'un moyen de cryptologie visée par l'article 434-15-2 du Code pénal.

Ainsi, si « l'atteinte au droit de se taire et au droit de ne pas s'auto-incriminer est constituée dès lors que les données ne peuvent exister indépendamment de la volonté du suspect », ce n'est « pas le cas des données contenues dans les téléphones, qui peuvent être obtenues par des moyens techniques »[250].

En effet, « le droit de ne pas s'incriminer soi-même ne s'étend pas aux données que l'on peut obtenir de la personne concernée en recourant à des pouvoirs coercitifs mais qui existent indépendamment de la volonté de l'intéressé »[251].

De même, l'exploitation du *smartphone* pendant la garde à vue est « assimilable à une perquisition »[252] de sorte que la remise sur sollicitation du code de déverrouillage – conçu comme « une information permettant l'accès à un espace privé préalablement identifié, qu'il soit ou non dématérialisé »[253] – hors la présence de l'avocat, qui ne constitue pas une audition, n'est pas irrégulière. D'où il « ressort que le téléphone portable est considéré comme un espace privé, non comme un ersatz de la personne »[254].

142.- La justice en général[255] et la justice pénale en particulier n'ont pas été, bien au contraire, « épargnées » par la numérisation et la dataisation, non seulement parce que les contentieux ont

---

[246] Et l'on songe déjà aux questions que poseront dans un avenir pas si lointain les implants connectés (« Elon Musk annonce que sa start-up *Neuralink* a posé son premier implant cérébral sur un patient », *Le Monde*, 30 janvier 2024).

[247] PARIZOT Raphaële, « Qu'est-ce qu'un téléphone portable ? », *RSC*, 2021, p. 128.

[248] *Ibid*.

[249] Crim. 13 oct. 2020, n° 20-80.150 (« Le code de déverrouillage d'un téléphone portable peut constituer une telle convention lorsque ledit téléphone est équipé d'un moyen de cryptologie. L'existence d'un tel moyen peut se déduire des caractéristiques de l'appareil ou des logiciels qui l'équipent ainsi que par les résultats d'exploitation des téléphones au moyen d'outils techniques, utilisés notamment par les personnes qualifiées requises ou experts désignés à cette fin, portés, le cas échéant, à la connaissance de la personne concernée ») ; AP, 7 nov. 2022, n° 21-83.146.

[250] Crim., 10 décembre 2019, n° 18-86.878.

[251] *Ibid*.

[252] Crim., 12 janvier 2021, n° 20-84-045, §10

[253] *Ibid*. §11.

[254] PARIZOT Raphaële, « Qu'est-ce qu'un téléphone portable ? », *RSC*, 2021, p. 128.

[255] Justice et transformation numérique, *Revue Justice Actualités*, n° 26, accessible en ligne : https://www.enm.justice.fr/api/getFile/sites/default/files/actu-pdf/RJA_26.pdf

été naturellement investis par ces questions mais, en outre, parce que les méthodes de travail ou les pratiques d'organisation s'en sont inévitablement trouvées également transformées. A ce dernier égard, les propos de Sandrine Zientara-Logeay s'agissant de l'*open data* des décisions de justice lorsqu'elle évoque de nouveaux objectifs pour la justice ou la jurisprudence qu'il s'agit de valoriser ou de repenser (au travers par exemple de la hiérarchisation des décisions des juridictions de fond) soulignent, si besoin en était, les transformations des pratiques et l'importance de l'attention qu'il convient de leur accorder[256].

La difficulté à saisir ce moment numérique, les bouleversements qu'il induit et les réactions qu'il provoque, se manifeste et se prolonge au travers de la difficulté à nommer, à forger les mots du droit.

II.- Nommer les transformations numériques

143.- C'est particulièrement vrai et lourd d'implications dans le champ du droit et de la procédure pénale. La pénétration des (nouvelles) technologies de l'information et de la communication (TIC) au sein de la procédure pénale s'est relativement peu accompagnée de l'introduction de termes nouveaux. Lorsque tel est le cas, la teneur et la portée exactes peuvent interroger et participer de la faible lisibilité de la matière, soit que les termes véhiculent – avec une justesse et une précision relatives – des considérations et enjeux techniques[257] (qui requièrent vulgarisation, formation ou compétences spéciales) soit qu'ils questionnent quant à leur relation avec les catégories juridiques en vigueur (insertion, renouvellement des catégories existantes ou aptitude à en faire émerger de nouvelles).

144.- A l'inverse, la formulation de dispositions entièrement nouvelles ou renouvelées peut témoigner de la diffusion d'un vocabulaire qui, tout en se voulant techniquement ou technologiquement « neutre », est susceptible de fragiliser les notions et, partant, la prévisibilité attendue du recours aux mesures en question.
Un exemple d'une telle hypothèse peut être tiré de l'emploi (prolifique) du substantif « accès » ou du verbe correspondant « accéder ». Concernant ce dernier, on notera les indications du rapport explicatif à la Convention de Budapest qui souligne que l'article relatif aux perquisitions et saisies de données informatiques stockées « utilise l'expression "perquisitionner ou ... accéder par un moyen similaire". L'emploi du mot classique "perquisitionner" traduit l'idée de l'exercice par l'État d'un pouvoir coercitif et montre que le pouvoir visé dans cet article est analogue à la perquisition classique. "Perquisitionner" veut dire rechercher, lire, inspecter ou examiner des données, et inclut aussi les notions de recherche de données et d'examen de données. En revanche, le mot "accéder" a un sens neutre, mais est plus fidèle à la terminologie informatique. Les deux termes sont utilisés pour combiner les notions classiques et la terminologie moderne »[258].
Ici se pose alors la question de savoir dans quelle mesure la neutralité du terme ne modifie pas la compréhension de la catégorie dans laquelle la mesure s'insère, une perquisition supposant une « pénétration » et des actes de recherche active, ce qui la distingue de la surveillance (de nature passive).

---

[256] ZIENTARA-LOGEAY Sandrine, « *Open data* des décisions des tribunaux judiciaires : une nouvelle étape novatrice », *Dalloz Actualité*, 11 janvier 2024.
[257] Par exemple, « convention secrète de déchiffrement d'un moyen de cryptologie » visée par l'article 434-15-2 du Code pénal.
[258] *Rapport explicatif de la Convention sur la cybercriminalité, 23.11.2001* (https://rm.coe.int/16800ccea4).

D'autres exemples peuvent être relevés, telle que l'alternative entre données « accessibles » ou « disponibles » pour le système informatique perquisitionné, qui figure à l'art. 57-1 CPP et à l'art. 19 de la convention de Budapest, mais qui n'est, semble-t-il, explicitée nulle part[259].

145.- Mais ces deux stratégies normatives – vocabulaire « technique » ou au contraire techniquement neutre – et l'absence de préférence en faveur de l'une ou l'autre témoignent, dans le prolongement de la difficulté à nommer, de la difficulté à qualifier par l'intermédiaire de catégories articulées entre elles[260] et auxquelles associer un régime déterminé.
La généalogie des mesures d'enquête et de la confection de leur régime procédural permet de le comprendre, compte tenu de la construction par strates, à la manière d'un millefeuille, de dispositions éparses et peu ou pas harmonisées, de sorte qu'il s'agirait plutôt de la forme culinaire du millefeuille déstructuré ; ce qui ne favorise pas l'édification d'un ou d'ensemble(s) homogène(s)[261].
Le recours aux TIC ou NTIC dans le cadre de l'enquête se présente en effet de manière diffuse et éclatée au sein du CPP et ne semble pas faire émerger de catégorie(s) autonome(s) ou particulière(s).

146.- Pourtant, une nouvelle « catégorie » – à moins qu'il s'agisse seulement d'une nouvelle terminologie[262] – est bel et bien apparue dans le CPP qui réunit – sans s'y limiter ni les englober toutes – plusieurs techniques d'enquête qui recourent aux TIC. Il s'agit des « techniques spéciales d'enquête », plus exactement des « autres » techniques spéciales d'enquête[263].
L'introduction de ce nouvel ensemble qui comprend aujourd'hui le recueil des données techniques de connexion et des interceptions de correspondances émises par la voie des communications électroniques (art. 706-95-20), la sonorisation et la fixation d'images de certains lieux ou véhicules (art. 706-96 - art. 706-98) et la captation de données informatiques (art. 706-102-1 - art. 706-102-5) répond à un objectif de clarification et d'harmonisation des régimes applicables, lequel met en lumière le stade législatif antérieur caractérisé par l'accumulation de dispositifs particuliers non coordonnés.
Or, un tel objectif est poursuivi au moyen d'une appellation nouvelle, non définie et non délimitée, qui plus est introduite pour rassembler une partie seulement (les « autres » TSE) et non l'entièreté de ce qui la compose. Ce procédé législatif, dont le succès demeure douteux[264], est instructif à plus d'un titre.

147.- D'abord, il témoigne du besoin de systématisation et de rationalisation en la matière. Certes ce besoin est généralisé, le CPP étant devenu notoirement illisible, ce qui explique par ailleurs les tentatives de simplification, parfois contestables ou illusoires, dont il fait

---

[259] Sans doute faudrait-il réfléchir de manière plus approfondie et transversale à cette notion d'accès aux technologies. On songe ici, par exemple, au lexique utilisé dans le titre 1 de la loi n° 2021-1017 du 2 août 2021 relative à la loi de bioéthique : « Élargir l'accès aux technologies disponibles sans s'affranchir de nos principes éthiques ». Utiliser la notion d'accès à une technologie permettant, le cas échéant, d'avoir un enfant facilite l'évitement du débat sur un « droit à l'enfant ».
[260] *Supra*, Partie 2, section 2.
[261] *Ibid*.
[262] PARIZOT Raphaële, « Les (autres) techniques spéciales d'enquête, une non-catégorie juridique », *in* S. PELLE (dir.), *Quelles mutations pour la justice pénale du XXIème siècle ?*, Dalloz, p. 71-81.
[263] Section VI (Des autres techniques spéciales d'enquête), du chapitre II (De la procédure), du titre XXV (De la procédure applicable à la criminalité et à la délinquance organisées et aux crimes), du Livre IV (De quelques procédures particulières).
[264] En dépit de la volonté d'unification du législateur, le nouveau régime apparaît ni ordonné ni cohérent, mais obscur, PARIZOT Raphaële, « Les (autres) techniques spéciales d'enquête, une non-catégorie juridique », *art. préc.*

régulièrement l'objet[265]. Mais le développement rapide et constant des mesures d'enquête visant à tenir compte et tirer profit des nouvelles technologies est pour beaucoup dans cet obscurcissement. Plus exactement c'est le processus législatif auquel il est recouru à cette fin qui y contribue très largement lorsqu'il emprunte le chemin des procédures dérogatoires (porte d'entrée du CPP pour des mesures considérées extraordinaires) avant d'être étendu (par extension du champ d'application des procédures dérogatoires) voire généralisé au-delà (par introduction dans le droit commun).

148.- Ensuite, il témoigne de l'influence des instruments et discours internationaux.
Car c'est en leur sein que semble résider l'origine de cette appellation et c'est à partir d'eux qu'est promu son emploi. Pourtant ici, comme dans le CPP (ou les débats parlementaires qui ont précédé puis accompagné son introduction), aucune définition n'est fournie. Comme le note, par exemple, le groupe de travail pour la Conférence des États parties à la Convention des Nations Unies contre la criminalité transnationale organisée, « il n'existe pas de définition arrêtée sur le plan international de ce que sont les « techniques d'enquête spéciales ». Pourtant, l'emploi de la terminologie qui semble avoir pour origine le cadre onusien (certainement depuis la convention de Palerme[266], mais semble-t-il déjà en germe dans le cadre de la Convention des Nations Unies contre le trafic illicite de stupéfiants et de substances psychotropes de 1988[267]) s'installe et diffuse dans les cadres régionaux et nationaux. Et ce, sans que ne progresse la compréhension exacte de ce qu'elle recouvre. Ainsi, lorsque le Comité des Ministres du Conseil de l'Europe adopte en 2005 une recommandation à leur propos, c'est sans prendre la peine de les définir ou de les identifier autrement que par la gravité des infractions qui autorisent d'y recourir et le caractère clandestin supposé les caractériser[268]. La recommandation (2017)6 qui la remplace ne fait pas mieux et reprend la « définition » (*sic*) initialement proposée[269]. Au sein de l'Union, la formule est employée, notamment par le Parlement européen dans certaines des résolutions par lesquelles il recommande à la Commission une étude comparative des TSE[270].

---

[265] Voir TOUILLIER Marc et SIZAIRE Vincent (dir.), *La simplification de la justice pénale. Derrière la promesse, quelle réalité juridique ?*, Dalloz, coll. « Les sens du droit », 2022.
[266] *Ibid*.
[267] NILSSON H.G., « Special Investigation techniques and Developments in Mutual Legal Assistance – The Crossroads between police cooperation and judicial cooperation », disponible à https://www.unafei.or.jp/publications/pdf/RS_No65/No65_07VE_Nilsson2.pdf
Le tremplin des TSE semble ainsi international et plus particulièrement lié au tournant opéré par la coopération policière et judiciaire dans le courant des années 80 vers une entraide plus directe entre services et autorités nationales jusqu'à la formation d'équipes communes.
La reprise de la formule, bien qu'aménagée par la Convention STE 141 à son article 4 (Pouvoirs et techniques spéciaux d'investigation), conforte le rôle de la coopération internationale en tant que (pro-)moteur de cette « catégorie » fonctionnelle (*i.e.* dont la définition est réalisée au moyen d'une liste non exhaustive de mesures). Autrement dit, c'est un objectif d'harmonisation pour les besoins de la coopération qui semble faire émerger la quasi-catégorie. Le rapport explicatif l'énonce clairement : « Le paragraphe 2 de l'article a été rédigé pour faire prendre conscience aux États des nouvelles techniques d'investigation qui sont pratique courante dans certains d'entre eux, mais qui n'ont pas encore été mises en œuvre dans d'autres. Ce paragraphe fait obligation aux États, au minimum, d'envisager l'adoption de techniques nouvelles qui, dans certains États, tout en sauvegardant les droits de l'homme fondamentaux, ont permis de combattre avec succès la criminalité grave. Ces techniques pourraient alors être utilisées aussi aux fins de la coopération internationale. Dans ces cas, le chapitre III, section 2, serait d'application. L'énumération des techniques n'est pas exhaustive ». Une analogie pourrait être établie avec la diffusion, en Europe (cf. le système Prüm) et dans le monde, de systèmes d'échanges de profils génétiques via l'accès à des bases de données.
[268] https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Rec_2005_10.pdf
[269] « Aux fins de la présente recommandation, on entend par "techniques spéciales d'enquête", les techniques appliquées par les autorités compétentes dans le cadre d'enquêtes judiciaires en vue de prévenir, de déceler et d'enquêter sur des infractions graves, et de poursuivre et réprimer leurs auteurs, dans le but de recueillir des informations sans attirer l'attention des personnes visées ».
[270] Résolution du 11 juin 2013 notamment (2012/2117 (INI)).

Mais là non plus, aucune définition n'est proposée. Un auteur[271] suggère néanmoins la possibilité de dégager deux traits distinctifs alternatifs : le caractère secret (ou clandestin) de la mesure ou son caractère trompeur quasi-déloyal (ou déceptif).

149.- Centrée sur la démarche du législateur français, l'analyse des TSE dans le CPP montre combien il est joué sur l'ambivalence de l'expression au risque de l'ambiguïté et de la confusion[272]. C'est ainsi que si l'adjectif spécial paraît de prime abord désigner les techniques d'enquête (notamment en ce qu'elles supposent l'intervention d'un technicien qualifié ou de fonctionnaires spécialement formés – c'est alors la dimension technico-technologique qui est soulignée), il semble par glissement qualifier l'enquête (ou plutôt la criminalité qui autorise le recours à des pouvoirs dérogatoires, *i.e.* spéciaux – c'est alors par le truchement de la gravité ou de la complexité de la délinquance visée qu'est souligné et justifié en creux le recours à des mesures spécialement intrusives).
Compte tenu du cadre d'apparition (le trafic de stupéfiants avant que la criminalité organisée ne prenne sa place), il est permis d'ajouter que ces traits distinctifs ne sont que la partie émergée d'une démarche qui se caractérise par un renversement de la conception classique de l'enquête pénale en faveur d'une perspective non plus réactive (déclenchée par la commission ou la suspicion de la commission d'une infraction) mais davantage proactive ou « approche en amont »[273] qui fait le pont avec les techniques de renseignement ou s'en inspire. Dans la mesure où il s'agit de découvrir l'activité criminelle mais également de comprendre comment fonctionne l'ensemble du marché criminel, cette approche consiste à réunir des informations, à les analyser et à rapprocher des données[274].
Finalement, ce procédé – de recours à une pseudo-classification ou à une non-catégorie[275] juridique – témoigne peut-être d'une période transitoire où le besoin de rationalisation fait apparaître des classifications imparfaites dont ne dérivent pas (encore) de nouvelles catégories opératoires.
Toujours est-il que les TSE ne recoupent pas exactement le recours en procédure pénale au TIC[276], ce que signale peut-être incidemment l'absence du vocable dans la convention de Budapest. Or l'insuffisante conceptualisation ou rationalisation de l'encadrement de ces techniques d'enquête pèse autant sur les pratiques[277], leur usage étant rendu complexe et incertain, qu'elle fragilise ou déstabilise les principes directeurs de la procédure pénale.

150.- Autre exemple de la difficulté (et de son importance) à nommer : la conservation dite rapide. C'est encore du droit international, en l'occurrence la Convention de Budapest, que viennent cette appellation (en anglais *quick freeze*) – peu claire – et la notion – non moins ambiguë – qu'elle recouvre, qui ont été promises à un succès inattendu en droit interne, peut-être précisément en raison de l'incertitude qui les entoure. Instrument de conciliation de l'inconciliable (?), la formule pénètre le droit interne à la faveur de sa mobilisation par les juges

---

[271] MOONEN T., « Special Investigation Techniques, Data Processing and Privacy. Protection in the Jurisprudence of the European Court of Human Rights », *Pace International Law Review Online*, 4-2010 https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1012&context=pilronline
[272] PARIZOT Raphaële, « Les (autres) techniques spéciales d'enquête, une non-catégorie juridique », *op. cit*.
[273] *Livre blanc sur le crime organisé transnational*, Conseil de l'Europe, 2014 qui consacre un paragraphe étendu aux TSE.
[274] *Ibid.* Pour une perspective historique et de science politique plus générale sur la convergence entre surveillance électronique et pratiques punitives, voir B. Harcourt, *La société d'exposition*, *op.cit*.
[275] PARIZOT Raphaële, « Les (autres) techniques spéciales d'enquête, une non-catégorie juridique », *op. cit*.
[276] L'utilisation des TIC ne constitue pas en soi une TSE ; NILSSON H.G., « Special Investigation techniques and Developments in Mutual Legal Assistance – The Crossroads between police cooperation and judicial cooperation », *op. cit*.
[277] *Supra*, Première partie, n°40 ou n°48.

du Conseil d'État et de la Cour de cassation qui ont décelé sa présence au sein du pouvoir de réquisition, avant même sa réception dans les textes et indépendamment d'elle.

151.- Les appellations de procédure pénale numérique ou de preuve électronique apparaissent encore davantage révélatrices de la fragilité du lexique procédural. La première apparaît en effet quelque peu déceptive dans la mesure où elle se réduit (même si ce n'est pas rien) à la numérisation (à droit constant) de la procédure pénale dès son origine, c'est-à-dire à la dématérialisation (disparition du papier) et au recours à la signature électronique, mais suppose une interconnexion des très nombreux systèmes d'information impliqués dans une procédure pénale[278]. Quant à la seconde, désormais fixée dans le vocabulaire européen au sein des textes de coopération en matière pénale[279], elle vise de manière étroite « les données relatives aux abonnés, les données relatives au trafic ou les données relatives au contenu stockées par un fournisseur de services ou pour le compte d'un fournisseur de services, sous une forme numérique, au moment de la réception d'un certificat d'injonction européenne de production (EPOC) ou d'un certificat d'injonction européenne de conservation (EPOC-PR) »[280], sans constituer une catégorie nouvelle.

Nés des besoins de la coopération judiciaire, ces nouveaux instruments témoignent de l'association étroite du processus de dataisation à celui de transnationalisation qu'il convient à présent d'envisager.

§2.- La transnationalisation ou la mise en réseaux du monde

152.- Deuxième processus, davantage (re)connu et travaillé, ce qui permettra de le mentionner seulement ici sans s'y arrêter spécialement, la transnationalisation modifie profondément les grands repères, en particulier juridiques. Car la transnationalisation touche et affecte tant les questions, phénomènes ou problèmes posés ou, en conséquence, les réponses apportées que – ce qui ne doit pas être ignoré – la construction des uns (en tant qu'enjeu ou menace, déviance ou infraction) et des autres (par la configuration d'une réaction politique, économique, sociale ou juridique et s'agissant de cette dernière, en termes de prévention, remédiation, réparation ou répression).

Or, ce processus de transnationalisation – auquel d'ailleurs contribue la dataisation – a pour effet de relativiser (sans l'annihiler) le rôle structurant de la frontière en droit en général et en procédure pénale en particulier (*I*). Il a aussi pour effet, ce d'autant plus lorsqu'il est conjugué à la dataisation, de « disqualifier » le territoire en tant que point de référence ou de rattachement pour la conception et l'application des règles de procédure (*II*).

I.- Brouillage des « frontières »

153.- Avec la transnationalisation et la porosité des frontières qu'elle induit, de nouvelles notions apparaissent sans se substituer aux notions voisines existantes ni s'articuler clairement

---

[278] Voir à ce propos la cartographie figurant dans le rapport de la Cour des comptes, *Les moyens affectés aux missions de police judiciaire*, Exercices 2017-2022, Annexe n° 17 (La « boîte à outils numériques de l'enquêteur »).
[279] *Règlement 2023/1543 du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale*.
[280] Art. 3 8) du Règlement.

avec elles. Tel est le cas de la notion d'espace, notamment consacrée à l'échelle de l'Union au travers de l'« espace de liberté, sécurité et justice »[281].
Plus largement, d'importantes distinctions perdent de leur tranchant. Il en va ainsi des distinctions suivantes liées entre elles : national/international, intérieur/extérieur, paix/guerre, justice/renseignement, prévention/répression, police administrative/police judiciaire, toutes distinctions qui structurent également le déroulement de l'enquête pénale, le périmètre et les modalités d'application des dispositions de procédure pénale.

II.- Dépassement du territoire

154.- Outre la question de la localisation des conduites, se pose de manière aiguë celle des contours et limites de la réponse pénale et, pour en permettre le déploiement, celles de l'étendue des pouvoirs policiers et judiciaires et des conditions de la coopération internationale.
La définition des actes d'enquête et la confection de leur régime sont directement affectées et transformées par ces considérations, comme le montre l'exemple paradigmatique des perquisitions.
Comme l'écrit Sophie Sontag Koenig[282], l'espace « clos et privé » devient un espace numérique et « prend une nouvelle dimension, presque abyssale, dans la mesure où le système informatique peut s'interconnecter avec d'autres et être relié au réseau internet. Prenant acte de cette possibilité technique, le législateur a donc permis d'atteindre les données accessibles à distance depuis le système initial, car délocalisées dans un autre système. De surcroît, cette perquisition distante peut même s'opérer depuis les locaux d'un service ou d'une unité de police ou de gendarmerie [[283]] ». Mais « quand le lieu s'externalise et se dématérialise, l'enquêteur doit répondre à une question supplémentaire tenant à la localisation des données auxquelles il veut accéder, ce qui pose une difficulté accrue dans le cas du *cloud computing*. Consistant à héberger sur des serveurs distants des traitements informatiques auparavant localisés sur un serveur local ou sur le poste de l'utilisateur, le *cloud computing* conduit à un stockage (et donc une localisation) fractionné de données sur plusieurs serveurs potentiels, parfois aléatoirement sollicités. L'enjeu est important car la localisation des données détermine le droit applicable. Si ces données sont situées hors du territoire national, le législateur impose à l'enquêteur de respecter les conditions d'accès prévues par les engagements internationaux en vigueur [[284]]. De façon littérale, cela signifierait que si l'officier de police judiciaire a conscience [[285]] que les données informatiques, accessibles depuis le territoire national, sont en fait stockées à l'étranger, deux options s'offrent à lui selon que l'État hébergeur a ou non ratifié la convention de Budapest qui exige un assentiment exprès de la personne concernée pour procéder à la perquisition à distance de ses données stockées à l'étranger. À défaut d'assentiment (ainsi que dans le cas où l'État conservant les données n'est pas partie à cette convention), l'enquêteur n'a en principe

[281] Au sein d'une abondante littérature, voir en particulier POILLOT-PERUZETTO Sylvaine « Le nouveau défi de la construction de l'espace de liberté, de sécurité et de justice », *in* VAYSSIERE Sylvaine (dir.), *L'Europe, objet renouvelé des sciences sociales*, PUM, 2013, pp. 125-136, qui souligne combien « l'utilisation du terme espace n'est pas neutre », en ce qu'elle permet « de dégager l'Europe de la conception classique du territoire » et ce faisant de porter en germes un renouvellement de la conception même du droit.
[282] Numéro spécial de l'AJ Pénal, « L'accès à la preuve obtenue par les nouvelles technologies d'investigation et de surveillance », qui constitue l'un des résultats de la présente recherche, 2023, n° 11 : SONTAG KOENIG Sophie, « La transformation des actes d'enquête : de la perquisition (informatique) aux autres techniques de captation », *AJ Pénal*, n° 11, 2023, p. 486 et s.
[283] Note de l'auteure : Art. 57-1, al. 2 CPP.
[284] Note de l'auteure : Art. 57-1, al. 3 CPP.
[285] Note de l'auteure : L'article utilise la formule « s'il est [...] avéré ».

d'autre choix que de faire appel à l'entraide pénale internationale afin d'autoriser toute recherche et saisie de ces données... »[286].

On l'a dit, ces processus de dataisation et de transnationalisation ou de mise en données et de mise en réseaux, se généralisent, convergent et s'alimentent. Or cette convergence débouche sur l'expansion de la surveillance à la faveur de la montée en puissance de la sécurité.

§3.- La « sécurisation » ou la mise sous surveillance du monde

155.- Le constat d'une mise sous surveillance du monde, servie par les mises en données et en réseaux, semble pouvoir être présenté comme le fruit du succès conjugué d'un concept, la sécurité (*I*) (et avec lui des modes de représentation/construction des enjeux politiques, économiques ou sociaux, des instruments de l'action politique et des traductions normatives), et d'une méthode, le renseignement (et ses acteurs) (*II*).

I.- Essor de la sécurité

156.- La montée en puissance du concept de sécurité, notamment sa prétention à concurrencer par absorption celui de sûreté, n'est pas neuve. Déjà l'intitulé de la loi Peyrefitte n° 81-82 du 2 février 1981, dite « sécurité et liberté » en témoignait[287]. Toutefois, sa transformation en concept total ou multidimensionnel, couvrant les champs politique (sauvegarde/restauration de la démocratie/maintien de l'ordre établi), économique (sauvegarde notamment du système financier) ou social et reliant dans un *continuum* l'intérieur et l'extérieur, apparaît plus récente, et est notamment liée au « contexte terroriste », national et mondial.
Le concept permet en effet de construire les risques ou menaces en mettant l'accent sur certaines menaces d'ordre systémique, ce qui requiert, compte tenu de leur gravité, des réponses du même ordre, c'est-à-dire des réponses se situant à la fois très en amont puisque le risque systémique ne doit pas se produire (dès lors qu'il met en péril le système lui-même, sa survie – que ce soit la démocratie ou le système bancaire) ; mais aussi des réponses exceptionnelles (à la mesure là aussi de risques extraordinaires, même si l'approche par les risques légitime aisément une réaction dès l'apparition de signaux faibles), donc dérogatoires au droit commun.
Enfin, et de manière déjà bien documentée, le concept de sécurité favorise des mécanismes de diffusion ou de contamination au-delà du cadre ou contexte de naissance.
C'est sa nature totalisante ou indéterminée qui le lui permet, comme le montre par exemple, de manière incidente, l'appellation de « forces de sécurité » qui, selon les cas ou contextes, désigne des acteurs exclusivement publics ou inclut des acteurs/opérateurs privés, des acteurs nationaux ou locaux, militaires ou civils, relevant de la police administrative ou judiciaire.

II.- Promotion du renseignement

157.- Ce « cocktail » d'anticipation et d'exception (dont le secret est l'une des caractéristiques majeures) s'est révélé très profitable au renseignement : ses objectifs, ses acteurs et ses méthodes. D'autant que le registre du dérogatoire peut servir de tactique ou mécanisme de légitimation. C'est par son biais qu'a été banalisée et normalisée l'hypothèse selon laquelle le

---

[286] SONTAG KOENIG Sophie, « La transformation des actes d'enquête : de la perquisition (informatique) aux autres techniques de captation », *op. cit.*, p. 487 et s.
[287] DELMAS-MARTY Mireille, *Les grands systèmes de politique criminelle*, Paris, PUF, 1992.

« branchement des techniques de renseignement sur les technologies automatisées de relevé de traces des activités et des transactions des individus [est] légitime »[288], en tant que « contrepartie d'une fonction de protection et de prévention permettant d'anticiper et d'éviter la violence »[289].

Si le constat d'une contribution du renseignement à la procédure pénale est loin de constituer une nouveauté[290], son rôle s'est cependant transformé à la faveur de la « promotion » juridique récente du renseignement. Tandis que la visibilité accrue et nouvelle du renseignement (action, domaine et acteurs) participe paradoxalement, grâce aux controverses et scandales, du processus de légitimation de ce dernier, le droit joue vis-à-vis d'un tel processus un rôle aussi majeur qu'ambivalent : « en exerçant une contrainte sur des services désormais sommés d'agir dans les règles, le droit constitue alors un puissant vecteur de normalisation de leurs pratiques »[291]. Ce qui explique sans doute en partie que l'encadrement juridique des pratiques soit réclamé par les acteurs eux-mêmes, étant souligné qu'ils ont au préalable convaincu de la légitimité de leurs méthodes par d'intenses démarches de lobbying à cette fin[292].
Cette promotion passe aussi par l'apparition de nouveaux acteurs du renseignement dont le nombre et les types augmentent : ainsi des cellules de renseignement financier qui se nourrissent de la dataisation.
Elle passe enfin par la proximité grandissante, pouvant confiner à la confusion, du renseignement et de la procédure pénale, ou à tout le moins par la circulation à double sens des données issues des sphères, de moins en moins étanches, du renseignement ou de la procédure pénale[293] et par la dépendance grandissante de la seconde vis-à-vis de la première qui maîtrise très largement les termes de leurs relations et les conditions de leurs interactions[294].

* *
*

158.- La déstabilisation des repères déborde et dépasse largement le champ de l'enquête pénale mais en déterminant les mouvements qui le traversent elle constitue son contexte de conception (des principes et règles qui l'encadrent) et d'application (des pratiques des acteurs chargés de sa mise en œuvre).
C'est la raison pour laquelle l'analyse de la confrontation entre la technique juridique (les règles de procédure pénale et la manière dont les acteurs s'en saisissent) et les technologies d'investigation et de surveillance requiert un effort continu de contextualisation qui interroge le moment politique, économique et social dans lequel nos sociétés se trouvent sous l'effet combiné de la dataisation, de la transnationalisation et de la sécurisation.

---

[288] BIGO Didier et BONELLI Laurent, « "Nous ne sommes pas un Big Brother !" », *Cultures & Conflits*, 114-115, 2019, 199-226, sp. §7.
[289] *Ibid*.
[290] ROSS Jacqueline E., « The emergence of foreign intelligence investigations as alternatives to the criminal process: a view of American counterterrorism surveillance through German lenses », *in* ROSS Jacqueline E., THAMAN Stephen C. (ed), *Comparative Criminal Procedure*, Elgar, 2016, p. 475.
[291] BONELLI Laurent, RAYNER Hervé et VOUTAT Bernard, « Contestations et (re)légitimations du renseignement en démocratie », Cultures & Conflits, 114-115, 2019, 7-28, sp. §21.
[292] *Ibid*.
[293] Voir, *supra*, Première partie, la *Cartographie des acteurs du recueil et de l'administration du renseignement et de la preuve numériques*.
[294] GUILLARD Antonin, « Sonorisation et fixation d'images au croisement de la procédure pénale et du renseignement », *AJ Pénal*, n° 11, 2023, (Dossier L'accès à la preuve obtenue par les nouvelles technologies d'investigation et de surveillance), p. 484.

Interface entre ce contexte et les règles de l'enquête pénale mises en pratique, l'encadrement normatif (toutes sources confondues : internationales, européennes, constitutionnelles, législatives ou réglementaires) trahit ou traduit l'effet de déstabilisation par le foisonnement des textes et l'incertitude ou l'indétermination relatives de leur contenu ainsi que plus fondamentalement la faiblesse de la rationalité ou cohérence d'ensemble.
Ainsi, la généalogie de chaque mesure d'investigation ou de surveillance témoigne, si besoin était car c'est une constante du droit de la procédure pénale des trente dernières années, de l'adoption continue de normes à la fois inflationnistes et précaires, alors que, dans le même temps, les acteurs expriment un besoin de certitude que la règle de procédure ne parvient pas à satisfaire, d'autant plus qu'elle est très largement exposée à sa contestabilité (non seulement quant aux usages dont elle est l'objet mais plus profondément quant à sa légitimité même).
Or, une partie – mais une partie seulement, il faut y insister – de la « réponse » à ce besoin (qui est plus largement la promesse dont doit être porteuse la règle pénale procédurale) semble résider dans l'émergence – désormais ancienne – et la consolidation – plus récente – d'un droit des données personnelles qui vient profondément rebattre les cartes des règles du jeu juridique en proposant ou imposant une approche renouvelée de l'exercice des pouvoirs d'enquête et de son produit, la preuve pénale.

Section 2 : Reconfiguration de l'enquête pénale

159.- Se pourrait-il alors que soit en cours ou en vue une reconfiguration de l'enquête et de la procédure pénales à partir du droit des données personnelles ? C'est l'hypothèse inattendue, encore provisoire et dont il faut avoir conscience des limites, que la recherche a fait émerger et dont elle a commencé à vérifier la pertinence (*§1*). Ainsi, si la rencontre du droit des données personnelles et de la procédure, en faisant advenir un nouvel objet : la donnée numérique pénale, invite et concourt à la formation d'une nouvelle configuration de l'enquête pénale, il se pourrait que cette rencontre produise des effets au-delà (*§2*).

§1.- Émergence de la donnée numérique pénale

160.- Incontestablement le droit de l'Union européenne et la jurisprudence de la Cour de justice, qui ont remarquablement marqué et scandé le rythme de la recherche au point d'en orienter largement le cours, y sont pour beaucoup.
Toutefois, comme la mise en contexte visait à le montrer, l'un et l'autre ne constituent sans doute qu'une réponse parmi d'autres aux mouvements de dataisation et de transnationalisation et non leur source.
Aussi bien, ce qui est apparu au cours de la recherche, c'est un nouvel objet ou champ de recherche qui serait constitué par ce que l'on pourrait nommer la donnée numérique pénale. En effet, les données numériques apparaissent comme la cible ou le matériau commun des mesures d'enquête étudiées. Mais alors se pose la question de savoir comment sont « constituées »[295] ces données pénales.
La question se dédouble car la construction peut être d'une part le résultat d'un processus proprement technologique ou relevant de la pratique policière et, d'autre part, le fruit de l'application du droit, de sorte que la construction de la donnée pénale apparaît la résultante

[295] Terme emprunté, et avec lui l'idée que les données n'ont rien de « donné » mais sont construites, à BIGO Didier et BONELLI Laurent, « "Nous ne sommes pas un Big Brother !" », *Cultures & Conflits*, 114-115, 2019, 199-226.

d'une construction tout autant extra- ou para-juridique que juridique. La recherche n'a cependant pu explorer tous les aspects d'une telle élaboration. S'agissant du premier versant, elle a tout de même permis de dévoiler le potentiel d'études et recherches à venir qu'appelle la donnée numérique pénale (*I*). Elle s'est cependant surtout concentrée sur le second versant, à savoir la construction juridique subséquente de la donnée numérique pénale, telle qu'elle résulte du droit en action (*II*).

I.- La construction extra-juridique de la donnée numérique pénale

161.- La construction de la donnée numérique pénale renvoie à la construction pénale de la donnée numérique, c'est-à-dire à la place et au rôle de la donnée dans l'enquête pénale. Or, parce que la donnée est tout à la fois susceptible d'orienter ou alimenter l'enquête (donc de déterminer l'action des enquêteurs) et de constituer le résultat de cette action (la preuve), son rôle et sa place varient, en particulier en fonction de la disponibilité d'autres éléments à même de remplir les mêmes fonctions ou fins.
De là, l'interrogation des professionnels pour déterminer l'effet de substitution (obsolescence) des NTIS aux mesures d'enquête plus traditionnelles, ou la ventilation et l'articulation du recours qui y est fait - respectivement - et dont il résulte que le dédoublement technologique d'une technique traditionnelle (analogique/physique) d'enquête ne fait pas disparaître l'intérêt de l'enquêteur pour cette dernière mais ajoute à sa palette. L'effet apparaît ainsi cumulatif (la mesure traditionnelle se « technologise »[296]) ou successif (les deux mesures se suivent) plutôt qu'alternatif[297].

162.- Mais, s'agissant de l'analyse des pratiques professionnelles, des enquêtes de grande ampleur sur le temps long permettraient de mieux mesurer, ce qui n'a pu qu'être effleuré ou deviné ici, la variation de la sensibilité aux technologies (et en particulier à la dataisation) selon les autorités/services et types d'enquête (*lato sensu*)[298]. Ainsi, à l'image de ce qui a pu être démontré dans le cadre d'une enquête au long court dans le domaine du renseignement[299], pourrait sans doute être vérifiée une différenciation – évolutive – entre les services/autorités dépendant des technologies *high tech* (tels que par exemple certains services de renseignement, notamment dans le champ économique et financier et à l'évidence les services spécialisés dans la cybercriminalité) et ceux davantage attachés aux méthodes *low tech*[300] ; cette variation n'interdisant pas de constater la diffusion d'un minimum « tech » commun[301].
163.- A ce dernier égard, c'est une autre question de recherche, seulement abordée ici, qui mériterait approfondissement, dans le sillage d'autres études générales ou sectorielles, à savoir le rôle de la numérisation (dans toutes ses déclinaisons notamment la superposition ou non de

[296] Ainsi par exemple de l'exemple de la filature, jugée « toujours » plus fiable, qui s'enrichit de la fixation d'images par exemple.
[297] *Supra,* Première partie, aucun des enquêtés, interrogé à ce propos, n'a constaté l'obsolescence d'une mesure d'enquête « traditionnelle » au profit de mesures fondées sur les nouvelles technologies ; s'observent plutôt des choix et stratégies d'emploi qui évoluent du fait de l'enrichissement de la gamme des mesures « offertes » à l'enquêteur et varient en fonction des circonstances particulières (intérêt pour l'enquête, risques pour l'enquêteur, conditions et contraintes juridiques d'emploi).
[298] Voir *supra*, Première partie, not. n°60 et l'« avance » de la Gendarmerie en matière d'enquête cyber.
[299] Cf. le projet ANR « UTIC », précité (https://anr.fr/Projet-ANR-14-CE28-0024).
[300] BIGO Didier et BONELLI Laurent, « "Nous ne sommes pas un Big Brother !" », *Cultures & Conflits*, 114-115, 2019, 199-226.
[301] Là encore, cette différenciation est illustrée par les entretiens réalisés, cf. *Supra* Première partie.

l'analogique, d'automatisation et d'interconnexion) sur les pratiques quotidiennes des professionnels de l'enquête et les modes opératoires ou de raisonnement[302].
Là aussi, la recherche n'apporte que de premiers éléments de réflexion ou de confirmation partielle d'intuitions quant au potentiel « révolutionnaire » des mutations technologiques sur les pratiques, entre « l'illusion du jamais vu et l'illusion du toujours ainsi »[303].
Ce qui apparaît néanmoins c'est une double quête d'économie de moyens, supposément permise par la technologie, et de recentrage sur l'activité d'enquête distinguée de tâches qualifiées d'administratives ou formelles en dépit (ou à cause) de leur lien avec la protection de garanties de procédure et donc de protection des droits fondamentaux[304].
164.- A l'arrière-plan de ces deux questions de recherche qui renvoient aux « techniques policières » et en ce sens à la construction « technique » de la donnée pénale, se pose la question de la construction « technologique » de la donnée pénale. Ce point n'a pu qu'être entrevu[305] au travers du rôle que jouent les acteurs souvent privés dans le développement et la fourniture de « solutions » technologiques aux besoins de la justice pénale ou l'offre de nouvelles opportunités. La solution « technologique », voire le solutionnisme technologique, peuvent ainsi venir s'insérer dans les marges ou insuffisances de l'encadrement juridique quand ils ne le contestent pas. C'est ce qu'illustre le cas des demandes d'accès direct aux opérateurs de communications électroniques en dehors du cadre « normal » de la plateforme numérique dédiée : la PNIJ et du recours aux logiciels privés[306].

II.- La construction juridique de la donnée numérique pénale

165.- Pour envisager la construction juridique de la donnée numérique pénale, il peut être recouru au vocabulaire informatique. Pour mettre au jour la nouvelle « configuration » qui semble se dessiner de l'enquête pénale, il faut d'abord en exposer les « paramètres système » (*A*) avant d'en explorer les « préférences système » (*B*). Les premiers correspondent au cadre imposé par le droit de l'Union, les secondes aux options nationales qu'il laisse ouvertes et dont se saisissent de façon variée les ordres internes.

A.- Paramètres d'une nouvelle configuration

166.- La construction de la donnée pénale n'est pas seulement une construction procédurale, elle est aussi nécessairement déterminée par ce qu'il faut démontrer : la qualification substantielle. Réciproquement, la construction de cette qualification peut valoriser certains

---

[302] Tel que par exemple le raisonnement de l'autorité en chargée de l'autorisation ou du contrôle, s'agissant de l'appréciation de la proportionnalité et de la subsidiarité de la mesure d'enquête, cf *supra* Première partie, n°50 et s.
[303] LACROIX Bernard, « Retour sur 1848 : Le suffrage universel entre l'illusion du "jamais vu" et l'illusion du "toujours ainsi"», *Actes de la recherche en sciences sociales*, n° 140, 2001, pp.41-50, cité par Didier Bigo et Laurent Bonelli ; sans avoir pu l'étayer suffisamment, les entretiens menés (*supra* première partie) paraissent rejoindre l'analyse menée par ces auteurs selon laquelle : « les évolutions qu'impliquent les transformations techniques et les opportunités nouvelles qu'elles offrent viennent en effet s'articuler avec du déjà-là, en termes de socialisations professionnelles et de routines de travail. Les changements qui peuvent advenir sont dès lors graduels et s'intègrent dans des missions, des savoirs et des finalités existant de longue date ».
[304] Voir par exemple, le rapport d'information n° 110 rédigé par les sénateurs Agnès Canayer et Philippe Bonnecarrère sur les modalités d'investigation recourant aux données de connexion dans le cadre des enquêtes pénales (15 novembre 2023), notamment p. 119 ou l'évocation du risque de « choc procédural », p. 108.
[305] Grâce notamment aux regards des professionnels de l'enquête ou du secteur privé sur les rôles des uns et des autres, cf. *supra* Première partie, n°73.
[306] CANAYER Agnès, BONNECARRERE Philippe, *op.cit*., p. 49-53.

acteurs, significativement ceux du renseignement, auparavant étrangers ou éloignés de l'enquête pénale et dont les méthodes affectent la procédure pénale.
Aussi, bien que centrée sur l'enquête, la recherche ne peut ignorer les déterminants substantiels de la confection des règles de procédure. Sur ce point, il faut revenir sur la place et le rôle du droit du renseignement et du « paradigme » sécuritaire[307] qui favorise l'anticipation de la répression et mobilise à cette fin le droit pénal spécial. L'expansion des infractions formelles ou obstacles illustre la façon dont le droit pénal spécial peut servir de chaînon permettant de construire le *continuum* renseignement – procédure pénale *via* la circulation des données. Ainsi, la position de premier plan reconnue désormais au(x services de) renseignement face à certaines formes de criminalité et l'intérêt, voire le caractère nécessaire/indispensable et non seulement utile, du renseignement pour la justice pénale ne peuvent être décorrélés de la définition des infractions en termes de menaces, laquelle nourrit des obligations de déclaration et des dispositifs de surveillance susceptibles d'alimenter le circuit pénal[308].
167.- Mais si la construction juridique de la donnée pénale est déterminée par le droit pénal de fond, les transformations qu'elle implique pour la procédure pénale paraissent tenir plus encore à la rencontre – nouvelle, difficile et délicate – de cette dernière avec certains droits fondamentaux anciens (le droit à la protection de la vie privée, de la liberté d'expression ou les droits de la défense) ou nouveaux (le droit à la protection des données personnelles). Plus encore, cette rencontre s'opère alors qu'émerge un droit des données personnelles qui, telle est l'hypothèse avancée, paraît reconfigurer l'enquête et la procédure pénale, à la faveur non seulement d'une politique normative (européenne) déterminée mais aussi d'une politique jurisprudentielle (également européenne) non moins engagée et fondée sur la promotion du droit fondamental à la protection des données personnelles. Par son intermédiaire apparaît une nouvelle grille de validité des procédures pénales qui, sans oblitérer les grilles préexistantes, en bouscule la structure et en fragilise la solidité tant en termes d'adéquation que de légitimité.

168.- Parmi les sources régissant et organisant le droit à la protection des données personnelles et à la vie privée, le droit de l'Union européenne[309] occupe, en effet, une place éminente, plus exactement la première, tant par le nombre, l'empire et l'emprise des textes qui organisent sa garantie que par l'ampleur de la jurisprudence de la Cour de Justice qui les interprète.
Il en résulte un ensemble complexe et dense, au sein duquel les données susceptibles d'intéresser la procédure pénale font l'objet d'un traitement pluriel et fluctuant.
Un traitement pluriel d'abord dans la mesure où le droit des données personnelles distingue non seulement de manière générale des dispositifs de droit commun[310] et des dispositifs sectoriels[311],

---

[307] *Supra*, §3 de la section précédente. Voir aussi les enseignements proches qui peuvent s'inférer du concept de sécuritisation, dont le second pilier serait l'effet de clôture des options politiques (« quand on sécuritise, on se prive – volontairement ou involontairement – de saisir les autres significations et les autres chaînes causales des phénomènes de sécurité ») et le troisième consisterait en une restriction drastique de la délibération publique (« on ne délibère plus car les termes du débat sont posés par la déclaration de danger sécuritaire), cf. Esprit de justice, « Qu'est-ce que la sécuritisation ? », *op. cit.*
[308] BACHMAIER WINTER, Lorena, « Criminal Investigation, Technological Development, and Digital Tools: Where Are We Heading? », *in* BACHMAIER WINTER Lorena, RUGGERI Stefano (eds), *Investigating and Preventing Crime in the Digital Era. New Safeguards, New Rights*, Springer Cham, 2022, p. 3-17.
[309] Au sein d'une littérature très abondante, voir notamment : TINIERE Romain, « Protection des données à caractère personnel », *in* PICOD Fabrice, RIZCALLAH Cecilia, VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne, Commentaire article par article*, Bruylant, 2ème éd., p. 211 et s ; DOUVILLE Thibault, *Droit des données à caractère personnel*, LGDJ, 2023.
[310] *Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* ; abrogée par le *Règlement (UE) 2016/679 général sur la protection des données du 27 avril 2016* (RGPD).
[311] Notamment : *directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications* ; abrogée par la *directive*

mais aussi les régimes et « types » de données numériques pénales. D'une part, les régimes des données numériques pénales *stricto sensu* incluent tant celles dont le caractère pénal tient à leur objet (ce sont celles relatives « aux condamnations pénales et aux infractions ou aux mesures de sûreté » [312]) que celles dont le caractère pénal tient aux autorités chargées de leur traitement et à la finalité de ce traitement (ce sont les traitement mis en œuvre par les autorités compétentes aux fins d'enquête, de poursuites ou d'exécution des condamnations)[313]. D'autre part, le régime des données numériques pénales *lato sensu* vise l'ensemble des autres données susceptibles d'intéresser l'enquête pénale (ce sont donc toutes les données collectées ou traitées par des tiers auxquelles les acteurs de la procédure – police, ministère public, juge des libertés et de la détention, juge d'instruction, et juridictions – sont susceptibles d'accéder pour les besoins de la recherche et de la manifestation de la vérité)[314].

Un traitement fluctuant ensuite, à raison du rythme de la succession des textes[315], favorisée notamment par l'enrichissement des traités, depuis l'entrée en vigueur du traité de Lisbonne, de bases juridiques dédiées[316], mais aussi par la rigueur de la jurisprudence de la Cour de justice qui n'hésite pas à invalider des dispositions clés[317] servant de fondement à la conservation (et conséquemment à l'accès à) de telles données ou à interpréter strictement les dérogations permises à ces fins par le droit commun.

169.- S'agissant des données numériques pénales *lato sensu*, c'est-à-dire celles qui ne sont pas pénales par nature parce que produites par les autorités compétentes en matière pénale (données relatives aux condamnations, infractions ou mesures de sûreté) ou traitées par elles à des fins de prévention et de détection des infractions pénales[318], mais qui deviennent pénales par « destination » du fait de leur intérêt potentiel pour la procédure pénale, autrement dit de données non produites mais consommées par le système pénal, elles ont pour trait caractéristique, déterminant de leur régime, de faire l'objet de recueil, stockage ou traitement par des tiers, tels que les opérateurs de communication électroniques : tiers vis-à-vis de la donnée (dans la mesure où la donnée concerne une personne physique ou morale, membre, abonnée, cliente ou adhérente) et vis-à-vis des autorités pénales.

2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « vie privée et communications électroniques »).

[312] Ainsi, le RGPD prévoit un régime particulier s'agissant de ces données, cf. art. 11 et 6§1 du règlement.

[313] C'est l'objet de la *directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données* (directive « police-justice »).

[314] Elles relèvent notamment des dérogations permises par la directive 2002/58 (directive « vie privée et communications électroniques », art. 15§1) et c'est donc en tant que dérogations qu'elles sont encadrées.

[315] Voir les notes précédentes : *directive 95/46/CE* abrogée et remplacée par le *RGPD* ; *directive 97/66/CE* abrogée et remplacée par la *directive 2002/58/CE*, elle-même modifiée par la *directive 2006/24/CE* finalement invalidée par la CJUE.

[316] Articles 16 TFUE et 39 TUE.

[317] *Directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE*, invalidée par CJUE (grande chambre), 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.* (affaires jointes C-293/12 et C-594/12).

[318] Ces dernières données se situent en réalité à la lisière des premières et des suivantes. Elles correspondent à celles qui résultent de ce que l'on peut qualifier (*infra*) d'accès direct (sans conservation préalable par un tiers) par l'autorité compétente, c'est-à-dire aux mesures d'enquête directement mises en œuvre par les enquêteurs qui leur permettent d'accéder directement aux données (voir par exemple le cas de « l'exploitation », selon le vocabulaire employé par les enquêteurs (*supra* première partie), d'un téléphone qui a donné lieu à un arrêt du 4 octobre 2024 de la Cour de justice (aff. C-548/21, *infra*, notamment paragraphe 200).

Sont donc ici en cause l'ensemble des données qui circulent grâce aux opérateurs ou fournisseurs de services électroniques. C'est pourquoi le cadre juridique applicable est déterminé à titre principal par la directive 2002/58/CE dite « vie privée et communications électroniques »[319], plus particulièrement son article 15§1 qui dispose que :

> « Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5[320] et 6[321], à l'article 8[322], paragraphes 1, 2, 3 et 4, et à l'article 9[323] de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive [95/46]. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit [de l'Union], y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne ».

Tel qu'interprété par la Cour de justice, ce cadre juridique repose de manière générale sur deux principes directeurs : premièrement, la garantie d'un niveau élevé de protection des données à caractère personnel et de la vie privée pour tous les services de communication électronique, quelle que soit la technologie utilisée [324] ; secondement, la confidentialité tant des communications électroniques que des données relatives au trafic y afférentes, laquelle implique l'interdiction faite en principe à toute personne autre que les utilisateurs de stocker, sans le consentement de ceux-ci, ces communications et données[325].

170.- Cet ensemble, dense et complexe, a produit un choc de grande magnitude sur les procédures répressives, de renseignement ou pénales nationales. Or, s'il en est ainsi, c'est peut-être en raison d'un renversement de perspective que paraît imposer le droit des données personnelles. Renversement qui tient à la configuration de ce droit nouveau vis-à-vis duquel la procédure pénale se pense comme dérogation, exception aux principes qui innervent ce droit.
Certes, une telle approche rejoint la relecture de la procédure pénale à l'aune des droits fondamentaux qu'entraînent sa constitutionnalisation et son internationalisation, tout particulièrement son européanisation. Pourtant, c'est bien un renversement qui semble s'observer ou, si l'on préfère, l'aboutissement du mouvement qui conduit à accorder aux droits

---

[319] CJUE (Grande chambre), 6 octobre 2020, *La Quadrature du Net e.a.*, affaires jointes C- C-511/18, C-512/18 et C-520/18, spécialement points 87-104. A noter que « lorsque les États membres mettent directement en œuvre des mesures dérogeant à la confidentialité des communications électroniques, *sans imposer des obligations de traitement* aux fournisseurs de services de telles communications, la protection des données des personnes concernées *relève non pas de la directive 2002/58, mais du seul droit national, sous réserve de l'application de la directive (UE) 2016/680* (…), *de telle sorte que les mesures en cause doivent respecter notamment le droit national de rang constitutionnel et les exigences de la CEDH* » (même arrêt, souligné par nous).
[320] Relatif à la « confidentialité des communications ».
[321] Qui concerne les « données relatives au trafic ».
[322] Relatif à la « présentation et restriction de l'identification de la ligne appelante et de la ligne connectée ».
[323] Qui concerne les « données de localisation autres que les données relatives au trafic ».
[324] CJUE (Grande chambre), 6 octobre 2020, *La Quadrature du Net e.a.*, affaires jointes C- C-511/18, C-512/18 et C-520/18, point 106, renvoyant à l'exposé des motifs de la proposition de directive à l'origine de la directive 2002/58.
[325] *Ibid.*, point 107.

fondamentaux sinon le premier rôle du moins celui de principe directeur[326], à la fois principe d'organisation et principe d'orientation des règles de procédure pénale en lieu et place de l'objectif de recherche des auteurs d'infractions (et donc de l'efficacité des actes de procédure[327]).
Autrement dit, ces droits ne sont plus seulement des limites ou conditions de la confection et du déploiement des règles procédurales mais le point de départ de leur conception.
De la sorte, l'objectif de recherche des auteurs d'infractions se trouve en quelque sorte relégué au rang de dérogation à la protection due aux droits fondamentaux (dont il prend pour ainsi dire la place).
Et s'il est vrai que c'est en réalité une conciliation qui est visée entre objectif de protection des (ou selon les cas certains) droits fondamentaux de quiconque (suspect ou non) d'une part et objectif de recherche des auteurs d'infractions pénales (lequel d'ailleurs protège aussi les droits des victimes d'infractions[328]) d'autre part, cette conciliation ne se pense pas exactement dans les mêmes termes selon que les droits ou garanties fondamentales sont conçus comme bornes à l'élucidation et à la prévention des infractions pénales lesquelles constituent l'objectif premier ou qu'à l'inverse ces finalités (d'élucidation et de prévention) sont pensées comme autant de dérogations à ces droits et garanties dont la préservation est le premier des devoirs de l'État.

171.- Naturellement, un tel renversement de perspective peut être contrarié ou complexifié selon le contenu donné au catalogue des droits fondamentaux appelés à constituer les « tables » de la procédure pénale. C'est ce qu'illustre parfaitement le rôle du « droit à la sécurité » qui tend à prendre la place du droit à la sûreté, à la faveur du retour de la raison d'État – si tant est qu'elle ait jamais disparu – sous les atours de la sécurité nationale, synonyme élargi de « sûreté » de l'État, et de la montée en puissance associée de la menace terroriste.
Aussi bien, il n'est pas exclu que ce renversement de perspective ne soit finalement qu'un leurre compte tenu de ce qu'il contient en son sein même les leviers de sa propre neutralisation. Pour le dire simplement, le piège de la raison d'État rebaptisée sécurité nationale, inscrite dans les textes et consacrée par les juges, pourrait finalement se refermer sur la construction nouvelle pourtant fondée sur une protection exigeante des libertés fondamentales.
Néanmoins, même dans ce cas, même neutralisé, le renversement de perspective ne peut être tout à fait écarté. C'est qu'il se manifeste au regard de l'enquête pénale par l'inscription de celle-ci dans un cadre plus large qui détermine ses conditions de possibilité.
En effet, le recueil ou la collecte de la preuve pénale n'est pas le point d'entrée, le point de départ du raisonnement mais en quelque sorte son point d'arrivée[329].
Il en résulte une centralité nouvelle de la problématique de la conservation des données aux fins de mise en œuvre des règles relatives à l'enquête pénale. Le droit des données détermine les conditions de disponibilité de celles-ci pour les besoins de l'enquête pénale.

---

[326] En ce sens, l'insertion récente (par la loi n° 2019-222) au sein de l'article préliminaire du CPP d'un nouvel alinéa consacré aux mesures portant atteinte à la vie privée (III, al. 6).
[327] VERGES E., « La procédure pénale technicienne (ou l'asphyxie procédurale) », *RSC* 2019, p. 667
[328] Dimension soulignée par la Cour au point 145 du premier arrêt *La Quadrature du Net* (6 octobre 2020) : « même les obligations positives des États membres susceptibles de découler, selon le cas, des articles 3, 4 et 7 de la Charte et portant, ainsi qu'il a été relevé aux points 126 et 128 du présent arrêt, sur la mise en place de règles permettant une lutte effective contre les infractions pénales ne sauraient avoir pour effet de justifier des ingérences aussi graves que celles que comporte une réglementation prévoyant une conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte de la quasi-totalité de la population sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi ».
[329] En ce sens, les premières conclusions de l'avocat Szpunar dans l'affaire C-470-21 : « Ainsi que l'a souligné la Cour, la conservation de données n'intervient qu'aux seules fins de rendre, le cas échéant, les données accessibles aux autorités nationales compétentes. Autrement dit, la conservation et l'accès à des données ne sauraient se concevoir isolément, alors même que le second est dépendant de la première », point 46.

172.- Ainsi, selon ce schéma, trois phases et non plus seulement deux organisent et déterminent la construction de la preuve pénale : d'abord, la phase de conservation qui commande la disponibilité des données potentiellement susceptibles de constituer des éléments de preuve, ensuite, la phase d'accès qui détermine leur mise à disposition et leur recueil, enfin, la phase d'exploitation qui conditionne leur utilisation ès-qualité (en tant que preuve).
Toutefois, une telle distinction s'efface lorsque l'accès aux données n'est plus indirect mais direct. Dans ce cas, en effet, la notion de « traitement » place sur le même plan collecte et conservation, qui d'ailleurs s'enchaînent plutôt dans cet ordre qu'inversement, si bien que le régime applicable concerne l'une et l'autre.
Chacune de ces trois phases – distinctes ou confondues – est configurée dans un premier temps à l'aune des principes du droit des données personnelles qui concrétise directement ou indirectement les garanties de la Charte des droits fondamentaux, puis, dans un second temps, au regard et dans la mesure de la conciliation entre ces principes et l'objectif de lutte contre la criminalité.
Ce dernier objectif de lutte contre la criminalité est ainsi triplement encadré et borné par le droit des données personnelles auquel s'amarrent d'autres droits, au premier rang desquels la protection de la vie privée, et qui assure en retour leur garantie. Par-là, le droit des données personnelles (et encore une fois avec lui d'autres droits fondamentaux qui le prolongent, le confortent ou le complètent) se constitue en contrainte structurelle des procédures pénales.
Dans cette perspective, la lutte contre la criminalité (équivalent européen de l'objectif à valeur constitutionnel de recherche des auteurs d'infractions pénales) ne justifie que certaines formes de conservation ou d'accès de certaines données selon certaines conditions.
173.- Certes la contrainte est variable.
Elle est forte s'agissant de la conservation au point de remettre en cause et le droit de l'Union lui-même et les (dés)équilibres sur lesquels s'étaient construits les droits nationaux. Toutefois, le bouleversement – bien réel – n'est pas sans soupape(s) qui à la fois constituent le gage de l'acceptabilité et de la praticabilité du renversement imposé et qui interrogent aussi quant à son sens et à son avenir. C'est ici que la (con)fusion de la sûreté et de la sécurité, ainsi que la montée en puissance de l'anti-terrorisme et du droit du renseignement évoqués plus haut mettent sous pression la reconfiguration en cours des procédures pénales.
La contrainte est également forte – peut-être plus encore qu'il n'y paraît et que ce qui s'observe concernant la conservation – en ce qui concerne l'accès, dans la mesure où elle atteint les articulations fondamentales internes des procédures pénales et n'affecte plus seulement celles-ci de l'extérieur, en amont.
Elle est en revanche plus lâche en ce qui concerne l'aval, l'exploitation ou, plus justement, le cœur de la procédure pénale : la construction de la preuve (les conditions de son admissibilité et de son appréciation). Pourtant, cette contrainte pourrait se resserrer dans la mesure où ce qui est pour partie en jeu est l'effectivité de la contrainte structurelle organisant les conditions de la licéité de la conservation des données personnelles et de leur accès.

Mais si avec ces trois étapes, ce sont trois ensembles de conditions de la confection de la donnée pénale en tant que preuve pénale qui se forment et impliquent des critères ou exigences distinctes à satisfaire, mobilisant des droits fondamentaux communs ou distincts, elles ont néanmoins en commun d'être tributaires des données qu'elles visent. On comprend alors que le préalable ou soubassement de la configuration nouvelle est déterminé par la compréhension et l'appréhension de l'objet ciblé : la donnée, ou plus exactement les données.
Dit autrement, une telle (re)configuration suppose une typologie des données qui toutes n'engagent pas les (mêmes) droits fondamentaux avec la même intensité.

1) Typologie des données : la formation d'un nouveau référentiel

174.- Cette typologie est d'abord déterminée par les textes mais elle est ensuite affinée par la jurisprudence qui, si elle est dans l'ensemble consolidée dans ses grandes articulations, laisse place aux doutes et, compte tenu des fortes critiques qu'elle suscite, à de possibles aménagements. La très grande variété des données et situations concrètes qu'elles saisissent invite ainsi à considérer que si les fondations (les divisions principales) sont posées, l'édifice reste encore à bâtir.
S'agissant des grandes distinctions, on peut discerner, moyennant un raffinement plus ou moins poussé, trois types ou catégories de données[330] selon l'ampleur de l'atteinte à la vie privée et au droit à la protection des données personnelles[331] dont elles sont porteuses et qui paraissent correspondre aux trois sphères de la vie privée que sont l'identité, la vie sociale et l'intimité physique (la voix, l'image) ou psychique (la pensée).

a) Classification tripartite

175.- Ainsi, le premier niveau de sensibilité de la donnée sur l'échelle de gravité de l'atteinte est constitué par l'identité telle qu'elle résulte des abonnements aux services de communications électroniques, d'attribution de noms de domaine sur l'internet et à certaines conditions de numérotation IP[332] et aux autres services de la société de l'information permettant la communication ou le stockage de données. S'y trouvent regroupées les données d'état civil mais aussi les données contractuelles ou de facturation et à certaines conditions les adresses IP[333]. Ainsi, le règlement *e-evidence* de 2023 vise au sein de la catégorie des « données relatives aux abonnés »[334] : « toutes données détenues par un fournisseur de services concernant l'abonnement à ses services », relatives d'une part à « l'identité d'un abonné ou d'un client, telles que le nom, la date de naissance, l'adresse postale ou géographique, les données de facturation et de paiement, le numéro de téléphone ou l'adresse électronique fournis » et d'autre part, au « type de service et sa durée, y compris les données techniques et les données identifiant les mesures techniques connexes ou les interfaces utilisées ou fournies par l'abonné ou le client au moment du premier enregistrement ou de la première activation, et les données relatives à la validation de l'utilisation du service, à l'exclusion des mots de passe ou autres moyens d'authentification utilisés à la place d'un mot de passe qui sont fournis par un utilisateur ou créés à la demande d'un utilisateur ».
176.- Le second échelon est constitué par la vie sociale *lato sensu* représentée numériquement par les activités, les interactions et les déplacements de la personne : ce sont les « données relatives au trafic ». Le règlement *e-evidence* les définit comme « les données relatives à la fourniture d'un service proposé par un fournisseur de services qui servent à fournir des informations contextuelles ou supplémentaires sur ce service et qui sont générées ou traitées par un système d'information du fournisseur de services, tels que la source et la destination d'un message ou un autre type d'interaction, l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, et d'autres

[330] Il s'agit de la typologie qui se dégage déjà dans la Convention de Budapest du Conseil de l'Europe (cf. art. 18.3) et que reprend et affine le règlement *e-evidence* de l'Union européenne (art. 3). Pour une présentation des typologies des autres instruments de l'Union, MORNET Alice, « Vers un nouveau droit commun de la preuve numérique », *Lexbase*, 8 mars 2023.
[331] Ces deux droits se recoupent pour partie, le second est un élément du premier et en assure la protection, mais le droit à la protection des données personnelles présente aussi une autonomie qui ne doit pas être ignorée : toutes les données personnelles bénéficient de sa protection quel(le) que soit leur (absence de) lien avec la vie privée.
[332] Voir le cas particulier de ces données, *infra*.
[333] *Ibid*.
[334] Art. 3, 9) du règlement.

métadonnées de communications électroniques et des données, autres que les données relatives aux abonnés, relatives au début et à la fin d'une session d'accès d'un utilisateur à un service, telles que la date et l'heure d'utilisation, la connexion et la déconnexion du service »[335]. Sont ici visées les métadonnées, parfois désignées par l'expression de « données de connexion », dont l'appréciation de la sensibilité s'est modifiée à mesure qu'était prise la mesure du type d'informations – loin d'être seulement techniques comme le laisse croire le terme de métadonnées – qui pouvait en résulter.

177.- Enfin, le troisième niveau concerne le cœur de la vie privée et les données les plus sensibles. Il s'agit des « données relatives au contenu », catégorie définie comme visant « toutes données dans un format numérique telles que du texte, de la voix, des vidéos, des images et du son, autres que les données relatives aux abonnés ou les données relatives au trafic »[336].

b) Distinctions supplémentaires

178.- Se dessine ainsi une première échelle de sensibilité des données qui permet de concevoir les conditions de leur conservation, accès et exploitation selon la gravité de l'atteinte que ces actions sont susceptibles d'engendrer.

Cette première échelle est encore imparfaite. Des gradations internes sont nécessaires afin de tenir compte du facteur temporel ou de la protection renforcée devant être reconnue aux données spécialement qualifiées de « sensibles »[337]. De même, des recoupements entre catégories peuvent se faire jour. Tel est le cas lorsqu'un « même » type de donnée peut relever d'une catégorie ou d'une autre, comme le montre l'exemple des adresses IP.

179.- *L'exemple des adresses IP*

Les frontières des catégories doivent en effet encore être affinées, ainsi que l'illustre le cas des adresses IP. Incluses au sein des données d'identité, elles constituent pourtant le point de bascule ou de jonction entre l'identité et la localisation ; elles témoignent combien la sensibilité de la donnée s'apprécie en soi, de manière en quelque sorte statique mais aussi de manière dynamique, au regard des croisements dont elle peut être l'objet. C'est précisément la place de ces données particulières (et en conséquence leur régime) qui est au cœur d'une affaire[338] dont l'importance est marquée par les étapes de la procédure dont elle a fait l'objet devant la Cour de justice. Alors qu'elle était déjà soumise à la formation de la grande chambre, cette dernière a décidé de la renvoyer à sa formation la plus solennelle : l'assemblée plénière, laquelle a décidé la réouverture de la phase orale de la procédure et invité les intéressés visés à l'article 23 du statut de la Cour de justice de l'Union européenne – le Contrôleur européen à la protection des données (CEPD) et l'Agence de l'Union européenne pour la cybersécurité (ENISA) – à participer à une nouvelle audience. A la faveur de cette procédure extraordinaire, qui donne lieu à un nouvel arrêt *La Quadrature du Net*[339], l'épisode II d'une saga qui pourrait être longue, deux jeux de conclusions présentées par l'avocat général Szpunar[340] permettent d'observer les

---

[335] Art. 3, 11) du règlement.

[336] Art. 3, 12).

[337] Voir par exemple, le point 181 de l'arrêt de la Cour de justice dans l'affaire C-470/21 (*La Quadrature du Net*) qui réserve spécialement le cas de ces données dans l'hypothèse ultra dérogatoire de l'analyse automatisée des données relatives au trafic et des données de localisation.

[338] Question préjudicielle introduite par le Conseil d'État concernant les instruments de lutte contre les infractions aux droits de propriété intellectuelle commises exclusivement en ligne, en particulier la procédure devant la Hadopi, Aff. C-470/21 : *La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs, Franciliens.net, French Data Network contre Premier ministre, ministère de la Culture*.

[339] CJUE (Assemblée plénière), 30 avril 2024, *La Quadrature du Net e.a.*, aff. C-470/21 (Données personnelles et lutte contre la contrefaçon).

[340] Le 27 octobre 2022 devant la Grande Chambre et le 28 septembre 2023 devant l'Assemblée Plénière.

évolutions – des premières conclusions aux secondes – du contexte et des positions des acteurs, y compris celle de l'avocat général lui-même.
La place des adresses IP est emblématique de l'évolution des textes et de l'affinement progressif de la compréhension par le législateur européen des besoins et des défis en la matière. En effet si, dans la directive 2002/58, les adresses IP ne sont visées que dans le préambule, là où est prévue « l'obligation d'effacer ou de rendre anonymes les données relatives au trafic », tandis que la classification proposée par le texte distingue (sans mentionner les adresses IP) les communications, les données relatives au trafic et les données de localisation autres que les données relatives au trafic, dans le règlement 2023/1543, les adresses IP sont spécialement visées au sein des « données demandées à la seule fin d'identifier l'utilisateur », catégorie nouvelle directement issue de la jurisprudence, intermédiaire entre les données relatives aux abonnés et les données relatives au trafic, auxquelles s'ajoutent les données relatives au contenu. Un palier supplémentaire est construit entre les données d'identité et les données de trafic : les données d'identification. Pour le surplus cependant, comme le souligne le considérant 32 du règlement, outre que « conformément à l'acquis de l'Union, les adresses IP doivent être considérées comme des données à caractère personnel et bénéficier de la protection complète prévue par l'acquis de l'Union en matière de protection des données (…) dans certains cas, les adresses IP peuvent être considérées comme des données relatives au trafic ». Ainsi, « [l]orsque des adresses IP, des numéros d'accès et des informations connexes ne sont pas demandés à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique, ils sont en général demandés pour obtenir des informations qui portent davantage atteinte à la vie privée, telles que les contacts ou la localisation de l'utilisateur. À ce titre, ils pourraient être utilisés pour dessiner un profil complet de la personne concernée, mais en même temps ils peuvent être traités et analysés plus facilement que les données relatives au contenu, étant donné qu'ils sont présentés dans un format standardisé et structuré. Il est dès lors indispensable que, dans ce cas, les adresses IP, les numéros d'accès et les informations connexes qui ne sont pas demandés à la seule fin d'identifier l'utilisateur dans le cadre d'une enquête pénale spécifique soient traités comme des données relatives au trafic et que la demande de telles données soit soumise au même régime que la demande de données relatives au contenu »[341].
Autrement dit, la donnée ne se conçoit pas seulement au regard de son contenu mais aussi au regard de son usage potentiel. C'est donc dire que la classification n'est pas figée mais appelée à suivre les évolutions des usages.
Aussi bien, dès l'arrêt *La Quadrature du Net (I)*, la Cour avait relevé que les adresses IP « sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'internet est effectuée. Dès lors, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, cette catégorie de données présente un degré de sensibilité moindre que les autres données relatives au trafic »[342].
Mais, « dès lors que les adresses IP peuvent être utilisées pour effectuer, notamment, un traçage exhaustif du parcours de navigation d'un internaute et, par la suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier et de tirer des conclusions précises sur la vie privée de l'utilisateur »[343].

[341] Considérant 33.
[342] CJUE (grande chambre), 6 octobre 2020, *La Quadrature du Net*, aff. jtes C-511/18, C-512/18, C-520/18, point 152.
[343] Premières conclusions du 22 septembre 2022 dans l'affaire concernant la procédure de la HADOPI, points 83 et s.

Dans l'affaire concernant la procédure Hadopi, c'est la mise en relation des données civiles avec les adresses IP qui est en jeu[344] et a conduit l'avocat général à proposer un « aménagement » de la jurisprudence de la Cour quant au régime de conservation de ces données (voir *infra*). Sans toujours le suivre, l'Assemblée plénière de la Cour de justice propose néanmoins une évolution sensible qui, sans remettre en cause les précédents, répond aux attentes et craintes des gouvernements et des enquêteurs qu'ils avaient suscitées quitte à décevoir les associations de défense des libertés publiques inquiètes de tout infléchissement ou concession en faveur d'arguments sécuritaires. Aussi bien, sur le terrain de la classification des données, l'arrêt du 30 avril 2024 conforte et donc confirme l'ambivalence des adresses IP. En revanche, sur le terrain des régimes d'accès, en apportant des éclaircissements attendus, elle propose selon les points de vue, un simple approfondissement qui consolide la construction ébauchée ou une réorientation moins-disante qui la fragilise[345].

180.- *La variable du facteur temporel*

Par ailleurs, l'échelle constituée de ces trois (identité, trafic, contenu) ou quatre niveaux (identité, identification, trafic, contenu) doit encore être affinée par la prise en compte du caractère passé ou à venir de la donnée visée. Ce caractère n'est naturellement susceptible de concerner que les deux catégories les plus sensibles, soit les données de trafic et les données de contenu, qui, toutes deux, à la différence des données relatives aux abonnés, peuvent faire l'objet d'un recueil en temps réel et ainsi viser les données à venir, au moment de leur « naissance » ou à l'occasion de leur circulation future.

C'est donc à partir et en contemplation de cette échelle distinguant six paliers – les données relatives aux abonnés, les données relatives aux adresses IP aux seules fins d'identification, les données de trafic passées (stockées), les données de trafic à venir, les données de contenu passées (stockées) et les données de contenu à venir – que se construisent les trois étapes de la circulation des données à des fins pénales.

2) Disponibilité des données : le préalable de la conservation

181.- Sans préjudice des hypothèses d'accès en temps réel, c'est la conservation qui commande la disponibilité de la donnée. Cette étape est donc fondamentale tant elle conditionne l'existence et le volume du « réservoir » de preuves que constituent les données stockées et en circulation. Dans le même ordre d'idées mais d'un autre point de vue, elle correspond en quelque sorte à la phase de surveillance pré-pénale ou encore à une sorte de mécanisme de pré-constitution (constitution *a priori*) de preuves pénales[346]. C'est dire l'importance des conditions de conservation des données qui déterminent la disponibilité des données dans le temps au-delà de l'instant de leur production ou circulation.

182.- Les données sont, en effet, susceptibles de constituer des ressources pour la procédure pénale soit parce qu'il est possible de les collecter au moment de leur production ou de leur circulation, soit parce qu'elles ont été stockées, conservées par la ou les personnes concernées ou par un tiers.

---

[344] Puisque « les données d'identité civile et les adresses IP étant, indépendamment les unes des autres, sans intérêt pour les autorités nationales dès lors que ni l'identité civile ni l'adresse IP en soi ne peuvent donner d'informations sur les activités des personnes physiques en ligne lorsqu'elles ne sont pas mises en relation », point 43 des premières conclusions du 22 septembre 2022.

[345] *Infra*, paragraphe 206, 223-244-225.

[346] L'apport des technologies à des mécanismes de « pré-constitution » de la preuve pénale s'observe dans d'autres champs tels que celui notamment des crimes internationaux, https://icc-cpi.int/sites/default/files/2023-06/ICC-Eurojust-CSO-Guidelines-Fra.pdf p. 34 et s.

Cette conservation peut être imposée. Elle peut aussi être volontaire et être le fruit d'une simple faculté. Dans le premier cas, elle résulte d'obligations de conservation adressées à certains tiers qui permettent et assurent la circulation des données, tels que les opérateurs de communication électronique ou les banques.
Dans le second cas, la conservation résulte soit de la conduite, délibérée ou non de tout un chacun vis-à-vis des données qui le concernent, soit de la politique commerciale des tiers qui en assurent le stockage ou la circulation. Parce qu'elles échappent ainsi à ceux qu'elles concernent, les données ne peuvent être conservées soit sur le fondement d'obligations soit sur le fondement de facultés qu'à certaines conditions destinées à préserver spécialement les droits à la protection des données personnelles, de la vie privée, de la liberté d'expression, sans oublier les droits de la défense et à un procès équitable.
183.- Comme rappelé plus haut, deux principes directeurs généraux s'imposent : la garantie d'un niveau élevé de protection des données à caractère personnel et de la vie privée pour tous les services de communications électroniques, quelle que soit la technologie utilisée[347], d'une part, et la confidentialité tant des communications électroniques que des données relatives au trafic y afférentes, laquelle implique l'interdiction faite en principe à toute personne autre que les utilisateurs de stocker, sans le consentement de ceux-ci, ces communications et données[348], d'autre part. Il en découle notamment que la conservation des données de trafic ou de localisation constitue, « par elle-même »[349], une dérogation à cette interdiction ainsi qu'une ingérence dans les droits au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, indépendamment du caractère éventuellement sensible de ces données, d'éventuels inconvénients subis par les intéressés en raison de cette ingérence ou de l'utilisation qui pourrait en être faite.
De l'ensemble textuel et jurisprudentiel européen résulte un encadrement apparemment serré de la conservation obligatoire *(a)* qui tranche avec un encadrement semble-t-il plus lâche de la conservation facultative *(b)*, laquelle ne doit pas être ignorée puisqu'elle constitue comme la première un réservoir de données pénales.

a) Conditions de licéité de la conservation obligatoire

(a1) Classification des modes de conservation

184.- La construction des régimes de conservation obligatoire repose sur une classification sophistiquée des modes de conservation, conçue en fonction des finalités poursuivies, lesquelles, limitativement énumérées par l'article 15§1 de la directive 2002/58, visent la sauvegarde de la sécurité nationale, la lutte contre la criminalité et la sauvegarde de la sécurité publique, les deux dernières se subdivisant à leur tour selon que la criminalité considérée ou les menaces à la sécurité publique sont ou non graves.
Ainsi se distinguent la conservation généralisée et indifférenciée, la conservation ciblée, la conservation rapide auxquelles s'ajoute le recueil ou transfert en temps réel susceptibles d'en constituer des variantes (l'opérateur ne conserve pas lui-même les données mais les recueille ou les transfère pour le compte/aux services de renseignement ou compétents en matière pénale).

[347] CJUE (Grande chambre), 6 octobre 2020, *La Quadrature du Net e.a.*, affaires jointes C- C-511/18, C-512/18 et C-520/18, point 106, renvoyant à l'exposé des motifs de la proposition de directive à l'origine de la directive 2002/58.
[348] *Ibid.*, point 107.
[349] *Ibid.*, point 115.

185.- Avant d'exposer en détail ces différents modes de conservation et les conditions de leur licéité au regard du droit de l'Union, il convient de souligner un enjeu spécifique pour les procédures pénales nationales, à savoir l'incompatibilité absolue[350] avec le droit de l'Union des dispositifs nationaux de conservation généralisée et indifférenciée (c'est-à-dire de tous les utilisateurs de services de communications électroniques et partant de la quasi-totalité de la population) des données de trafic à des fins de lutte contre la criminalité même grave.
C'est à cet égard que la jurisprudence de la Cour subit les plus vives critiques et sans doute ce qui constitue le point de bascule et l'axe à partir duquel se dessine la reconfiguration partielle des procédures pénales nationales.
186.- Aussi n'est-il pas inutile de mettre en exergue les arguments saillants du raisonnement qui conduisent la Cour à adopter une position aussi (apparemment) radicale.

> « [C]ompte tenu du *caractère sensible* des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée. Ainsi, et compte tenu, d'une part, des *effets dissuasifs sur l'exercice des droits fondamentaux* consacrés aux articles 7 et 11 de la Charte (…) que la conservation de ces données est susceptible d'entraîner et, d'autre part, de la gravité de l'ingérence que comporte une telle conservation, il importe, dans une société démocratique, que celle-ci soit (…) *l'exception et non la règle* et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose *même à l'égard des objectifs de lutte contre la criminalité grave* et de prévention des menaces graves contre la sécurité publique ainsi que de l'importance qu'il convient de leur reconnaître »[351].
>
> « [U]ne réglementation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation *couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi*. Une telle réglementation (…) concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, *sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales*. Elle s'applique donc *même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec cet objectif* de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique »[352].
>
> « En particulier, (…) une telle réglementation n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un *cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave*, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave »[353].
>
> « Or, *même les obligations positives* des États membres susceptibles de découler, selon le cas, des articles 3, 4 et 7 de la Charte et portant (…) sur la mise en place

[350] « [L]a conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique », CJUE, 6 octobre 2020, *La Quadrature du Net*, point 141.
[351] CJUE, 6 octobre 2020, *La Quadrature du Net*, point 142.
[352] CJUE, 6 octobre 2020, *La Quadrature du Net*, point 143.
[353] CJUE, 6 octobre 2020, *La Quadrature du Net*, point 144.

de règles permettant une lutte effective contre les infractions pénales *ne sauraient avoir pour effet de justifier des ingérences aussi graves* que celles que comporte une réglementation prévoyant une conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte de la quasi-totalité de la population sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi »[354].

(a2) Possibilités et limites de la conservation généralisée et indifférenciée

187.- Le premier mode de conservation – la conservation généralisée et indifférenciée – est *a priori* et par principe exclu lorsqu'il implique une surveillance automatique et sans limite de sorte qu'il est nécessairement disproportionné, et ce de manière telle que c'est dans leur substance même que les droits protégés et garantis par la Charte des droits fondamentaux pourraient être atteints.
La question se pose néanmoins de savoir s'il convient de réserver l'hypothèse, semble-t-il illustrée par l'affaire *EncroChat*[355], d'une conservation généralisée et indifférenciée des données de l'ensemble des utilisateurs d'un réseau de communications par nature illicite voire aussi par destination dès lors qu'il est exclusivement dédié à la commission d'infractions.
En tout état de cause, un tel mode de conservation peut être envisageable à certaines conditions et en fonction du type de données concernées.

188.- Les données de trafic et de localisation
Lorsqu'elle concerne l'ensemble des données de connexion (sans distinction) de tous les abonnés et utilisateurs (sans distinction) concernant tous les moyens de communication électronique (sans distinction), elle constitue naturellement un mode de conservation très attentatoire. Le plus attentatoire qui, semble-t-il, puisse être conçu sans franchir le Rubicon, à l'instant évoqué, de l'atteinte à la substance même des droits ; si attentatoire qu'il est réservé au cas supposé exceptionnel de sauvegarde de la sécurité nationale, comprise comme « l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société [y inclus] la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme »[356].
Elle n'est licite qu'à quatre conditions : une condition de fond qui tient à la caractérisation sur la base de circonstances suffisamment concrètes d'une menace grave, réelle, actuelle et prévisible pour la sécurité nationale ; une condition de temps qui impose que la conservation soit temporellement limitée au strict nécessaire (la période pouvant être renouvelée en cas de persistance de la menace) ; la prévision de limitations et garanties strictes permettant de protéger les données contre les risques d'abus ; une condition de procédure qui requiert un contrôle effectif soit par une juridiction soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant et visant à vérifier les conditions qui précèdent[357].

---

[354] CJUE, 6 octobre 2020, *La Quadrature du Net*, point 145.
[355] Pour une présentation complète des faits et des caractères du dispositif technique, voir CEDH, *A.L. et E.J. c. France*, précité. Voir aussi, également à propos d'*EncroChat*, les conclusions de l'avocat général Capeta (précitées, en particulier le point 11) dans l'affaire portée devant la CJUE là où sont présentées les interrogations de la juridiction de renvoi à cet égard.
[356] CJUE, 6 octobre 2020, *La Quadrature du Net*, point 135.
[357] Cf. pour toutes, le dispositif de l'arrêt du 6 octobre 2020, *La Quadrature du Net*.

En droit français, cette hypothèse conduit à la publication périodique d'un décret[358] portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories[359] de données de connexion[360]. Elle est, selon la chambre criminelle de la Cour de cassation, également couverte par l'exposition de la France « depuis décembre 1994, à une menace grave et réelle, actuelle ou prévisible à la sécurité nationale [autorisant à] conserver de façon généralisée et indifférenciée les données de trafic et de localisation, aux fins de la recherche, de la constatation et de la poursuite des infractions portant atteinte aux intérêts fondamentaux de la Nation et des actes de terrorisme, incriminés aux articles 410-1 à 422-7 du code pénal »[361].

189.- Les seules adresses IP attribuées à la source

Lorsque la conservation généralisée ou indifférenciée concerne les seules adresses IP attribuées à la source d'une connexion[362], compte tenu de la gravité de l'ingérence dans les droits fondamentaux qu'elle implique, elle n'est licite qu'aux fins de lutte contre la criminalité grave et la prévention de menaces graves contre la sécurité publique (et *a fortiori* de la sauvegarde de la sécurité nationale) et sous réserve d'être temporellement limitée au strict nécessaire et à des conditions et garanties strictes quant à l'exploitation des données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées[363]. Tel était l'état de la jurisprudence fixé avec le premier arrêt « La Quadrature du Net » en 2020[364]. C'était sans compter sur le deuxième, rendu le 30 avril 2024 à propos du dispositif français de la HADOPI[365] qui affine et diversifie les hypothèses. L'Assemblée plénière de la Cour indique en effet que le précédent de 2020 n'épuise pas la question de la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source. Si en dépit « du constat de moindre sensibilité des adresses IP servant exclusivement à identifier l'utilisateur d'un service de communications électroniques », elle considérait que leur conservation généralisée et indifférenciée constituait une ingérence grave limitant en conséquence les motifs envisageables à la lutte contre la criminalité grave, la prévention de menaces graves à la sécurité publique ou la sauvegarde de la sécurité nationale, c'était en raison du risque d'un « traçage exhaustif du parcours de navigation d'un internaute » susceptible de permettre l'établissement d'un « profil détaillé de ce dernier »[366]. Partant, la voie est libre pour dire sans se dédire que « toute conservation généralisée et indifférenciée d'un ensemble, le cas échéant vaste, d'adresses IP

---

[358] En dernier lieu : *Décret n° 2024-901 du 7 octobre 2024 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion*.

[359] Celles énumérées au V de l'article R. 10-13 du code des postes et des communications électroniques et à l'article 6 du décret n°2021-1362 du 20 octobre 2021.

[360] CJUE, 6 octobre 2020, *La Quadrature du Net*, point 135.

[361] Crim., 12 juillet 2022, n° 21-83.820, §9.

[362] Selon la Cour de justice, « les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic » CJUE, 6 octobre 2020, *La Quadrature du Net*, point 152. Sur le recours aux adresses IP afin de procéder au traçage exhaustif du parcours de navigation d'un internaute et de son activité en ligne, voir le point suivant (153) de ce même arrêt et la décision précitée de la Cour concernant l'HADOPI (30 avril 2024, C-470/21).

[363] CJUE, 6 octobre 2020, *La Quadrature du Net*, point 156.

[364] *Ibid*.

[365] CJUE (Assemblée plénière), 30 avril 2024, précité ; *supra*, paragraphe 179.

[366] *Ibid*. points 77-78.

statiques et dynamiques utilisées par une personne dans une période donnée ne constitue pas nécessairement une ingérence grave dans les droits fondamentaux garantis aux articles 7, 8 et 11 de la Charte »[367]. En particulier, une obligation de conservation généralisée et indifférenciée peut être imposée à des fins de lutte contre la criminalité en général[368] si les modalités de cette conservation sont de nature à garantir qu'est exclue toute combinaison desdites adresses IP avec d'autres données conservées permettant de tirer des conclusions précises sur la vie privée, ce qui impliquerait une ingérence grave[369], c'est-à-dire à garantir une séparation étanche entre les données. Le tout étant sans préjudice de l'exigence commune d'une conservation limitée dans le temps au strict nécessaire, prévue par des règles claires et précises en fixant les conditions matérielles et procédurales et assurant que les personnes concernées disposent de garanties effectives contre les risques d'abus ainsi que contre tout accès et toute utilisation illicite.

190.- Les seules données d'identité

Lorsqu'en revanche, la conservation généralisée et indifférenciée concerne les seules données d'identité, dans la mesure où l'atteinte qui en résulte pour les droits à la protection de la vie privée et des données personnelles ne saurait en principe être qualifiée de grave, elle peut être prévue sans délai particulier pour les besoins de la lutte contre la criminalité en général et la sauvegarde de la sécurité publique en général[370] (et *a fortiori* de la sauvegarde de la sécurité nationale).

(a3) Alternatives à la conservation généralisée et indifférenciée : l'enjeu des données de trafic et de localisation

191.- Conservation ciblée

Le second mode est la conservation dite ciblée, c'est-à-dire limitée à certaines catégories de personnes ou à certains lieux, délimitées sur la base d'éléments objectifs et non discriminatoires pour une période temporellement limitée au strict nécessaire, mais renouvelable. Elle peut être licitement prévue aux fins sauvegarde de la sécurité nationale, de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique.

Ce mode de conservation a fait l'objet de vives critiques compte tenu de son incapacité à compenser l'interdit de la conservation généralisée et indifférenciée des données de trafic à des fins de lutte contre la criminalité même grave, considérée indispensable à la poursuite des infractions pénales, à tout le moins les plus graves[371] ; compte tenu également des risques discriminatoires dont elle est porteuse. Elle a pourtant été mobilisée par le législateur belge selon des modalités telles que l'entièreté du territoire national se trouve finalement couvert, ce qui était l'objectif précisément recherché par le législateur national[372] mais sans doute pas par la Cour de justice.

---

[367] *Ibid*. point 79.
[368] *Ibid*. point 92.
[369] *Ibid*. points 83-84.
[370] CJUE, 6 octobre 2020, *La Quadrature du Net*, points 158 et 159.
[371] Voir notamment, la position – elle-même critiquée – du Conseil d'État à ce propos : Assemblée, 21 avril 2021, requête n°393099, §54.
[372] FLUMIAN Baptiste, FRANSSEN Vanessa, « Le nouveau cadre légal belge en matière de conservation des données de communications électroniques : "*Old Wine in New Bottles*" pour les autorités judiciaires ? », *in* FRANSSEN Vanessa, MASSET Adrien (dir.), *Le droit pénal et la procédure pénale en constante évolution*, Anthemis, 2023, vol. 217, p. 315-360.

192.- Conservation rapide

Le troisième mode de conservation, dite rapide, est un « emprunt » à la Convention de Budapest du Conseil de l'Europe. Ce mode de conservation constitue la « soupape » ou le compromis rendu nécessaire par l'incompatibilité de la conservation généralisée et indifférenciée des données de trafic et de localisation à des fins de lutte contre la criminalité, fût-elle grave.

En effet, la conservation rapide permet, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation des données relatives au trafic et des données de localisation dont ils disposent, c'est-à-dire celles qui sont stockées ou traitées par eux conformément aux articles 5, 6 et 9 de la directive ou aux dispositions nationales prises en vertu de l'article 15§1 de la directive. Partant, sont susceptibles de faire l'objet d'une telle conservation non seulement les données volontairement stockées et traitées à des fins commerciales mais aussi les données obligatoirement stockées pour des raisons relevant des objectifs exhaustivement énumérés par l'article 15 de la directive. Sont donc incluses les données conservées aux fins de sauvegarde de la sécurité nationale, c'est-à-dire celles qui, sous réserve d'une menace grave et avérée, et sous les conditions rappelées plus haut, peuvent faire l'objet d'une conservation généralisée et indifférenciée.

C'est pourquoi si la hiérarchie des finalités ne peut être inversée à la faveur d'un accès à des fins qui ne permettent pas la conservation des données[373], en revanche la variété et la combinaison des types de conservation peut permettre *in fine* qu'un tel accès soit en réalité envisageable.

193.- Ainsi, la distinction entre les notions et donc les régimes de la conservation, d'une part, et de l'accès, d'autre part, permet tout à la fois de mieux encadrer et révéler les enjeux distincts que posent et l'une et l'autre. Toutefois, et de manière contre-intuitive, certains types de conservation masquent finalement des cas d'accès *a priori* exclus. Plus exactement, par le truchement de la conservation rapide des modes d'accès peuvent être transformés en mode de conservation de sorte que des données qui, parce qu'elles ont été conservées – de manière généralisée et indifférenciée – sur le fondement exclusif de la sauvegarde de la sécurité nationale ne sauraient donner lieu à un accès sur un fondement hiérarchiquement inférieur au sein de l'échelle des objectifs légitimes, tel que la lutte contre la criminalité grave, peuvent tout à fait faire l'objet d'une conservation rapide à cette fin et partant – certes sous réserve des conditions qui lui propres et s'ajoutent dans un deuxième temps à celles distinctes de la conservation rapide – d'un accès à cette même fin.

En ce sens, la conservation rapide peut tenir lieu de chaînon manquant entre la conservation préventive et la conservation répressive et, partant, permettre que le réservoir de données pénales soit alimenté par la conservation généralisée et indifférenciée dont la finalité ne peut pourtant être que la sauvegarde de la sécurité nationale à l'exclusion de la lutte contre la criminalité même grave.

---

[373] CJUE, Grande chambre, 5 avril 2022, *Commissioner of An Garda Síochána*, point 100 : « les données relatives au trafic et les données de localisation ne peuvent pas faire l'objet d'une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave et, partant, un accès à ces données ne saurait être justifié à ces mêmes fins. Or, lorsque ces données ont exceptionnellement été conservées de manière généralisée et indifférenciée à des fins de sauvegarde de la sécurité nationale contre une menace qui s'avère réelle et actuelle ou prévisible (…) les autorités nationales compétentes en matière d'enquêtes pénales ne sauraient accéder auxdites données dans le cadre de poursuites pénales, sous peine de priver de tout effet utile l'interdiction de procéder à une telle conservation aux fins de la lutte contre la criminalité grave ».

194.- Analyse automatisée et recueil en temps réel (pour le compte ou par les services de renseignement)

Catégories séparées qui ne correspondent ni à la conservation ni à l'accès mais transcendent la distinction en permettant aux services de renseignement de « se brancher » directement sur les réseaux, l'analyse automatisée et le recueil en temps réel[374] sont, tout en tenant compte de leurs spécificités, soumis aux mêmes conditions que celles qui ont été examinées à propos de la conservation généralisée et indifférenciée des données de trafic et de localisation.

195.- S'agissant de ce type de données, l'analyse automatisée, parce qu'elle couvre de manière généralisée et indifférenciée les données des personnes faisant usage des moyens de communications électroniques et est susceptible de révéler la nature des informations consultées en ligne, n'est compatible avec le droit de l'Union qu'en cas de menace grave, réelle, actuelle ou prévisible, pendant une période strictement limitée, et pourvu que la décision l'autorisant puisse faire l'objet d'un contrôle effectif soit par une juridiction soit par une autorité administrative indépendante, dont la décision est contraignante et vise à vérifier l'existence de la menace ainsi que le respect des conditions et garanties prévues, parmi lesquelles l'exigence de spécificité, de fiabilité et de non-discrimination des modèles et critères du traitement, l'exigence de réexamen individuel non automatisé avant l'adoption de toute mesure individuelle préjudiciable (telle le recueil en temps réel) et l'exigence de réexamen régulier des critères et modèles de traitement.

196.- Quant au recueil en temps réel des données de trafic et localisation, dans la mesure où il est davantage intrusif que le recueil en temps différé car s'agissant des données de localisation il permet une « surveillance quasiment parfaite »[375] et constitue une ingérence aggravée lorsqu'il s'étend aux données de trafic, si l'objectif de prévention du terrorisme peut le justifier, ce n'est qu'à l'égard des « personnes pour lesquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme » ; au-delà, seul un accès différé est envisageable, et ce dans des situations particulières, telles que des activités de terrorisme, et lorsqu'il existe des éléments objectifs permettant de considérer que les données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre le terrorisme[376]. En outre, la décision autorisant ces recueils est soumise aux conditions précitées tenant à la prévision légale de critères objectifs et non-discriminatoires et à l'existence d'un contrôle préalable effectif[377] (sous réserve de l'urgence, qui permet un contrôle *a posteriori* dans de brefs délais).

b) Conditions de licéité de la conservation facultative

197.- Selon la Cour, en adoptant la directive 2002/58 « Vie privée et communications électroniques », le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes

---

[374] Examinés au regard du droit français du renseignement anti-terroriste : art. L851-2 à L-851-4 CSI dans leur version issue de la *loi n° 2015-912 relative au renseignement* ; rédaction remaniée à la faveur notamment de la décision *La Quadrature du Net* par la loi 2021-998 du 30 juillet 2021 relative à la *prévention d'actes de terrorisme et au renseignement*.

[375] CJUE, 6 octobre 2020, *La Quadrature du Net*, précité, point 187.

[376] CJUE, 6 octobre 2020, *La Quadrature du Net*, précité, point 188.

[377] CJUE, 6 octobre 2020, *La Quadrature du Net*, précité, point 189.

restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement[378].
S'agissant, en particulier, du traitement et du stockage des données relatives au trafic par les fournisseurs de services de communications électroniques, un tel traitement n'est autorisé que dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation de ceux-ci et à la fourniture de services à valeur ajoutée. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit qu'elles ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés[379].
Ces considérations délimitent les contours et conditions de la conservation facultative – c'est-à-dire non imposée par les pouvoirs publics et volontairement mise en œuvre par les opérateurs – des données, lesquelles sont, le cas échéant, susceptibles de faire l'objet d'une conservation rapide aux fins de lutte contre la criminalité grave s'agissant des données de trafic et localisation et aux fins de lutte contre la criminalité en général s'agissant des données d'identité (*supra*).

3) Accessibilité des données : les possibilités d'accès

198.- Le réservoir des données abondé, son contenu n'est accessible qu'à certaines conditions distinctes mais supposées conçues en cohérence avec celles qui déterminent la conservation. En effet, la conservation des données et l'accès à celles-ci constituent des ingérences distinctes dans les droits fondamentaux[380] ; ils exigent pour cette raison une justification distincte[381].

a) Principe de séparation des régimes de conservation et d'accès

199.- Cette séparation des régimes de conservation et d'accès implique que la conservation des données soit licite pour que l'accès à celles-ci soit envisageable. La condition de conservation licite constitue bien une condition nécessaire, un préalable indispensable. Aussi bien, le régime de l'accès ne saurait compenser ou corriger les insuffisances des conditions de conservation des données. Il en va de même des obligations pesant sur les fournisseurs de services de communications électroniques visant à assurer la sécurité et la protection des données conservées. Un tel régime comme de telles obligations ne sauraient « par nature, être susceptible[s] ni de limiter ni même de remédier à l'ingérence grave qui résulterait de la conservation généralisée [des] données »[382].
Dans la même ligne, ainsi que cela a déjà été signalé plus haut, les finalités légitimant l'accès ne sauraient conduire à priver d'effet utile les conditions requises pour une conservation licite de sorte que l'accès aux données ne saurait en principe être autorisé pour des motifs différents, en tout état de cause d'une importance moindre, de ceux qui ont valablement permis leur conservation[383]. Mais comme le montre l'exemple français, des modes d'accès peuvent être relus en modes de conservation (tel le pouvoir de réquisition revisité à l'aune et en tant que mode de conservation rapide) tandis que des modes de conservation – en particulier la conservation rapide – se distinguent mal en pratique d'un mode d'accès (ou plus exactement, dans ce dernier cas, l'intérêt et la portée de la distinction entre conservation et accès sont difficilement perceptibles).

---

[378] *Ibid.*, point 107.
[379] Art. 9§1 de la directive ; CJUE, 21 décembre 2016, *Tele2*, aff. C 203/15 et C 698/15, point 86).
[380] CJUE (sixième chambre), 17 novembre 2022, *Spetisalizirana prokuratura*, aff. C-350/21, point 58.
[381] *Ibid.*
[382] *Ibid.*
[383] Cf. *supra* ; CJUE, 5 avril 2022, précité, point 100.

200.- Dans le cas d'un accès sans conservation préalable, c'est-à-dire d'un accès direct par les autorités compétentes aux données numériques pénales sans l'intermédiaire de tiers, lorsque l'accès peut être ramené à un traitement de données personnelles, son régime est déterminé non par la directive 2002/58 (« Vie privée et communications électroniques ») mais par la directive 2016/80 (« Police-justice »)[384]. Tel est le cas, par exemple, « lorsque des autorités de police saisissent un téléphone et le manipulent à des fins d'extraction et de consultation des données à caractère personnel contenues dans ce téléphone », peu important que la tentative d'accès aux données soit couronnée de succès ou non[385]. Tel est le cas plus largement de « la collecte de données à caractère personnel dans le cadre d'une procédure pénale, et la conservation de celles-ci par les autorités de police »[386] aux fins de « de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »[387].
Si les sources du régime de l'accès direct (sans conservation préalable) et de l'accès indirect (moyennant conservation préalable) diffèrent, les paramètres mobilisés sont en revanche sensiblement proches, à tout le moins comparables, les deux directives poursuivant dans leur champ respectif et selon leurs modalités propres l'objectif commun de préserver le droit à la protection des données personnelles. Aussi bien, dans tous les cas, l'accès doit poursuivre des objectifs légitimes qui, pour ne pas être identiques, ont en commun la lutte contre la criminalité, répondre à une exigence de nécessité et de proportionnalité et assurer le droit à un recours juridictionnel effectif, lequel implique, en cas d'ingérence grave, un contrôle préalable indépendant et, en tout état de cause, le respect du droit à l'information.

b) Régime propre de l'accès

201.- *Objectifs légitimes*
A l'image du raisonnement déployé en matière de conservation, l'accès, en tant qu'il constitue une dérogation aux principes fixés par la directive 2002/58 et au premier chef au principe de confidentialité des communications[388], doit, en premier lieu, poursuivre l'un des objectifs visés et énoncés de façon exhaustive à l'article 15§1 de la directive 2002/58, soit, en substance, la sauvegarde de la sécurité nationale, la lutte contre la criminalité ou la sauvegarde de la sécurité publique. L'interprétation livrée par la Cour de justice conduit à distinguer et décliner ces deux derniers objectifs selon que la criminalité ou la menace sont graves ou envisagées de manière générale.
Apparaissent alors des enjeux de qualification : que recouvrent ces objectifs ? Qu'en est-il de leur déclinaison grave et non grave ? Par qui (le législateur ou le juge) ou à quel niveau (européen ou national) cette qualification doit-elle être opérée ? Dans la formation du droit de l'Union européenne, ces interrogations rejoignent la question classique de l'identification des notions autonomes, ces termes ou ensembles de termes qui, figurant dans les textes mais dépourvus de définition, ne renvoient pas au droit national de sorte qu'ils appellent une interprétation autonome et uniforme afin d'assurer les exigences d'application uniforme du

[384] CJUE (grande chambre), 6 octobre 2020, *La Quadrature du Net*, précité, point 103 ; CJUE (grande chambre), 4 octobre 2024, aff. C-548/21, points 57-58 et 69 et s.
[385] CJUE (grande chambre), 4 octobre 2024, aff. C-548/21, point 77.
[386] *Ibid.*, point 80. Où l'on voit que, dans ce cas, l'ordre entre conservation et accès s'inverse, celle-là découlant de celui-ci.
[387] Art. 1er, §1 de la directive 2016/680 « police-justice ».
[388] Ce qui inclut les communications *stricto sensu* mais ne se limite pas et s'étend au contraire aux données afférentes à ces communications en raison de leur potentiel d'atteinte aux droits à la vie privée et à la protection des données personnelles.

droit de l'Union et le principe d'égalité[389]. S'agissant de l'accès aux données dans le cadre de l'enquête pénale, déterminer à qui revient la tâche d'apprécier la gravité de la criminalité, laquelle détermine les types et conditions d'accès légitime, est donc crucial. Aussi bien, savoir si elle doit faire l'objet d'une interprétation/appréciation autonome et partant européenne ou non constitue l'arrière-plan de la jurisprudence de la Cour de justice. Et le doute était permis car si la notion elle-même n'est pas, à la différence des notions autonomes « habituelles », issues des textes mais de la jurisprudence, sa place et son rôle dans l'économie générale de la construction de la Cour inclinaient à lui reconnaître une certaine autonomie[390]. Dans le même temps, outre son origine, son objet même semblait postuler son caractère relatif, conduisant plutôt à la lui dénier[391]. C'est ce que la Cour a fini par reconnaître[392], admettant que cette question relève – pour l'instant – de la compétence des États membres[393]. Elle concède ainsi, de manière classique, que « pour autant que l'Union n'ait pas légiféré en la matière »[394], la législation pénale et les règles de procédure pénale relèvent de la compétence des États membres qui doivent l'exercer dans le respect du droit de l'Union. Puis, elle observe, en des termes inédits, que « la définition des infractions pénales, des circonstances atténuantes et aggravantes et des sanctions reflète tant les réalités sociales que les traditions juridiques qui varient non seulement entre les États membres, mais aussi dans le temps. Or, ces réalités et traditions revêtent une importance certaine pour déterminer les infractions considérées comme présentant un caractère grave »[395]. Toutefois, la compétence temporairement réservée des États membres n'est pas sans limites. Celles-ci résultent du texte à interpréter : l'article 15§1 de la directive. Or, parce qu'il prévoit des dérogations, il doit être interprété strictement. Et, parce qu'il renvoie aux principes généraux du droit de l'Union et à la Charte des droits fondamentaux, il active leur applicabilité. En particulier, « les États membres ne sauraient dénaturer la notion d'infraction grave" et, par extension, celle de "criminalité grave", en y incluant, aux fins de l'application de cet article 15, paragraphe 1, des infractions qui ne sont manifestement pas graves, au regard des conditions sociétales prévalant dans l'État membre concerné »[396]. De la sorte, la Cour ne renonce pas totalement à peser sur le contenu de la notion, au travers de ses contours et des termes de son appréciation, soit *in abstracto* soit *in concreto*. Sur ce dernier point, tout en soulignant la pertinence du recours à un critère objectif tel qu'un seuil de pénalité

---

[389] Cf., par exemple, ce rappel à propos de la notion d'interception de télécommunications au sens de la directive 2014/41 relative à la décision d'enquête européenne : « selon une jurisprudence constante, il découle tant des exigences de l'application uniforme du droit de l'Union que du principe d'égalité que les termes d'une disposition du droit de l'Union qui ne comporte aucun renvoi exprès au droit des États membres pour déterminer son sens et sa portée doivent normalement trouver, dans toute l'Union, une interprétation autonome et uniforme qui doit être recherchée en tenant compte non seulement des termes de cette disposition, mais également de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie », CJUE (grande chambre), 30 avril 2024, *M.N.*, aff. C-670/22 (*EncroChat*), point 109.

[390] Notamment premières conclusions de l'avocat général Szpunar présentées le 27 octobre 2022, point 74.

[391] Voir aussi les arguments avancés par les sénateurs : *Rapport d'information sur les modalités d'investigation recourant aux données de connexion dans le cadre des enquêtes pénales* précité, p. 89 et s.

[392] Subrepticement dans l'arrêt d'assemblée plénière du 30 avril 2024, là où elle indique, concernant le délit de contrefaçon de l'article L335-2 du Code de la propriété intellectuelle, « qu'il est loisible aux États membres de considérer qu'un tel délit, en tant qu'il porte atteinte à un intérêt fondamental de la société, relève des formes graves de criminalité » (aff. C-470/21, point 145) ; de manière conséquente, dans l'arrêt du même jour rendu en grande chambre : aff. C-178/22, points 46 et s.

[393] CJUE (grande chambre), 30 avril 2024, aff. C-178/22, point 46 : « compte tenu de la répartition des compétences entre l'Union et les États membres en vertu du traité FUE et des différences importantes qui existent entre les systèmes juridiques des États membres dans le domaine pénal, il y a lieu de considérer qu'il incombe aux États membres de définir les [infractions graves] aux fins de l'application de l'article 15, paragraphe 1, de la directive 2002/58 ».

[394] *Ibid.*, point 44.

[395] *Ibid.*, point 45.

[396] *Ibid.*, point 51.

maximum, sous réserve que ce dernier ne soit pas fixé à un « niveau excessivement bas »[397], elle relève son insuffisance à satisfaire seule l'exigence de proportionnalité ; d'où l'appui de l'entité chargée du contrôle de l'accès aux données qui garantit une appréciation au cas par cas indispensable de la gravité de l'infraction[398].
En définitive, le paramètre clé de la gravité de la criminalité n'est pas abandonné aux choix nationaux[399]. Si l'appréciation résultant de ces derniers prévaut, c'est sous réserve d'un encadrement européen tant des critères mobilisés que de leur mise en œuvre par les instances de contrôle.
Dans le cadre de l'accès direct (sans conservation préalable par un tiers) par l'autorité compétente, l'objectif légitime est défini en référence au standard de l'article 52§1 de la Charte des droits fondamentaux de l'Union européenne[400].

202.- *Exigence générale de proportionnalité*
L'accès doit, en second lieu, satisfaire à l'exigence de proportionnalité qui requiert que l'objectif poursuivi soit en relation avec la gravité de l'ingérence dans les droits fondamentaux qu'entraîne l'accès aux données, l'ingérence étant déterminée par la nature des données concernées, selon que sont visées les données de contenu, de trafic, de localisation ou d'identité, et l'ampleur de celles-ci, en fonction des critères subjectifs et temporels bornant cet accès.
Miroir de la mesure de la gravité de la criminalité qui conditionne l'accès (type et conditions) et relève d'une marge d'appréciation qui, pour être nationale, est encadrée par le droit de l'Union, la mesure de la gravité de l'ingérence que représente l'accès lui-même ressortit à la marge d'interprétation qui, pour être européenne, s'ouvre aux considérations opérationnelles (nationales)[401].
C'est ainsi, peut-être, que l'on peut comprendre sans le craindre[402], le passage de l'arrêt rendu à propos de la procédure française de réponse graduée qui, après avoir rappelé que « même si la liberté d'expression et la confidentialité des données à caractère personnel sont des préoccupations primordiales et si les utilisateurs des télécommunications et des services Internet doivent avoir la garantie que leur intimité et leur liberté d'expression seront respectées, ces droits fondamentaux ne sont pas pour autant absolus », souligne que « dans le cadre d'une mise en balance des droits et intérêts en cause, ceux-ci doivent parfois s'effacer devant d'autres droits fondamentaux et des impératifs d'intérêt général tels que la défense de l'ordre public et la prévention des infractions pénales ou la protection des droits et libertés d'autrui. Tel est, en particulier, le cas lorsque la prépondérance accordée auxdites préoccupations primordiales est de nature à entraver l'efficacité d'une enquête pénale, notamment en rendant impossibles ou excessivement difficiles l'identification effective de l'auteur d'une infraction pénale et l'imposition d'une sanction à son égard »[403].
Par-là, la proportionnalité de l'ingérence s'apprécie aussi à l'aune d'une telle impossibilité ou difficulté excessive lesquelles peuvent (doivent ?) permettre de la tolérer. C'est

---

[397] *Ibid.*, point 55 ; en l'occurrence : « un seuil fixé par référence à une peine maximale de réclusion de trois ans n'apparaît pas, à cet égard, comme étant excessivement bas », point 56.
[398] *Ibid.*, points 60 et suivants.
[399] *Infra*, B.
[400] En particulier, « un traitement de données à caractère personnel dans le cadre d'une enquête policière visant la répression d'une infraction pénale, tel qu'une tentative d'accès aux données contenues dans un téléphone portable, doit être considéré, en principe, comme répondant effectivement à un objectif d'intérêt général reconnu par l'Union, aff. C-548/21, point 86.
[401] *Infra*, B.
[402] *Supra*, paragraphes 170 et suivants, en lien avec le renversement de perspective que semble imposer l'approche de l'enquête pénale par le prisme du droit à la vie privée et à la protection des données personnelles (et plus largement des droits fondamentaux).
[403] CJUE (Assemblée plénière), 30 avril 2024, précité, point 116.

particulièrement vrai s'agissant des infractions commises en ligne pour lesquelles le « réel risque d'impunité systémique » tenant aux possibilités démultipliées d'anonymat peut participer à la détermination des mesures – d'enquête et plus largement d'accès – légitimement disponibles[404].
S'agissant de l'accès direct (sans conservation préalable par un tiers) par une autorité publique, l'exigence de proportionnalité implique la pondération de la gravité de la limitation apportée à l'exercice des droits fondamentaux en cause (laquelle dépend de la nature et de la sensibilité des données auxquelles les autorités de police compétentes sont susceptibles d'avoir accès), de l'importance de l'objectif d'intérêt général poursuivi par cette limitation, du lien existant entre la personne ciblée et l'infraction pénale en cause ou encore de la pertinence des données en cause pour constater les faits[405].

203.- *Condition de stricte nécessité*
En troisième lieu, la configuration du régime de l'accès doit garantir que ce dernier ait lieu dans les limites du strict nécessaire[406] et soit subordonné à des garanties appropriées[407]. Ces dernières incluent au premier chef une exigence de légalité (des règles claires, précises et de valeur contraignante indiquant en quelles circonstances et sous quelles conditions l'accès aux données doit être accordé par les opérateurs) [408]. Elles supposent en second lieu la prévision de conditions matérielles et procédurales précises qui dépassent la seule exigence que l'accès réponde à l'un des objectifs précités.
C'est pourquoi « un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire, la réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits »[409].
En particulier, lorsque l'objectif poursuivi est la lutte contre la criminalité, l'accès ne peut être accordé qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction pénale ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction[410].
De plus, lorsque l'ingérence est grave, comme c'est le cas de l'accès aux données de trafic et de localisation, l'infraction considérée doit relever de la criminalité grave[411]. En outre, dans

[404] *Ibid.*, points 117-121.
[405] Aff. C-548/21, point 90 et s.
[406] CJUE, *Tele2*, point 116.
[407] Art. 15§1 de la directive 2002/58.
[408] CJUE, *Tele2*, point 117.
[409] *Ibid.* point 119. En tant qu'elle traduit l'exigence de proportionnalité et de stricte nécessité, l'affirmation énoncée au regard des données de trafic et de localisation paraît pouvoir être généralisée.
[410] *Ibid.*
[411] Toutefois, l'affinement de l'appréhension de la nature de certaines données relatives au trafic, telles les adresses IP, conduit à tempérer l'affirmation. Ainsi, non seulement l'accès aux adresses IP attribuées à la source, dans la mesure où il ne poursuit et permet que l'identification et non le traçage d'un parcours de navigation ou le profil détaillé d'un utilisateur, est possible à des fins de lutte contre les infractions pénales en général, mais en outre cet objectif « permet de justifier qu'il soit donné accès aux données de trafic et de localisation qui ont été stockées et donc conservées dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation et à la fourniture de services à valeur ajoutée, comme l'autorise l'article 6 de la directive 2002/58 », c'est-à-dire dans le cadre d'une conservation facultative. Énoncée au point 98 du deuxième arrêt *La Quadrature du Net*, l'affirmation surprend. D'une part, la Cour l'appuie sur un renvoi exprès au premier arrêt *La Quadrature du Net*, en particulier ses points 108 et 167. Or, le premier se contente d'indiquer les contours de la conservation facultative des donnés de trafic et de localisation. Le second énonce que la faculté des États membres de prévoir l'accès à ces données peut s'exercer à des fins de lutte contre la criminalité *grave* ou de sauvegarde de la sécurité nationale…D'autre part, aucun élément d'explication n'est avancé en soutien.

certaines situations particulières, telles celles dans lesquelles les intérêts vitaux de la sécurité nationale sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes peut être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient dans un cas concret apporter une contribution effective à la lutte contre de telles activités[412].

C'est ici, peut-être, que l'accès direct régi par la directive Police-Justice se distingue dans la mesure où la gravité de la limitation des droits découlant de l'accès aux données n'implique pas de restreindre un tel accès à la criminalité grave. Selon la Cour, « considérer que seule la lutte contre la criminalité grave est susceptible de justifier l'accès à des données contenues dans un téléphone portable limiterait les pouvoirs d'enquête des autorités compétentes, au sens de la directive 2016/680, à l'égard des infractions pénales en général. Il en résulterait un accroissement du risque d'impunité pour de telles infractions, compte tenu de l'importance que peuvent avoir de telles données pour les enquêtes pénales. Ainsi, une telle limitation méconnaîtrait la nature spécifique des missions accomplies par ces autorités aux fins énoncées à l'article 1er, paragraphe 1, de cette directive, (…) et nuirait à l'objectif de réalisation d'un espace de liberté, de sécurité et de justice au sein de l'Union que poursuit ladite directive »[413].

La Cour s'empresse cependant d'indiquer que « ces considérations sont sans préjudice » des exigences découlant de l'article 52, paragraphe 1, de la Charte, en particulier de légalité (la base légale autorisant une telle limitation doit en définir la portée de manière suffisamment claire et précise) et de nécessité (outre les liens entre la cible et l'infraction devant être attestés par des soupçons raisonnables étayés par des éléments objectifs et suffisants[414], le risque[415] d'ingérence particulièrement grave en cas d'accès à des données sensibles conduit à estimer que ce dernier ne peut être considéré nécessaire que dans un « nombre de cas limité »[416]).

204.- *Exigences complémentaires de garantie judiciaire et de droit à l'information.*

En quatrième lieu, s'agissant des garanties procédurales, deux exigences supplémentaires s'imposent, qui constituent la condition des garanties qui précèdent : le respect, d'une part, de la garantie judiciaire et, d'autre part, du droit à l'information[417] des personnes dont les données ont été recueillies ou analysées, notamment des motifs ayant fondé l'autorisation de l'accès[418].

La garantie judiciaire inclut *a minima* la sauvegarde du droit à une protection juridictionnelle effective, du droit à un recours juridictionnel permettant la vérification *a posteriori* du respect des conditions précitées. C'est dire que dès lors qu'un certain seuil de gravité est franchi la garantie judiciaire requiert le contrôle *a priori* de la stricte nécessité en l'espèce de l'accès à certaines données[419].

---

[412] *Ibid.* Voir BVerGericht 1er octobre 2024, 1 BvR 1160/19, décision d'inconstitutionnalité partielle (sur les pouvoirs de la police en matière de collecte et conservation données concernant les personnes contacts de personnes poursuivies pour terrorisme).

[413] CJUE, 4 octobre 2024 (C-548/21), point 97.

[414] *Ibid*., point 101.

[415] C'est bien le risque qui suffit et non l'ingérence effective, *ibid*. à propos de la simple tentative (infructueuse) d'accès.

[416] Cette affirmation peut être lourde de conséquences là où l'exploitation d'un téléphone est devenue banale…

[417] *Infra*, paragraphe 229.

[418] CJUE, 4 octobre 2024 (C-548/21), point 120 : à propos de l'accès direct (traitement), l'information s'impose « dès le moment où cela n'est pas susceptible de compromettre les enquêtes ». C'est pourquoi, s'agissant de l'exploitation d'un téléphone portable, la connaissance par l'intéressé de la saisie de son téléphone imposait son information préalable dans la mesure où il n'apparaît pas que l'« informer du fait que les autorités allaient tenter d'accéder à ces données était susceptible de nuire aux enquêtes ».

[419] Ainsi, lorsque l'accès procède d'une ingérence non grave, un tel contrôle préalable n'est pas exigé. Tel est le cas de la procédure française qui permet l'accès par la Hadopi aux adresses IP attribuées à la source aux seuls fins d'identification, sous réserve des cas qualifiés d'atypiques par la Cour de justice susceptibles de se produire au stade où la Hadopi est appelée à décider de saisir ou non le ministère public en vue de la poursuite de la

205.- La nécessité d'un contrôle préalable[420] – c'est-à-dire d'un régime d'autorisation – emporte avec elle, selon la Cour, plusieurs exigences associées : ce contrôle doit être réalisé, sur la base d'une demande motivée, soit par une juridiction soit par une autorité administrative indépendante disposant de toutes les attributions et présentant toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts (selon le cas la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave ou la prévention de menaces graves pour la sécurité publique) et droits en cause (à la vie privée, aux données personnelles, à la liberté d'expression ou de propriété[421]).
Précisément, « [s]'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès »[422].
Or, « l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable (…) impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique (…) que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale »[423].
Voilà pourquoi le ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique, ayant pour mission non pas de trancher en toute indépendance un litige, mais de le soumettre, le cas échéant, à la juridiction compétente, en tant que partie au procès exerçant l'action pénale, ne saurait satisfaire l'exigence d'indépendance ainsi entendue[424]. Il en va de même de la police judiciaire[425].

206.- *Champs et portée différenciée*
Pour l'heure, un tel régime d'autorisation s'impose à l'endroit des données de trafic et de localisation[426]. A l'inverse, tel ne paraît pas être le cas s'agissant des seules données d'identité, compte tenu de l'ingérence non grave que leur accès implique[427].
A mi-chemin entre les données de trafic et de localisation, d'une part, et les simples données d'identité, d'autre part, la question du sort de la conservation et de l'accès aux adresses IP attribuées à la source d'une connexion[428] s'est posée à la faveur du recours préjudiciel formé par le Conseil d'État français à propos du dispositif de protection des droits d'auteur et de lutte

---

contravention de négligence caractérisée ou du délit de contrefaçon : l'introduction d'un contrôle préalable avant l'éventuel envoi de la notification constatant des faits pouvant constituer la contravention s'impose (CJUE (Assemblée plénière), 30 avril 2024, précité, points 137 et 141).
[420] Sous réserve de « cas d'urgence dûment justifiée, auquel cas le contrôle [devant] intervenir dans de brefs délais », CJUE (grande chambre), 2 mars 2021, *Prokuratuur*, aff. C-746-18, point 58.
[421] Pour ce dernier, voir l'affaire C-470/21 concernant les pouvoirs de l'HADOPI.
[422] CJUE (grande chambre), 2 mars 2021, *Prokuratuur*, aff. C-746-18, point 52.
[423] CJUE (grande chambre), 2 mars 2021, *Prokuratuur*, aff. C-746-18, point 54.
[424] *Ibid*.
[425] CJUE (sixième chambre), 17 novembre 2022, *Spetsializirana prokuratura*, aff. C-350/21, point 114.
[426] CJUE (grande chambre), 2 mars 2021, *Prokuratuur*, aff. C-746-18, points 51 et s.
[427] Leur conservation généralisée et indifférenciée étant permise sans délai particulier aux fins de recherche, de détection et de poursuites des infractions pénales en général.
[428] Cf. affaire devant l'assemblée plénière de la Cour C-470/21.

contre la contrefaçon, en particulier la procédure dite de réponse graduée mise en œuvre par la HADOPI[429].

207.- L'affaire, dont les enjeux dépassent et la procédure française ou le secteur de la propriété intellectuelle et le régime des adresses IP pour intéresser les coordonnées générales de la conservation et de l'accès aux données personnelles en Europe, a été en conséquence l'objet de toutes les attentions, des acteurs publics et privés, politiques, économiques et citoyens, français et européens, chacun faisant de la procédure un test ou une étape-clé pour la construction en cours devant (et par) la Cour de justice. Témoins de ces enjeux et controverses, les deux jeux de conclusions présentées par l'avocat général Szpunar qui invitait celle-ci à emprunter la voie étroite « non pas [d']un revirement de la jurisprudence exigeante et protectrice des droits fondamentaux développée par la Cour depuis les arrêts *Tele2 Sverige* et *Watson e.a.* et *La Quadrature du Net e.a.*, mais [d']un développement nécessaire de celle-ci qui s'inscrit (…) dans le prolongement des principes édictés par la Cour [et qui] vise non pas à remettre en cause la jurisprudence existante, mais à permettre, au nom d'un certain pragmatisme, son adaptation en des circonstances particulières et très étroitement circonscrites »[430]. C'est ainsi qu'il proposait notamment une appréciation précisée, pour ne pas dire renouvelée, de la proportionnalité de la conservation et de l'accès à certaines données. Apparaîtrait pour ce faire parmi les paramètres de cette appréciation une catégorie « intermédiaire », en tout cas distincte, entre la criminalité en général (*i.e.* non grave) et la criminalité grave, constituée par les infractions exclusivement commises en ligne, l'affinement dans l'appréciation de la gravité de l'ingérence dans les droits fondamentaux permettant de considérer que la conservation et l'accès à des adresses IP n'est pas grave par nature, mais qu'ils le deviennent lorsque ces données peuvent conduire à un traçage exhaustif du parcours de navigation et à tirer des conclusions très précises sur la vie privée[431] ; ce d'autant que ces données pourraient constituer le seul moyen permettant la détection et la poursuite de certaines infractions et en tout état de cause le moyen permettant la moindre ingérence dans les droits fondamentaux. Sur cette base, l'exigence d'un contrôle préalable pourrait être écartée, les conditions entourant la conservation et l'accès suffisant à garantir que ces derniers soient limités au strict nécessaire[432]. L'Assemblée plénière de la Cour de justice n'a pas choisi cette voie même si elle adopte la démarche générale proposée par son avocat général.
S'agissant de l'accès[433] aux adresses IP, la Cour confirme que le régime de ce dernier est fonction de l'utilisation susceptible d'en être faite, laquelle « rétroagit » et modifie la nature de cette donnée : « [l]orsqu'une adresse IP est ainsi utilisée à seule fin d'identifier son titulaire dans le cadre d'une procédure administrative spécifique pouvant déboucher sur des poursuites pénales contre celui-ci et non à des fins visant, par exemple, à révéler les contacts ou la localisation de ce titulaire, l'accès à cette adresse à cette seule fin concerne ladite adresse *en tant que donnée relative à l'identité civile plutôt qu'en tant que donnée relative au trafic* »[434]. Mais la labilité de la nature de cette donnée impose des précautions. Car si en principe l'accès

---

[429] Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet ; depuis le 1er janvier 2022, elle a fusionné avec le CSA (Conseil supérieur de l'audiovisuel) pour former l'ARCOM (Autorité de régulation de la communication audiovisuelle et numérique, *Loi n° 2021-1382 du 25 octobre 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique*).
[430] Point 30 des conclusions présentées le 28 septembre 2023. Si l'avocat général y insiste : la distinction entre revirement et développement nécessaire « n'est pas seulement sémantique », l'affirmation outre qu'elle peut ne pas convaincre signale la position délicate de la Cour appelée à concilier (plutôt que choisir entre) exigence et pragmatisme.
[431] Secondes conclusions présentées le 28 septembre 2023 dans l'affaire C-470/21, point 55.
[432] *Ibid.* point 75.
[433] Concernant la conservation, *supra*, paragraphe 189.
[434] CJUE (assemblée plénière), 28 avril 2024, précité, point 101.

aux adresses IP par la Hadopi ne permet pas de tirer des conclusions sur la vie privée des utilisateurs, de sorte qu'il ne constitue pas une ingérence grave[435], le contexte dans lequel s'inscrit cet accès ne permet pas d'exclure que dans certaines situations « atypiques [pourraient être révélées] des informations, le cas échéant sensibles, sur des aspects de la vie privée de la personne en cause qui, prises ensemble, pourraient permettre [à la Hadopi] de tirer des conclusions précises sur la vie privée de celle-ci par exemple en établissant son profil détaillé »[436]. Cependant, « en l'occurrence, l'ingérence dans la vie privée (…) ne revêt pas nécessairement un degré de gravité élevé », compte tenu de ce que l'accès est « réservé à un nombre limité d'agents agréés et assermentés », « tenus à une obligation de confidentialité », d'une « autorité publique [qui] bénéficie d'ailleurs d'un statut indépendant » ; qu'il poursuit un « but unique » d'identification (à partir d'éléments permettant de soupçonner une activité illicite) ; qu'il est « strictement limité aux données nécessaires à cette fin »[437].

4) Exploitabilité des données : les conditions d'utilisation

208.- La construction de la donnée pénale n'est « parfaite » qu'à la condition que celle-ci soit exploitable et partant de pouvoir prétendre à la qualité de preuve admissible dans le cadre de la procédure pénale. Se pose dès lors la question de savoir si la donnée pourtant juridiquement indisponible (parce que sa conservation n'est pas autorisée en elle-même ou que les conditions de celle-ci n'ont pas été respectées si bien que sa conservation n'est pas licite) ou juridiquement inaccessible (parce que son accès n'était pas autorisé ou que les conditions de celui-ci n'ont pas été respectées si bien que cet accès est illicite) peut prétendre présenter malgré tout une telle qualité. C'est donc poser par la même occasion la question de la sanction applicable à la conservation ou à l'accès illicites à des données dans le cadre d'une procédure pénale.

209.- La question de l'exploitabilité des données a été posée à la Cour qui propose une réponse très en retrait en comparaison du traitement qu'elle réserve aux questions de la disponibilité (conservation) et de l'accessibilité (accès) des données. Pourtant, ainsi qu'il vient d'être souligné, de la réponse à cette question dépend la garantie, même partielle et indirecte, des conditions de la disponibilité et de l'accessibilité des données. Toujours est-il que compte tenu de la répartition des compétences entre l'Union et ses membres et en l'état des textes adoptés par celle-là, « il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave[[438]], d'informations et d'éléments de preuve qui ont été obtenus par une telle conservation de données contraire au droit de l'Union »[439]. En particulier, en l'absence de règles de l'Union en la matière, le principe d'autonomie procédurale confère aux ordres juridiques internes le soin de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union[440]. Toutefois le droit national doit à cette occasion garantir le respect des principes d'équivalence *(a)* et d'effectivité *(b)*.

---

[435] *Ibid.*, point 99.
[436] *Ibid.*, point 111.
[437] *Ibid.*, pour tous, voir points 113 et 114.
[438] La mention s'explique par le cadre de la question préjudicielle. Cependant, l'affirmation doit pouvoir être étendue au-delà du seul cadre de la criminalité grave.
[439] CJUE (grande chambre), *La Quadrature du Net e.a.*, précité, point 222.
[440] CJUE (grande chambre), *La Quadrature du Net e.a.*, précité, point 223.

a) Principe d'équivalence

210.- Quant au premier, qui exige que la méconnaissance du droit de l'Union (ici la conservation ou l'accès illicites) bénéficie d'un régime analogue et qui, en tout état de cause, ne soit pas moins favorable que celui dont sont assorties les violations comparables du droit interne, cela revient, au regard de la procédure pénale française, à activer le régime des nullités[441].

b) Principe d'effectivité

211.- S'agissant du second, il garantit que l'exercice des droits conférés par le droit de l'Union ne soit pas rendu impossible en pratique ou excessivement difficile. A propos de l'admissibilité et de l'exploitation des informations et des éléments de preuve, la Cour observe qu'elles ont pour objectif « d'éviter que des informations et des éléments de preuve qui ont été obtenus de manière illégale portent indûment préjudice à une personne soupçonnée d'avoir commis des infractions pénales »[442].
Mais si elle concède, compte tenu de la grande variété en la matière des approches procédurales, allant de l'exclusion totale ou partielle de tels éléments à leur admissibilité pleine ou relative, qu'un tel objectif peut être poursuivi de diverses manières, non seulement elle souligne que la nécessité d'une éventuelle exclusion s'apprécie au regard des risques pour le principe du contradictoire, donc du droit à un procès équitable[443], mais elle réserve en outre la situation dans laquelle « une partie ne serait pas en mesure de commenter efficacement un moyen de preuve qui ressortit à un domaine échappant à la connaissance des juges et qui est susceptible d'influencer de manière prépondérante l'appréciation des faits »[444] ; dans un tel cas, le juge national « doit constater une violation du droit à un procès équitable et exclure ce moyen de preuve afin d'éviter une telle violation »[445].
Il n'est pas inutile de noter que, ce disant, la Cour se réfère à sa propre jurisprudence dans laquelle, renvoyant à celle de la CEDH[446], elle soulignait que « lorsque les parties concernées sont en droit de formuler, devant le tribunal, des observations sur un moyen de preuve, il doit s'agir là d'une possibilité véritable de commenter efficacement celui-ci pour que la procédure revête le caractère équitable exigé par l'article 6, paragraphe 1, de la CEDH. Une vérification de ce point s'impose en particulier *lorsque le moyen de preuve ressortit à un domaine technique échappant à la connaissance des juges* et est susceptible d'influencer de manière prépondérante l'appréciation des faits par le tribunal »[447].

On le voit, les « paramètres système » qui se dégagent de la jurisprudence de la Cour exercent une pression plus ou moins intense sur les ordres nationaux appelés, dans ce cadre-là, à définir leurs « préférences système ».

---

[441] *Infra*, paragraphes 226 et suivants.
[442] CJUE (grande chambre), *La Quadrature du Net e.a.*, précité, point 225.
[443] *Ibid*, point 226.
[444] *Ibid*.
[445] *Ibid*.
[446] Deux affaires françaises au demeurant : CEDH, *Mantovanelli c. France*, 18 mars 1997, *Recueil des arrêts et décisions* 1997-II, § 33 et 34 ; CEDH, *Pélissier et Sassi c. France*, 25 mars 1999, *Recueil des arrêts et décisions* 1999-II, § 45.
[447] CJUE (grande chambre), *La Quadrature du Net e.a.*, précité, point 226 (nous soulignons).

B.- Préférences de la nouvelle configuration

212.- Si la « contrainte structurelle » qui pèse désormais sur les procédures pénales nationales et qui découle de l'ensemble composé des textes de droit primaire et dérivé de l'Union et de l'interprétation qu'en livre la Cour se déploie d'abord et avant tout par le biais de la définition des « paramètres » (au sens du vocabulaire informatique) de la configuration nouvelle déterminant la circulation des données pour les besoins de l'enquête pénale, elle se prolonge aussi au travers de l'encadrement des marges de manœuvre que le droit européen des données personnelles ménage au profit des ordres internes.
Ce sont elles qui permettent de définir les « préférences » (également au sens du vocabulaire informatique) nationales autorisées, les options nationales envisageables qui, par un effet de boucle, sont susceptibles de rétroagir sur le droit européen des données, ses textes comme sa jurisprudence, en poussant, par la manifestation de résistances ou la proposition de solutions de compromis, à des aménagements, infléchissements ou approfondissements.
Ces préférences, conçues dans le cadre permis par les marges laissées aux ordres internes (*1*), sont à leur tour déterminées très largement par les traditions et choix nationaux, tant constitutionnels que liés aux approches et équilibres de la procédure pénale, et qui en constituent les variables (*2*).

1) Marges

213.- On l'a déjà souligné, c'est une gradation qui se fait jour à partir de la combinaison des textes et de la jurisprudence de la Cour dans laquelle des contraintes fortes enserrent la conservation des données qui ne reculent qu'en apparence avec l'accès et se réduisent en revanche à peu de choses avec l'exploitation.
Dès lors, si la compétence de principe du droit national est rappelée par la Cour s'agissant de l'accès, là où elle souligne « qu'il appartient au droit national de déterminer les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données dont ils disposent »[448], c'est pour préciser immédiatement que « pour satisfaire à l'exigence de proportionnalité, une telle réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire »[449]. Ces conditions, ainsi qu'il a été vu plus haut, se révèlent bien plus détaillées et exigeantes que ne semblait l'augurer le rappel de la compétence nationale.

214.- S'agissant de l'exploitation, la marge nationale est bien plus ample puisqu'« il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave[[450]], d'informations et d'éléments de preuve qui ont

[448] Parmi d'autres CJUE (grande chambre), 2 mars 2021, *Prokuratuur*, précité, point 48.
[449] *Ibid*.
[450] La mention s'explique par le cadre de la question préjudicielle. Cependant, l'affirmation doit pouvoir être étendue au-delà du seul cadre de la criminalité grave.

été obtenus par une telle conservation de données contraire au droit de l'Union »[451] ; les contraintes apparaissent beaucoup plus lâches dans la mesure où elles se limitent à l'énoncé, moyennant quelques maigres précisions, des principes d'équivalence et d'effectivité[452].

Mais les marges ne se logent pas seulement là où le droit national est expressément supposé détenir ou conserver la main, elles se manifestent aussi au sein des options ouvertes par le droit de l'Union. C'est ce qu'illustrent les *choix* variés des États membres adoptés pour pallier ou minimiser les effets de la limitation de la conservation généralisée et indifférenciée des données de trafic et de localisation à la seule fin de sauvegarde de la sécurité nationale. C'est ce que mettent en relief aussi les *tentatives* de déjouer les contraintes propres à la conservation en leur substituant celles de l'accès, mais aussi les *stratégies* de neutralisation de l'ensemble grâce à la reconnaissance d'une exploitabilité étendue des données, en dépit de l'illicéité de leur conservation ou collecte[453].

2) Variables (constitutionnelles)

215.- Ne seront ici examinés que les premiers (les choix), dans la mesure où les tentatives ont quant à elles échoué, la Cour ayant tué dans l'œuf toute velléité en ce sens[454], tandis que les stratégies lui échappent pour l'heure et relèvent d'enjeux et considérations plus larges[455].

216.- Les transformations imposées par la jurisprudence de la Cour varient logiquement en fonction de l'état du droit applicable et en particulier du cadre constitutionnel de référence. C'est ce qu'ont permis de révéler plusieurs séminaires d'étude sur la réception comparée de la jurisprudence de la CJUE notamment en Allemagne, Belgique, Italie ou Irlande[456].
Là où comme en Allemagne la question de la protection des données personnelles fait l'objet d'une protection constitutionnelle ancienne et consolidée[457], l'impact est moins sensible que

---

[451] CJUE (grande chambre), *La Quadrature du Net e.a.*, précité, point 222.
[452] *Supra*, paragraphes précédents.
[453] Tendance plus largement observable ailleurs, cf. AP, 21 décembre 2022 dissociant l'obtention (déloyale) de l'usage (possible) et procédant à un revirement motivé par la jurisprudence de la CEDH.
[454] CJUE (grande chambre), 5 avril 2022, *Commissioner of the Garda Síochána e.a.*, aff. C-140/20, point 100 (« les données relatives au trafic et les données de localisation ne peuvent pas faire l'objet d'une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave et, partant, un accès à ces données ne saurait être justifié à ces mêmes fins. Or, lorsque ces données ont exceptionnellement été conservées de manière généralisée et indifférenciée à des fins de sauvegarde de la sécurité nationale contre une menace qui s'avère réelle et actuelle ou prévisible, dans les conditions visées au point 58 du présent arrêt, les autorités nationales compétentes en matière d'enquêtes pénales ne sauraient accéder auxdites données dans le cadre de poursuites pénales, sous peine de priver de tout effet utile l'interdiction de procéder à une telle conservation aux fins de la lutte contre la criminalité grave »), CJUE, (grande chambre), 20 septembre 2022, *SpaceNet AG*, aff. C-793/19, point 130 ; CJUE (sixième chambre), 17 novembre 2022, *Spetsializirana prokuratura*, aff. C-350/21, point 47.
[455] *Infra, §2.*
[456] Séminaire du 21 novembre 2022 organisé par l'équipe de recherche NTIS, avec les interventions sur l'Allemagne de Benjamin Vogel (Max Planck Institute for the Study of Crime, Security and Law) et sur l'Italie de Mariagisa Landolfi (Université de Pise) ; séminaire du 3 avril 2023 avec les interventions sur la Belgique de Vanessa Franssen (Université de Liège), sur l'Italie de Michele Caianiello et Giulia Lasagni (Université de Bologne), sur l'Irlande de TJ Mcityre (University College Dublin).
[457] Dans un arrêt du 15 décembre 1983, la Cour constitutionnelle allemande consacrait, à l'occasion de l'examen d'une loi sur le recensement, le droit à l'autodétermination informationnelle (« *Informationnelle Selbstbestimmung* »), déduit des articles 1er (dignité de l'homme) et 2 (droit au libre développement de sa personnalité) de la Loi fondamentale. Elle jugeait ainsi que « la Constitution garantit en principe la capacité de l'individu à décider de la communication et de l'utilisation de ses données à caractère personnel ». Depuis, ce droit à l'autodétermination informationnelle « irrigue la jurisprudence postérieure de la Cour en matière de protection des données personnelles, concernant par exemple la recherche policière par recoupements dans le cadre de la lutte

dans des systèmes où une telle protection est plus récente et encore largement médiatisée par le droit au respect de la vie privée, comme en France[458]. Sans doute aussi ces écarts de protection constitutionnelle se nourrissent-ils de l'histoire politique et de la conception de l'État qui en découle, comme l'illustre le concept tiré de la jurisprudence du tribunal constitutionnel fédéral allemand dès 2010[459] de « compte global de surveillance » qui alerte sur la nécessité de mesurer le degré de surveillance dans une société donnée et entend marquer le point de rupture au-delà duquel la surveillance dépasse le seuil de ce qui est démocratiquement acceptable, empêchant, notamment, l'ajout de nouvelles mesures de surveillance et imposant en conséquence de choisir parmi elles.

217.- La différence d'approche peut ensuite s'observer à travers les réponses que les ordres juridiques nationaux adoptent pour lever les incompatibilités du droit interne avec le droit de l'Union. C'est ainsi que sur la base d'un même arrêt les concernant tous deux, les ordres juridiques français et belge ont opté pour deux voies différentes dont on retiendra ici qu'elles ont en commun de tenter d'obvier autant que possible les effets de l'exclusion de la conservation généralisée et indifférenciée des données de trafic aux fins de lutte contre la criminalité même grave.

a) L'option de la conservation ciblée

218.- La lecture de l'arrêt la *Quadrature du Net* par la Cour constitutionnelle belge[460] tranche singulièrement avec celle du Conseil d'État[461], l'une et l'autre livrées avec un jour d'écart.

Se conformant sans réserve, comme elle y est accoutumée[462], à la jurisprudence de la CJUE, la première annule les dispositions de la loi belge du 29 mars 2016, conduisant ensuite le législateur belge[463] à déployer une stratégie consistant à faire fond sur l'option de la conservation ciblée quitte à friser l'absurde mais en soulignant ce faisant les limites et faiblesses de la jurisprudence de la Cour de justice. En effet, exploitant les différents critères de la conservation ciblée, le législateur parvient à couvrir par son intermédiaire la quasi-totalité du territoire et de la population[464].

b) La préférence pour la conservation rapide

219.- La position du Conseil d'État se distingue alors nettement de celle de la juridiction constitutionnelle belge. Le dispositif français est largement sauvé en particulier s'agissant de la

---

contre le terrorisme ou la collecte de données dans le cadre des assurances », *Le numérique et les droits fondamentaux*, *op.cit.*, p. 267.

[458] Voir sur la consécration constitutionnelle récente de la protection du droit à la vie privée, MAZEAUD Vincent, « La constitutionnalisation du droit au respect de la vie privée », *Les nouveaux cahiers du Conseil constitutionnel*, n° 48, 2015 (§1) ; sur la protection constitutionnelle des données personnelles, SURREL Hélène, « La protection des données à caractère personnel, domaine emblématique des interactions jurisprudentielles entre cours européennes et Conseil constitutionnel », *Titre VII*, n°2, 2019.

[459] Sur lequel voir notamment, LELIEUR Juliette, SAAS Claire et WEIGEND Thomas « Chronique de droit pénal constitutionnel allemand. Année 2010 », *RSC*, n°3, 2011, pp. 690-701.

[460] Cour constitutionnelle belge, 22 avril 2021 n°57/2021 (https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/04/2021-057f.pdf).

[461] CE, ass., 21 avr. 2021, n° 393099, *French data network*.

[462] Voir déjà la décision de la Cour constitutionnelle belge du 11 juin 2015, n° 84/2015 faisant suite à l'arrêt *Digital Rights* (CJUE (grande chambre), 8 avril 2014, aff. jtes C-293/12 et C-594/12.

[463] Loi du 20 juillet 2022.

[464] FLUMIAN Baptiste, FRANSSEN Vanessa, « Le nouveau cadre légal belge en matière de conservation des données de communications électroniques : "*Old Wine in New Bottles*" pour les autorités judiciaires ? », *in* FRANSSEN Vanessa, MASSET Adrien (dir.), *Le droit pénal et la procédure pénale en constante évolution*, Anthemis, 2023, vol. 217, p. 315, sp. p. 342.

conservation généralisée et indifférenciée des données de trafic et de localisation au nom de la sauvegarde de la sécurité nationale (conservation préventive), compte tenu des menaces prévisibles et actuelles liées à la persistance d'un risque terroriste élevé, à un « risque d'espionnage et d'ingérence étrangère », à des menaces graves liées à « une augmentation de l'activité des groupes radicaux et extrémistes », sous réserve néanmoins de l'absence de réexamen périodique de la persistance de la menace qui condamnerait le dispositif[465].
Quant aux autres objectifs de défense de la sécurité publique et de poursuite des infractions pénales, si le Conseil d'État relève d'abord la possibilité offerte par la conservation ciblée, c'est pour mieux en souligner les limites techniquement impraticables et l'efficacité opérationnelle incertaine[466], de sorte qu'elle ne permet pas de garantir « le respect des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment celle des atteintes à la sécurité des personnes et des biens, ainsi que de recherche des auteurs d'infractions, notamment pénales »[467]. Il en va de même de la conservation rapide[468], qui, cependant, combinée à la conservation préventive, permet à « [l]'autorité judiciaire d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie » [469].
Il ne restait plus à la Cour de cassation[470] qu'à s'engouffrer dans la brèche en faisant elle aussi de la conservation rapide l'un des véhicules de la compatibilité -relative- du droit français et du sauvetage -maximal- des procédures pénales en cours et à venir.
220.- Reste que la solution française qui, sur ce point, a pour elle le raisonnement de la Cour de justice, en révèle dans le même temps les limites.
D'une part, elle confirme que la notion juridico-politique de sécurité nationale est au cœur de la construction, en constituant l'une de ses clés comme son talon d'Achille. Si elle en est sans doute une condition d'acceptabilité, elle peut tout aussi bien en représenter la faille : faille qui fragilise l'édifice sans trop lézarder la façade mais qui pourrait conduire à un déséquilibre fatal. En effet, la « trouvaille » qui consiste à combiner conservation préventive et conservation rapide pour garantir le maintien de l'accès aux données de connexion aux fins d'enquête pénale, à tout le moins en matière de criminalité grave, mine la portée d'un encadrement apparemment strict de la conservation généralisée et indifférenciée des données de trafic et de localisation.
Source de fragilité ou de force, l'appui sur la sécurité nationale ne permet le maintien de la conservation – temporaire et contrôlée – des données de trafic et de localisation, c'est-à-dire ce qui alimente le réservoir des données, que sous réserve de la persistance d'une menace actuelle ou prévisible. Celle-ci venant à disparaître, cette source d'alimentation du réservoir viendrait à se tarir. Or, si une telle perspective est évidemment souhaitable, elle constituerait une fort mauvaise nouvelle pour les services d'enquête. Où l'on voit que l'ensemble repose sur un fonctionnement anormal, pathologique, au sens où il faudrait que persistent des menaces graves pour que soient disponibles des données utiles aux enquêtes pénales.
D'autre part, la distinction entre conservation et accès, que pose et consacre avec insistance la Cour, paraît neutralisée par le mécanisme de la conservation rapide. Le relai de la mesure procédurale des réquisitions judiciaires le montre parfaitement : par son intermédiaire, une injonction de conservation rapide peut être émise, de sorte que ce qui est fondamentalement un mode procédural d'accès (la réquisition) est commodément reconverti en mode de conservation ; par là-même et inversement, ce qui est un mode de conservation (la conservation rapide) se rapproche d'un mode d'accès. Plus exactement, l'accès qui n'est pas permis faute de poursuivre

[465] Décrets n° 2021-1363 du 20 octobre 2021 ; n°2022-1327 du 17 octobre 2022 ; n° 2023-933 du 10 octobre 2023 ; n°2024-901 du 7 octobre 2024.
[466] Points 53 et 54.
[467] Point 57.
[468] Et de la conservation facultative, point 57.
[469] Point 57.
[470] Crim., 12 juillet, n° 21-83.710, n° 21-83.820 et 21-84.096.

une finalité à la hauteur de celle qui peut justifier la conservation généralisée et indifférenciée, le devient grâce à la courroie de transmission que représente la conservation rapide, qui, sachant qu'elle peut porter sur l'ensemble des données conservées par ailleurs (par l'effet des obligations de conservation préventive et des facultés de conservation), permet quant à elle de poursuivre une finalité de moindre niveau, la lutte contre la criminalité grave, et ainsi ouvrir la voie à un accès à cette même fin.

C'est précisément par l'intermédiaire des « préférences système » ou options nationales que les interactions entre le droit de l'Union et le droit national nées de la rencontre entre le droit des données personnelles et l'enquête pénale sont susceptibles de provoquer une configuration qui dépasse le seul cadre de cette rencontre.

§2.- Au-delà de la donnée numérique pénale

221.- Tous les actes d'enquête, même ceux qui, objet de la présente recherche, sont tributaires (ou constituent) des technologies d'investigation ou de surveillance, ne relèvent pas du droit des données personnelles[471]. Cependant, le mouvement d'encadrement (définition de limites, conditions et bornes) qu'il implique produit des effets au-delà de son champ d'application car il impose d'y confronter les mesures qui lui échappent et qui ainsi se trouvent indirectement déterminées, en tout cas, affectées par lui.
Aussi, les appels divers appelant à la réécriture du Code de procédure pénale à partir de la « preuve numérique »[472] ou la « donnée numérique »[473] portent, conscients des effets en chaîne sur la procédure pénale, au-delà du numérique[474]. Prolongeant les constats des rendez-vous manqués du législateur avec l'ouverture d'une période de « reconstruction » [475] et de « réécriture » [476] du Code de procédure pénale pour lui « apporter une architecture cohérente »[477] et cesser d'alimenter « une sensation d'asphyxie procédurale »[478], le rapport sénatorial sur les données de connexion dans le cadre de l'enquête pénale souligne ainsi que « [l]'évolution de la législation sur ce sujet gagnerait de fait à s'inscrire dans le cadre de la clarification et la restructuration du Code de procédure pénale envisagée par le projet de loi d'orientation et de programmation du ministère de la Justice 2023-2027. Les rapporteurs considèrent en effet nécessaire qu'une véritable évolution du code de procédure pénale

[471] Voir par exemple s'agissant de la géolocalisation, l'applicabilité différenciée du droit des données personnelles (en particulier la directive 2002/58) selon qu'un dispositif de type balise est installé ou que le suivi en temps réel est assuré par l'intermédiaire d'un opérateur de communications électroniques, Crim., 27 février 2024, n° 23-81.061 ; SCHERER Théo, « Consécration de la dualité des régimes de géolocalisation par la chambre criminelle », *Dalloz Actualité*, 6 mars 2024. Toutefois, bien que la Cour de cassation n'en dise mot, l'inapplicabilité de la directive « Vie privée » n'épuise pas la question ; elle n'exclut pas notamment l'applicabilité de la directive « Police-Justice » si la pose de balise peut être ramenée à un traitement de données personnelles par l'autorité compétente…
[472] CANAYER Agnès et BONNECARRERE Philippe, *Rapport d'information sur les modalités d'investigation recourant aux données de connexion dans le cadre des enquêtes pénales*, Sénat, 15 novembre 2023 ; AUROY Benoît, « La preuve numérique en procédure pénale : un système à (re)construire », *D.* 2023, p. 697.
[473] VERGES Étienne, « La procédure pénale technicienne (ou l'asphyxie procédurale). Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice », *RSC* 2019, p. 667. MORNET Alice, « Vers un droit commun de la preuve numérique ? », *Lexbase Pénal*, *op.cit.*
[474] « En matière de procédure pénale, les données de connexion sont ainsi le reflet d'une désorganisation générale du droit de la preuve numérique », CANAYER Agnès et BONNECARRERE Philippe, *op. cit.*, p. 30.
[475] *Ibid*.
[476] *Ibid*.
[477] *Ibid*.
[478] *Ibid*.

intervienne, ce qui revient à s'inscrire dans un mouvement de réforme et non une simple refonte »[479].

222.- Parallèlement, à l'échelle de l'Union, les acteurs s'organisent et entendent peser sur les réformes en cours au niveau national et européen. En atteste, par exemple, la déclaration commune faite à Lisbonne le 30 mars 2023 par les responsables des services de police de vingt-six États membres[480] appelant à une évolution de la jurisprudence européenne. L'illustre plus encore l'installation d'un groupe d'experts de haut niveau en juin 2023 sous l'autorité conjointe de la Commission et du Conseil, « témoignant de la volonté de nombreux États membres de réévaluer les contraintes générées par les arrêts de la CJUE et de proposer un *nouveau cadre de réflexion* »[481]. En mai 2024, 42 recommandations sont publiées qui couvrent notamment les évolutions législatives suggérées (recommandations n° 25 à 42), lesquelles comprennent de manière significative l'adoption de règles minimales permettant l'admissibilité mutuelle des preuves (recommandation n°42), soit le point faible de la coopération judiciaire européenne et la clé de voûte des procédures pénales nationales, comme le révèlent les affaires nées du réseau de communication crypté, *EncroChat*[482].

Au stade où nous en sommes, c'est autour de deux principes cardinaux que semblent se cristalliser les besoins et propositions de réforme : la proportionnalité[483] d'une part qui innerve et fonde tout cadre et acte d'enquête[484], la garantie judiciaire[485] d'autre part, qui conditionne sa vérification et la sanction de son respect. A travers eux, ce sont notamment quatre questions[486] qui se dégagent et illustrent à la fois les limites ou l'inachèvement de la configuration nouvelle et les potentialités de celle-ci pour une recomposition plus large de la procédure pénale, toutes articulées autour de l'accès[487] aux éléments de preuve : celle du référentiel de proportionnalité qui doit réguler cet accès (*I*) et ainsi ordonner le régime des actes d'enquête, celle des contours du contrôle de cet accès (*II*), celle de la sanction des irrégularités entachant ce dernier (*III*) et, enfin, celle de l'information des intéressés de son existence (*IV*).

I.- La proportionnalité de l'accès aux éléments de preuve

223.- On l'a souligné, parmi les paramètres d'appréciation de la proportionnalité de l'accès figure en bonne place le critère de gravité. Celui-ci, selon qu'il qualifie – ou non – l'un des objectifs légitimes autorisant cet accès, modifie le type et les conditions d'un accès licite. Ainsi, la hiérarchie des objectifs légitimes poursuivis par une mesure d'enquête se conçoit au travers

---

[479] CANAYER Agnès et BONNECARRERE Philippe, *op. cit.*, p. 100.
[480] https://justica.gov.pt/Portals/0/Ficheiros/Confer%C3%AAncia%20PJ/Joint%20Declaration%20of%20the%20European%20Chiefs%20of%20Police%20FV.pdf
[481] CANAYER Agnès et BONNECARRERE Philippe, *op. cit.*, p. 13, souligné par nous.
[482] Voir en particulier le contentieux auquel il a donné lieu devant la CJUE (30 avril 2024, *M.N.*, aff ; C-670/22) ou devant la CEDH (*AL et EJ c. France*, req n° 44715/20 et 47930/21), ou encore devant les cours notamment constitutionnelles nationales (cf. références citées par l'avocat général Capeta dans l'affaire C-670/22 en note 4).
[483] Bien qu'il ne faille pas négliger la prévisibilité, soit l'exigence de prévision légale qui appelle à viser les actes innomés qui naissent de la pratique policière.
[484] « [C]lé de voûte de l'examen d'une mesure nationale de conservation ou d'accès à des données personnelles au titre » de l'art. 15§1 de la directive 2002/58, secondes conclusions de l'avocat général Szpunar présentées le 28 septembre 2023, point 42.
[485] C'est-à-dire la question tant de la place (en amont ou en aval) et le rôle (étendue et intensité) du contrôle des autorités judiciaires.
[486] Qui n'épuisent pas le sujet, loin s'en faut ; ainsi, par exemple la teneur et la portée du droit de ne pas s'auto-incriminer, au cœur par exemple de l'affaire *EncroChat* et sur laquelle à ce propos voir la décision d'irrecevabilité rendue par la CEDH (17 octobre 2024, précité).
[487] Qu'il soit direct ou indirect.

d'une échelle de gravité qui se précise avec la jurisprudence. Au sommet, la sauvegarde de la sécurité nationale inclut les infractions « plus que » (hyper ?) graves de terrorisme. Aux échelons suivants, se trouvent la criminalité grave puis la criminalité en général. Cette gradation dont les termes ne constituent pas des notions autonomes[488] s'apprécie *in abstracto*, à l'aide de critères objectifs tels que le quantum de la peine encourue qui ne doit pas être « excessivement bas », et *in concreto*, par l'intermédiaire de l'entité chargée du contrôle de l'accès[489]. Ce faisant, pèse sur les juridictions nationales un rôle qui n'est qu'en partie le leur et qui en tout état de cause paraît exclure toute approche générale (et prévisible). La jurisprudence de la Cour de cassation le montre depuis les arrêts de juillet 2022[490]. Celle de la Cour de justice l'illustre tout autant. Ainsi, dans l'arrêt relatif à la procédure de réponse graduée de la Hadopi, elle classe la contravention de « négligence caractérisée »[491] parmi les infractions pénales en général. Quant au délit de contrefaçon[492], elle estime qu'il est « loisible pour un État membre de considérer qu'un tel délit, en tant qu'il porte atteinte à un intérêt fondamental de la société, relève des formes graves de la criminalité »[493]. Et dans un autre arrêt du même jour, elle insiste sur la nécessité d'une vérification concrète par l'entité de contrôle, au cas par cas, de l'appartenance de l'infraction en cause à la criminalité grave[494].

224.- Dans le même ordre d'idées, l'invitation de l'avocat général Szpunar à l'adresse de la Cour d'aménager sa jurisprudence à la faveur de la question préjudicielle concernant la procédure Hadopi inclut aussi la question du critère de criminalité grave mais sous un autre regard. Il invitait à adjoindre à la dichotomie peu maniable car trop simple entre criminalité grave et criminalité en général un troisième terme : la criminalité en ligne (les infractions exclusivement constituées en ligne[495]), ce qui n'est pas sans faire écho aux diverses formes de reconnaissance en droit pénal et procédure pénale de la spécificité et de l'autonomie relatives de celle-ci, lesquelles signalent également une appréhension de la gravité au prisme de la difficulté dans laquelle se trouvent les autorités judiciaires pour en identifier les auteurs, et ce du fait même de la technologie. Si la Cour ne l'a pas suivi[496], elle accueille néanmoins les arguments soulignant la spécificité des infractions commises en ligne. Ainsi, l'accès à certaines données (en l'occurrence les adresses IP) peut constituer le seul moyen – ou le moyen le moins intrusif[497] – d 'investigation permettant l'identification effective de la personne à laquelle cette adresse était attribuée au moment de la commission de l'infraction[498]. Le risque d'impunité systémique des infractions pénales commises en ligne ou dont la commission ou la préparation est facilitée par les caractéristiques propres à Internet constitue une circonstance pertinente afin d'apprécier si une mesure est proportionnée au regard de l'objectif de lutte contre les infractions pénales[499].

---

[488] *Supra*, paragraphe 201.
[489] *Ibid*.
[490] Cette appréciation ne saurait s'effectuer au regard de la seule peine encourue et doit notamment s'effectuer « au regard de la nature des agissements de la personne poursuivie, du montant du préjudice qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue », cf. note explicative accompagnant les arrêts du 12 juillet 2022.
[491] Art. R.335-5 du Code de la propriété intellectuelle.
[492] Art. L.335-2 du Code de la propriété intellectuelle.
[493] CJUE (assemblée plénière), 30 avril 2024, C-470/21, point 146.
[494] CJUE (grande chambre), 30 avril 2024, C-186/22, point 60.
[495] Notamment premières conclusions de l'avocat général Szpunar présentées le 27 octobre 2022, points 78 et s ; secondes conclusions de l'avocat général Szpunar présentées le 28 septembre 2023, point 81.
[496] CJUE (assemblée plénière), 30 avril 2024, précité ; *supra* paragraphe 201.
[497] CJUE (assemblée plénière), 30 avril 2024, précité, points 120-121.
[498] CJUE (assemblée plénière), 30 avril 2024, précité, point 117.
[499] CJUE (assemblée plénière), 30 avril 2024, précité, point 119.

On pourrait encore envisager d'autres angles d'attaque, comme l'ampleur quantitative et non qualitative de la criminalité visée pour apprécier la proportionnalité de l'accès. Elle est en effet indirectement évoquée dans l'affaire relative à la procédure de la Hadopi, là où est abordée la possibilité d'un traitement automatisé des données en raison du « caractère massif des contrefaçons constatées sur les réseaux de pair à pair par les organismes d'ayants droit »[500].
Aussi bien, la réflexion est aussi appelée à s'enrichir et s'affiner à la faveur de la sophistication accrue de la typologie des données. Si l'évolution de l'appréhension des données de connexion a permis de prendre la mesure de leur potentiel intrusif, il n'est pas exclu que, numérisation et dataisation obligent, cette appréhension connaisse des infléchissements afin de prendre en compte l'avantage comparatif que ces données offrent lorsqu'elles constituent le seul point d'entrée pour la poursuite de certaines infractions ou permettent d'éviter le recours à des mesures plus attentatoires.

II.- Le contrôle préalable de l'accès aux éléments de preuve

225.- Quant au contrôle de l'accès, la position française est singulièrement délicate[501]. Tirant les leçons de l'arrêt *Prokuratuur*, la Cour de cassation a reconnu l'inaptitude du parquet à assurer le contrôle préalable requis pour autoriser l'accès aux données de trafic et de localisation, mais considéré que le juge d'instruction pouvait être épargné de cette critique[502]. Outre la solidité de cette dernière conclusion, c'est plus largement la question du contrôle de l'enquête qui est posée et la place (et partant les moyens) à cet égard du JLD[503].
Cela revient, dans le prolongement de réflexions doctrinales ou de travaux parlementaires[504], à interroger la distribution des pouvoirs de contrôle (*a priori et a posteriori*) entre les différents magistrats intervenant dans la procédure. C'est notamment envisager non seulement la perspective d'un véritable juge des libertés ou juge de l'enquête, contrôlant l'ensemble des mesures de contraintes ou des mesures probatoires attentatoires à la vie privée[505] susceptibles d'être prises au cours de l'enquête. Mais c'est aussi, et peut-être surtout, repenser les conditions de possibilité du déploiement d'une telle fonction, car la question du « comment contrôler ? » est au moins aussi importante que celle du « qui contrôle ? »[506]. Or, si la relative jeunesse de cet acteur procédural et l'ambiguïté, persistante sinon entretenue, de sa place, expliquent sans doute la difficile et incertaine mue d'un « juge spécialisé » [507] en « juge des libertés » [508], il n'en demeure pas moins qu'apparaît de manière toujours plus manifeste l'incohérence (voulue ou tolérée) qu'il y a à lui confier des pouvoirs supposés conditionner sinon totalement en tout cas largement la légitimité de dispositifs procéduraux fortement attentatoires aux droits et libertés et à refuser de lui en donner les moyens[509].

---

[500] CJUE (assemblée plénière), 30 avril 2024, précité, point 154.
[501] Sur le cas très particulier mais instructif de la procédure de réponse graduée de la Hadopi, voir les points 123 et suivants de l'arrêt rendu dans l'affaire C-470/21.
[502] Crim., 12 juillet 2022, 21-83.820, §§ 13 et 23.
[503] VERGES Etienne, « Quel juge pour contrôler les atteintes aux libertés ? », *Droit pénal* n° 5, Mai 2023, dossier 6. Voir aussi les constats et les propositions formulés dans le Rapport du Sénat précité, not. p. 102 et s.
[504] CANAYER Agnès et BONNECARRERE Philippe, *op. cit.*, p. 101 et s.
[505] VERGES Etienne, « Quel juge pour contrôler les atteintes aux libertés ? », *Droit pénal* n° 5, Mai 2023, dossier 6. Voir aussi les constats et les propositions formulés dans le Rapport du Sénat précité, not. p. 102 et s.
[506] CANAYER Agnès et BONNECARRERE Philippe, *op. cit.*, p. 108.
[507] VERGES Etienne, « Quel juge pour contrôler les atteintes aux libertés ? », *Droit pénal* n° 5, Mai 2023, dossier 6. Voir aussi les constats et les propositions formulés dans le Rapport du Sénat précité, not. p. 102 et s.
[508] *Ibid*.
[509] Voir à ce propos, *supra*, première et deuxième parties quant aux limites actuelles du contrôle et, en termes prospectifs, CANAYER Agnès et BONNECARRERE Philippe, *op. cit.*, p. 104.

III.- La sanction d'un accès irrégulier aux éléments de preuve

226.- La question de la sanction procédurale de l'accès irrégulier (ou, en amont, celle de la conservation illicite) est, on l'a vu, largement laissée aux mains des procédures et des juges nationaux. La Cour de cassation ne s'y est pas trompée, allant selon certains auteurs « à reprendre d'une main ce qu'[elle] a donné de l'autre »[510] : la consécration de la contrariété du droit français au droit de l'Union est presque dépourvue de portée concrète, le régime des nullités permettant de neutraliser au cas par cas l'illicéité constatée de l'accès. Mais, outre la question d'une éventuelle dénaturation[511] du contrôle de légalité, tel qu'il résulte du contrôle de conventionnalité du droit interne et tel qu'il découle du régime des nullités, c'est plus largement ce dernier dans son ensemble qui se trouve mis en cause.
Sans doute, rabattre la contradiction au droit de l'Union (soit une question de légalité entendue comme l'exigence du respect de la hiérarchie des normes) sur la théorie des nullités laisse sceptique[512]. Les représentants de la conférence nationale des procureurs, auditionnés par les sénateurs Canayer et Bonnecarrère, ne disent pas autre chose lorsqu'ils insistent « sur la position délicate dans laquelle ces décisions les placent, en les autorisant implicitement à continuer à requérir des données de connexion tout en jugeant expressément qu'une telle pratique n'est pas conforme au droit. Ces magistrats y voient à la fois une source d'insécurité juridique et une négation des termes de leur serment » [513].
« L'irrégularité attachée à la contrariété d'une réquisition avec le droit de l'UE ne trouve pas, en effet, sa source dans une transgression de la loi interne, mais dans le fait que l'application littérale de cette loi est, en raison du contenu de celle-ci, incompatible avec des normes qui lui sont hiérarchiquement supérieures. Aussi, l'irrégularité ne réside pas, au sens de l'article 802 du Code de procédure pénale, dans une violation d'une forme prescrite par la loi à peine de nullité ou une inobservation de formalités substantielles sanctionnable par la nullité, dans la mesure où la loi interne, qui est incompatible avec le droit de l'UE, a été respectée »[514]. Comme le souligne un auteur, la contrariété (du fait de l'illégalité, ici l'inconventionnalité) implique sans autre condition, partant sans la preuve d'un grief, la mise à l'écart de la norme incompatible. Or un acte de procédure fondé sur une loi incompatible avec le droit de l'Union et pour cette raison immédiatement inapplicable ne devrait-il pas suivre le même sort ?
Cela étant, il faut reconnaître que la Cour de justice, dans un même élan, rejette le maintien des effets d'une législation incompatible avec le droit de l'Union et restreint, par le renvoi qu'elle organise au droit interne, les conséquences d'une telle incompatibilité sur l'exploitation en procédure pénale d'éléments de preuve recueillis en vertu d'une telle législation.

227.- Même envisagée dans le cadre et au nom du régime des nullités, la solution retenue par la Chambre criminelle peine à convaincre. Plus justement peut-être, elle met en lumière les faiblesses de ce régime, le droit des données personnelles confirmant de nouveau ses vertus révélatrices des faiblesses de la procédure pénale[515] et des perspectives d'une recomposition de celle-ci. Ainsi la requête en annulation a-t-elle vraiment ou seulement pour fondement la protection de la vie privée du requérant ? Ce fondement ne réside-t-il pas plutôt « dans l'exercice du droit à un recours effectif destiné à vérifier la légalité d'actes coercitifs à son

---

[510] BOTTON Antoine, *Aperçu rapide, JCP G n° 38 du 26 septembre 2022.*
[511] Voir aussi OLLARD Romain, « Un an de droit pénal numérique », *Droit pénal*, 2022, n° 12, chr. 12, sp. n°12.
[512] MESA Rodolphe, « Conservation et exploitation des données électroniques dans l'enquête et l'instruction / droit de l'Union européenne », Gazette du Palais, 2022, n° 38, p. 16 et s, sp. p. 19.
[513] CANAYER Agnès et BONNECARRERE Philippe, *op. cit.*, p. 93.
[514] *Ibid*.
[515] Voir à cet égard, BUISSON Jacques, « La requête en annulation : le droit à un recours effectif quelque peu malmené ? », *Procédures*, 2022, n°11, étude 12.

encontre, la protection des droits du citoyen dans l'administration de la preuve pénale, singulièrement les droits du procès équitable »[516] ? D'autant qu'il se peut en effet que l'acte critiqué n'emporte aucune atteinte dans sa vie privée mais mette en péril ses droits au procès équitable ; hypothèse que vise justement la réserve finale[517] de la Cour de justice qui impose la mise à l'écart d'un moyen de preuve au nom de la violation du droit à un procès équitable dans la situation où une partie ne serait pas en mesure de le commenter efficacement, alors qu'il ressortit à un domaine échappant à la connaissance des juges et est susceptible d'influencer de manière prépondérante l'appréciation des faits. « En sorte que la question posée (…) est celle non pas de savoir si [l]a vie privée [de l'intéressé] a été méconnue mais de déterminer si les indices recueillis à son encontre, qui l'impliquent dans le dossier en cause, ont été légalement recueillis. La question est d'importance car elle gouverne la qualification de la nullité en cause : d'ordre public ou non »[518]. Or, la compétence relève en principe des normes d'ordre public, si bien que l'incompétence de l'agent – en l'occurrence le ministère public ou l'officier de police judiciaire – rend l'acte nul, indépendamment de la question de savoir si un grief peut être établi, si une atteinte à la vie privée peut être démontrée, l'acte attentatoire à la vie privée accompli par une autorité qui n'était pas compétente portant nécessairement atteinte aux intérêts du requérant. Mais la solution n'est plus pleinement assurée depuis que la Cour de cassation distingue entre les réquisitions en vue de procéder à des examens techniques et scientifiques (pour lesquelles cette solution est maintenue) et celles adressées à personne pour l'obtention d'informations intéressant l'enquête, désormais rétrogradées au rang de nullité d'ordre privé[519].

228.- En tout état de cause, de nouveau, le raisonnement de la chambre criminelle neutralise les conséquences de l'incompatibilité (et partant l'incompatibilité elle-même[520]) du droit français et de sa mise en œuvre en l'espèce avec le droit de l'Union : « l'acte attentatoire à la vie privée accompli par un agent compétent mais sans le contrôle d'un tiers alors que celui-ci était prévu par la loi ne porte pas nécessairement atteinte aux intérêts de la personne ». Or, déduire de l'objet de la mesure (l'accès aux données de connexion) l'atteinte exclusive d'un intérêt privé occulte sinon brise le lien entre les qualités de l'autorité habilitée à exercer un contrôle et la bonne administration de la justice[521]. Surtout, la distinction entre l'incompétence qui permet à tout le moins de présumer le grief mais qui s'agissant du ministère public en enquête préliminaire ou de l'officier de police judiciaire agissant en flagrance n'est pas établie et le défaut de contrôle par un tiers des autorités compétentes, qui, lui, suppose la preuve d'un grief laisse perplexe. Une autrice l'énonce parfaitement :« Peut-on cependant affirmer qu'une autorité ne réunissant pas les qualités requises par une norme supérieure pour réaliser le contrôle attendu demeure encore compétente ? Peut-on, semblablement, admettre que l'irrégularité tient au fait que ladite autorité, prétendument compétente, a agi sans le contrôle préalable d'une juridiction ou d'une entité administrative indépendante alors que ledit contrôle n'a pas été prévu ? La circularité du raisonnement frappe tant la sanction attachée à la légalité formelle de la mesure – absence de contrôle préalable – devient tributaire d'une atteinte à la légalité matérielle [puisque selon la Cour] l'existence d'un grief pris de l'absence d'un tel contrôle est établie si l'accès aux données de trafic et de localisation a méconnu les conditions matérielles posées par le droit de l'Union »[522]. C'est donc dire que l'absence de contrôle préalable peut être

---

[516] *Ibid.*, n°15.
[517] Voir supra, dans cette partie, Section 2, §1, II.A. 4).
[518] BUISSON Jacques, « La requête en annulation : le droit à un recours effectif quelque peu malmené ? », *op.cit.*, n°15.
[519] GOGORZA Amane, « L'accès aux données de connexion : les affres du pluralisme normatif », *Droit pénal* n° 10, octobre 2022, étude 20, n° 7.
[520] Voir aussi OLLARD Romain, « Un an de droit pénal numérique », *Droit pénal* n° 12, 2022, chr. 12, sp. n°12.
[521] GOGORZA Amane, « L'accès aux données de connexion : les affres du pluralisme normatif », *Droit pénal* n° 10, octobre 2022, étude 20.
[522] *Ibid*.

compensée par un contrôle *a posteriori* révélant que la conservation et les autres conditions de l'accès aux données étaient en l'occurrence conformes au droit de l'Union.
Or, une telle conclusion est précisément et explicitement écartée par la Cour de justice (*supra*), ce qui devrait conduire au contraire à reconsidérer la théorie des nullités et à poser que le fait d'être privé de la garantie d'un contrôle préalable « fait nécessairement grief dans la mesure où, d'une part, tout rôle prophylactique de la règle s'en trouve confisqué et que, d'autre part, rien ne garantit une identité d'appréciation entre les autorités chargées de procéder au contrôle *a priori* et *a posteriori*. Prétendre le contraire revient à mettre en cause l'essence même du contrôle préalable et d'une certaine manière, la nature de sa violation »[523].
Pourtant si, comme beaucoup le pressentent ou l'espèrent, c'est au JLD que reviendra le contrôle[524], alors il apparaît qu'effectivement le procureur ou éventuellement l'OPJ en flagrance sera bien l'autorité compétente pour demander l'accès à l'autorité de contrôle (le JLD) et l'obtenir effectivement si l'autorisation est donnée, voire la devancer en cas d'urgence.

IV.- L'information sur l'accès aux éléments de preuve

229.- L'information sur l'accès est encore l'objet de trop peu d'attention. Comme le note Maxime Lassalle, « la question des droits à une notification et à un recours est négligée »[525].
Pourtant, la CJUE, comme la CEDH, exige que les personnes concernées par des mesures secrètes en soient informées et bénéficient de voies de recours contre les mesures portant atteinte à leur droit à la vie privée[526].
Dans le premier arrêt *La Quadrature du Net* rendu par la Cour de justice, le droit à l'information était en particulier attaché au recueil en temps réel des données relatives au trafic et des données de localisation[527]. La Cour soulignait que « cette information est, de fait, nécessaire pour permettre à ces personnes d'exercer leurs droits, découlant des articles 7 et 8 de la Charte, de demander l'accès à leurs données à caractère personnel faisant l'objet de ces mesures et, le cas échéant, la rectification ou la suppression de celles-ci, ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte, un recours effectif devant un tribunal, un tel droit étant d'ailleurs explicitement garanti à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 79, paragraphe 1, du règlement 2016/679 »[528].
Dans la décision précitée rendue le 4 octobre 2024, à propos de l'accès direct et partant de la directive « Police-justice », elle affirme « qu'il incombe aux autorités nationales compétentes ayant été autorisées, par un juge ou une entité administrative indépendante, à accéder aux données conservées d'informer les personnes concernées, dans le cadre des procédures nationales applicables, des motifs sur lesquels cette autorisation repose, dès le moment où cela n'est pas susceptible de compromettre les enquêtes menées par ces autorités »[529].
La question n'est pas propre aux seules mesures d'enquête attentatoires au droit à la protection des données personnelles et interroge au-delà la complétude des régimes applicables aux actes d'enquête, mais aussi l'articulation avec certains critères traditionnels de confection de ces régimes, tels que la coercition.

---

[523] *Ibid*.
[524] CANAYER Agnès et BONNECARRERE Philippe, *op. cit.*, p. 101 et s.
[525] LASSALLE Maxime, « La mue des réquisitions, signe avant-coureur d'une transformation plus large ? », *AJ Pénal*, 2023, n° 11, p. 491.
[526] CJUE, 21 décembre 2016, *Tele2*, aff. C-203/15 et C-698/15, point 121.
[527] Arrêt précité, point 190.
[528] *Ibid*.
[529] Affaire C-548/21, précitée, point 120.

Surtout, elle ajoute et s'ajoute au besoin général – des acteurs, des textes ou des observateurs – qui traverse la recherche d'une vision globale sur l'empire et l'emploi des nouvelles technologies d'investigation et de surveillance.

Conclusions

230.- Une vision globale manque, en effet.

Elle manque d'abord aux acteurs eux-mêmes : du mis en cause ou son avocat lorsque les conditions du recueil du matériel probatoire ou pré-probatoire sont couvertes par le secret[530] ou lorsqu'il ignore l'existence même de la mesure, en passant par l'enquêteur ou le magistrat chargé de le contrôler qui peinent à maîtriser un cadre juridique toujours plus complexe et ce faisant incertain ou instable, jusqu'au juge supranational dont la lucidité inquiète l'oblige à reconnaître que « pour se prononcer sur la conformité à la Convention des régimes encadrant dans les États contractants l'interception en masse, technologie précieuse qui permet de détecter les nouvelles menaces de nature numérique, la Cour est appelée à examiner les garanties contre l'arbitraire et les abus qui y sont prévues *tout en ne disposant que d'informations limitées sur la manière dont ils fonctionnent* » [531].

Elle manque ensuite aux rédacteurs des textes, dont la confection témoigne d'une insuffisante maîtrise de la technique légistique propre à la construction de la norme de procédure pénale alors « paradoxalement » qu'elle repose sur un excès par multiplication ou empilement de règles techniques[532] et de régimes particuliers qui alourdissent la charge pesant sur les acteurs de l'enquête[533].
Sans doute est-ce parce que les principes n'ont pas encore trouvé leur place et ne parviennent pas encore à jouer leur rôle directeur et régulateur. Sans doute plus largement parce que les « systèmes » de référence sont multiples – technologiques et juridiques – et multiscalaires – nationaux, européen(s) voire internationaux, ou plus largement globaux, ce qui n'est pas sans ajouter au paradoxe de constructions politiques et juridiques parcellaires ou morcelées d'objets pourtant globaux ou globalisés et globalisants.

On comprend enfin qu'une vision d'ensemble manque aussi aux observateurs et aux chercheurs.
231.- Sans doute, la présente recherche n'en propose-t-elle pas encore une.
Toutefois, par différentes propositions et innovations de recherche, elle s'emploie à dégager les instruments et analyses – cartographie[534], glossaire[535], observations empiriques[536], généalogie

---

[530] Voir à ce propos le volet *EncroChat* devant la CJUE et la CEDH (décisions précitées), en particulier s'agissant des inquiétudes exprimées (mais pour l'heure sans réponse autre que l'invocation de la garantie du droit à un procès équitable) quant à l'intégrité des données obtenues par une mesure d'interception qui ne peut pas être vérifiée en raison d'une confidentialité étendue (secret défense) quant aux modalités techniques de réalisation de l'interception.
[531] CEDH, 25 mai 2021, *Big Brother Watch e.a c. Royaume-Uni*, requêtes n° 58170/13, 62322/14 et 24960/15, §323 (nous soulignons).
[532] Au sens du modèle procédural dessiné par Etienne Vergès in « Construire la norme en procédure pénale : une étude des techniques juridiques à travers un cas symptomatique, la géolocalisation », *RSC*, 2014, p. 599.
[533] Voir aussi CANAYER Agnès, BONNECARRERE Philippe, *op.cit.*, p. 23 ou 108.
[534] *Supra*, en fin de première partie.
[535] *Infra*.
[536] *Supra*, première partie.

[537]et comparaisons[538] normatives, contextualisations[539] – permettant d'équiper et de doter les uns et les autres des moyens à cette fin, autrement dit de dégager les conditions ou coordonnées systémiques d'une / de mise en cohérence d'ensemble.

232.- Dans le prolongement de cette démarche, nécessairement inachevée et donc incomplète, tant le processus de construction est lui-même inabouti et se cherche encore, il convient en guise de conclusions provisoires de mettre en exergue ce qui, resté à l'arrière-plan de la présente recherche, devrait alimenter celles qui suivront et aider à faire advenir cette vision globale qui nous fait encore défaut : l'enjeu de la surveillance privée ou plus justement de l'articulation des surveillances publiques et privées.

Cette vision d'ensemble manquante est naturellement au cœur de l'édification du régime de conservation et d'accès aux données de connexion[540]. Ce dernier ne se conçoit et ne se comprend qu'à l'aune de la dépendance dans laquelle se trouvent les mesures et les acteurs de l'enquête vis-à-vis de tiers, qui sont des opérateurs privés transnationaux, généralement hyper-puissants.

C'est ainsi que l'accent sur la conservation obligatoire[541] ne doit pas occulter l'importance de la conservation facultative[542] des données en tant que gisement[543] ou réservoir[544] de données numériques pénales.

Elle est aussi dépendante d'une vision transnationale de l'enquête pénale, ainsi que l'illustre l'affaire *EncroChat*[545], dont les premiers, mais sans doute nombreux autres, contentieux se font jour[546] et devraient très probablement participer à l'élaboration de la vision d'ensemble qui se dérobe encore.

Elle est encore plus largement l'enjeu de l'articulation entre logique trans- ou supra- nationale de marché et logique également trans- ou supra- nationale de droits humains, comme l'illustre une autre affaire pendante devant la CJUE[547], sur questions préjudicielles posées par le Conseil d'État le 6 mars 2024[548] qui confronte la libre circulation des services numériques et notamment le principe dit du pays d'origine, tel que notamment « protégé » par la CJUE elle-même au risque du *forum shopping*[549], et la protection des droits des victimes mineures exposées à des contenus illicites, en particulier pornographiques. Cette affaire signale notamment combien la

---

[537] *Supra*, Deuxième partie, §1.
[538] *Supra*, Deuxième partie, §2.
[539] *Supra* Troisième partie, Section 1.
[540] *Supra*, Troisième partie, Section 2, §1.
[541] *Supra*, Troisième partie, II, A), 2), a).
[542] *Supra*, Troisième partie, II, A), 2), b).
[543] CANNAYER Agnès, BONNECARRERE Philippe, *op. cit.*, p. 27.
[544] *Supra*, Troisième partie, II, A).
[545] Voir l'affaire C-670/22, devant la grande chambre de la CJUE, à propos de la décision d'enquête européenne émise par un parquet allemand en vue de disposer des données interceptées par les autorités françaises. L'avocat général Capeta a présenté ses conclusions le 26 octobre 2023, l'arrêt a été rendu le 30 avril 2024. Parallèlement, la CEDH a rendu un (premier ?) arrêt d'irrecevabilité (à raison du défaut d'épuisement des voies de recours internes) concernant la France sur cette affaire aux contentieux multiples en Europe : 17 octobre 2024, *A.L. et E.J. contre France*, requêtes n°44715/20 et n°47930/21.
[546] *La preuve transfrontière*, Grand'Chambre de la Cour de cassation, 1er juin 2023, https://www.courdecassation.fr/agenda-evenementiel/la-preuve-transfrontiere
[547] C-188/24.
[548] Décision n° 461193 et 461195, *société WebGroup Czech Republic et autre* et décision n° 453763, *société Coyote System*.
[549] CJUE, 9 novembre 2023, *Google Ireland*, aff. C-376/22.

surveillance privée est appelée à être toujours davantage mobilisée -sinon enrôlée- par les pouvoirs publics afin de concourir à la poursuite d'objectifs d'intérêt général : la contribution à l'enquête au travers du concours contraint à la détection des infractions se double d'une contribution à la répression, voire plus largement encore à la prévention et à l'orientation des conduites, dans le droit fil du développement d'un droit de la conformité[550].

233.- La prise en compte de l'enjeu de la surveillance privée, enjeux propres et conjugués à ceux de la surveillance publique, ne vise pas seulement à rééquilibrer la crainte qu'inspirent davantage « les États pourtant garants de l'intérêt général, [plutôt] que les géants du numérique dont la puissance concurrence celle des autorités publiques et qui font des données qu'ils collectent un usage extrêmement intrusif qui, loin de se cantonner à la sphère mercantile, peut avoir un impact non seulement sur les choix de consommation des individus mais aussi sur les délibérations politiques d'un pays »[551].

Elle vise surtout à alerter sur la nécessité de concevoir les surveillances ensemble, globalement, dans leurs rapports avec la procédure pénale, ce que le concept de compte global de surveillance[552] pourrait aider à penser et que l'on pourrait imaginer de décliner à l'échelle d'une société donnée pour accompagner le législateur lors de la conception de la norme procédurale ou le juge au moment de l'interpréter mais aussi à l'échelle d'une procédure pénale donnée pour permettre aux acteurs d'opérer de manière raisonnée et raisonnable, donc mesurée, proportionnée.

[550] FRISON-ROCHE Marie Anne, DUFOUR Olivia, « You porn : La CJUE face au défi de la protection des mineurs », Actu-Juridique, 11 mars 2024, https://www.actu-juridique.fr/id/AJU426197.
[551] CANNAYER Agnès, BONNECARRERE Philippe, *op. cit.*, p.24.
[552] *Supra*.

Annexes

- Liste des entretiens
- Questionnaire type
- Journées d'études (programmes)
- Synthèse comparative des mesures
- Glossaire

Liste des entretiens

Entretien n° 1 : 17 janvier 2022

Magistrat
Mission de Prévention et de Lutte contre la Cybercriminalité

Entretien n° 2 : 31 janvier 2022

Officier de police
Brigade criminelle

Entretien n° 3 : 14 février 2022

Magistrat
JIRS JUNALCO

Entretien n° 4 : 14 février 2022

Lieutenant-Colonel
Officier de liaison cyber-gendarmerie
JUNALCO

Entretien n° 5 : 2 novembre 2022

Secrétaire général
Groupe privé, expert des technologies d'investigation et des services pour la sécurité globale.

Entretien n° 6 : 10 novembre 2022

Avocat – Spécialité droit pénal

Entretien n° 7 : 16 novembre 2022

Major
Chef de groupe des Enquêteurs en Nouvelles Technologies
Section Opérationnelle de Lutte contre les Cybermenaces BDRIJ

Entretien n° 8 : 17 octobre 2023

Avocat – spécialité libertés publiques

Entretiens n° 9-10-11 : 22 novembre 2023

Magistrats (JLD)

Entretien n° 12 : 30 novembre 2023

Brigadier-Chef de Police
Officier de Police Judiciaire
Investigateur en cybercriminalité

Questionnaire type

Principes et pratiques de l'enquête pénale
à l'épreuve des nouvelles technologies d'investigation et de surveillance (NTIS)

1. Présentation de la recherche

Réponse à un appel à projets lancé par le GIP Mission Droit et Justice, devenu l'IERDJ (Institut des Études et de la Recherche sur le Droit et la Justice), la recherche commencée en janvier 2021 est dirigée par Florence Bellivier et Juliette Tricot. Elle est conduite par une équipe de 12 chercheurs.

La recherche a pour objectif d'interroger l'usage des techniques (technologies) d'investigation et de surveillance[553] dans le cadre de la procédure pénale à titre principal (et dans le domaine du renseignement à titre complémentaire).
A cette fin, la recherche entend s'appuyer sur l'analyse des pratiques (à partir d'entretiens).

2. Questionnaire

Questions d'ordre général

I/ Fonctions

1. Quelles sont vos fonctions aujourd'hui ?

2. Depuis quand occupez-vous ce poste ?

3. Quelles fonctions avez-vous exercé auparavant ?

553

- Interception des correspondances émises par la voie des communications électroniques
- Fixation d'images de certains lieux et véhicules
- Réquisition de documents
- Injonction de donner un mot de passe
- Sonorisation de certains lieux et véhicules
- Accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique
- Infiltration numérique
- Géolocalisation
- Captation des données informatiques
- Perquisition informatique
- *IMSI-catcher*
- Conservation rapide de données informatiques stockées
- Saisie de données informatiques stockées

II/ NTIS

4. Qu'évoque pour vous la formule « technologies ou techniques d'investigation et de surveillance » ?

5. Avez-vous / êtes-vous amené à en faire usage ?

Si oui
- à quelle fréquence ?
- quelles sont / ont été les mesures prévalentes ?

6. Quelle place ou part occupent selon vous ces mesures ou certaines d'entre elles dans une enquête pénale « lambda » aujourd'hui ?

7. La place actuelle de ces mesures est-elle un fait récent ou ancien ?

8. Selon votre expérience, quelles sont les dates/moments clés qui y ont conduit ?

9. Qu'a changé selon cette nouvelle donne pour les acteurs de l'enquête pénale ?

Données statistiques / mesure de l'emploi

1. Existent-ils des données statistiques concernant l'emploi de ces mesures ou certaines d'entre elles ?

- Volume
- Domaines
- Acteurs
- Coûts

2. Quelles sont les mesures les plus utilisées ?

3. Quelles sont les mesures les moins utilisées ?

4. Ce constat a-t-il évolué ?
5. Certaines mesures auparavant très utilisées ont-elles été « remplacées » par d'autres ?

6. Certaines ont-elles été frappées d'obsolescence ?

7. Selon les mesures, peut-on parler d'usages routiniers, ponctuels ou exceptionnels voire rares ?

8. Existent-ils des données statistiques concernant l'impact des mesures sur l'enquête et l'issue de la procédure ?

9. D'après votre expérience, le développement de ces mesures a-t-il produit des effets inattendus sur la procédure pénale en général et sur l'enquête en particulier ?

Questions particulières sur certaines mesures :

1. Comment se déroule très concrètement la mesure étape par étape ?
- L'intervention d'un seul ou de plusieurs acteurs est-elle nécessaire ?
- Combien et lesquels ?
- Comment se déroule l'intervention de tiers ?
    - Y a-t-il des craintes à propos de l'intégrité des éléments de preuve recueillis ou conservés par les experts du privé ?

2. Quelles compétences sont requises ?

Sont-elles largement partagées ou spécialisées ?

3. Quels équipements sont requis

Sont-ils largement disponibles ?

Questions sur les obstacles/ freins :

1. Quelles sont les obstacles à l'emploi des mesures ou de certaines d'entre elles ?

2. Ces obstacles sont-ils plutôt techniques ou juridiques ou les deux ?

3. Parmi les obstacles ou contraintes techniques quels sont ceux qui vous semblent
- les plus importants ?
- les moins importants
- dépassables ? comment ?

4. Parmi les obstacles ou contraintes juridiques quels sont ceux qui vous semblent
- les plus importants ?
- les moins importants
- dépassables ? comment ?

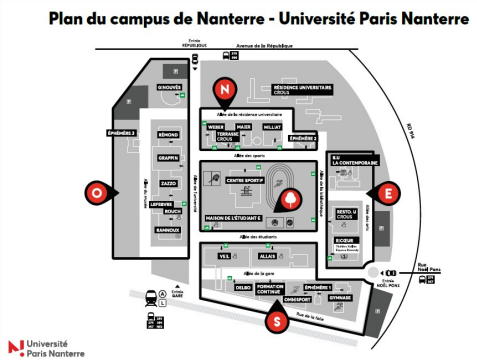
5. Quel est votre avis sur les dernières évolutions de la jurisprudence de la CJUE ?

6. Quel est votre avis sur l'avenir de ces mesures et de l'enquête pénale ?

Journées d'études

Université Paris Nanterre

cd·pc



Accès : RER A (Station Nanterre Université).

Centre de droit pénal et de criminologie (CDPC)
Bâtiment Veil
4ème étage - Salle 417
https://cdpc.parisnanterre.fr/accueil/

Université Paris Nanterre
200 avenue de la République
92001 Nanterre Cedex
www.parisnanterre.fr

Université Paris Nanterre

cd·pc

Principes et pratiques de l'enquête pénale à l'épreuve des nouvelles technologies

(Projet NTIS)

Journée d'études

Réceptions comparées de la jurisprudence européenne sur la conservation et l'accès aux données en procédure pénale

Lundi 3 avril 2023
8h30 – 18h

Teams. Code équipe : 2jswt0k

Bâtiment Max Weber

Avec le soutien financier de l'Institut des Études et de la Recherche sur le Droit et la Justice

Institut des Études et de la Recherche sur le Droit et la Justice

Université Paris Nanterre

cd·pc

8h30 : Accueil-café

9h-9h15 : Mots de bienvenue

9h15-9h45 : **La réception en Belgique**
Vanessa Franssen, Université de Liège

9h45-10h : Discussion

10h-10h30 : **La réception en Italie**
Michele Caianiello, Université de Bologne
Giulia Lasagni, Université de Bologne

10h30-10h45 : Discussion

10h45-11h : Pause

11h-11h30 : **La réception en Allemagne**
Benjamin Vogel, Max Planck Institute for the Study of Crime, Security and Law

10h30-10h45 : Discussion

11h45-12h15 : **La réception en Irlande**
TJ McIntyre, University College Dublin

12h15-12h30 : Discussion

12h30-14h15 : Déjeuner (Restaurant VIP).

Université Paris Nanterre

cd·pc

14h30-15h45 : **La réception en France**
Myriam Benlolo-Carabot, Université Paris Nanterre, Maître des requêtes en service extraordinaire au Conseil d'État
Frédéric Desportes, premier avocat général à la chambre criminelle de la Cour de cassation
Thibault Douville, Université de Caen

15h45-16h15 : Discussion

16h15-16h30 : Pause

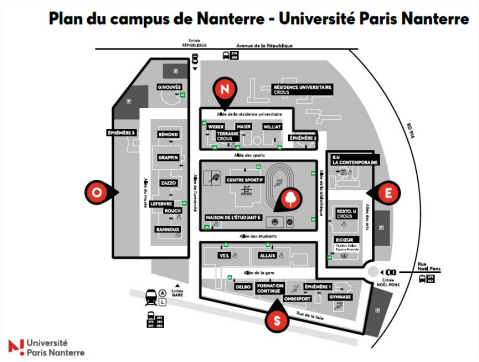
16h30-17h30 : **Mise en perspectives**
Benoit Dupont, Université de Montréal
Etienne Vergès, Université de Grenoble.

17h15-17h45 : Discussion

18h : Fin des travaux

Université Paris Nanterre

cd·pc



Accès : RER A (Station Nanterre Université).

Centre de droit pénal et de criminologie
(CDPC)
Bâtiment Veil
4ème étage - Salle 417
https://cdpc.parisnanterre.fr/accueil/

Université Paris Nanterre
200 avenue de la République
92001 Nanterre Cedex
www.parisnanterre.fr

Université Paris Nanterre

cd·pc

Principes et pratiques de l'enquête pénale à l'épreuve des nouvelles technologies

(Projet NTIS)

Journée d'études

Que font les NTIS à l'enquête pénale ?

Échanges avec
Silvia Allegrezza (Université du Luxembourg
Laurent Bonelli (Université Paris Nanterre)
Raphaële Parizot (Université Paris I)

Et les professionnels sollicités au cours de la recherche

Vendredi 19 janvier 2023
8h30 – 18h

Avec le soutien financier de l'Institut des Études et de la Recherche sur le Droit et la Justice

Institut des Études et de la Recherche sur le Droit et la Justice

Université Paris Nanterre

cd·pc

Université Paris Nanterre

cd·pc

Que font les NTIS à l'enquête pénale ?

Matinée – Bâtiment de la formation continue-salle 402

9h15 *Accueil*

9h30-9h45 *Introduction*
par Florence Bellivier : définition, champs et hypothèses

I.- Pratiques

9h45-11h45 *Cartographie des acteurs*
par Sophie Sontag-Koenig et Antonin Guillard :
Discussion

11h-11h15 *De nouveaux métiers*
par Vissarion Giannoulis
Discussion et pause-café : (15 mn)

11h30-12h *L'articulation des techniques et des technologies : une question de mesure(s)*
par Florence Bellivier
Discussion générale :12h-12h45

Déjeuner au VIP

Après-midi – Bâtiment Max Weber – Salle de séminaire 2

II.- Principes

14h30-15h15 *Déstabilisation des repères*
par Juliette Tricot
Discussion : 15 minutes

15h30-16h15 *Reconfiguration à partir du droit des données personnelles ?*
Hypothèse, Juliette Tricot
Morceaux choisis, Vissarion Giannoulis
Discussion : 15 minutes
Pause

16h30 Conclusions-discussions : Limites de la configuration

17h30 : fin des travaux

Synthèse comparative des mesures

Les techniques d'enquête numérique judiciaire

Nota : Le caractère insusceptible de recours est sans préjudice des requêtes en nullité fondées sur l'insuffisance des mentions légalement requises dans la décision autorisant la mesure ou sur le dépassement de celles-ci lors de l'exécution de celle-là.

Perquisitions informatiques

Définition
Accéder, lors d'une perquisition « classique », sur les lieux de la perquisition, à un système informatique trouvé sur place (ex. un ordinateur), aux données qui y sont stockées et au-delà, à celles qui, délocalisées dans un autre système localisable (possiblement à l'étranger) peuvent être accessibles à distance depuis ce système informatique (dit initial), art. 57-1 al. 1 ; ou accéder à distance, depuis les locaux d'un service ou d'une unité de police ou de gendarmerie, via le système informatique appartenant aux enquêteurs, à des données stockées dans un autre système informatique que celui de l'intéressé, si ces données « sont accessibles depuis le système informatique initial », art. 57-1 al. 2.

Cadre légal
Renvoi au cadre légal des perquisitions « classiques » : art. 56 s. pour l'enquête de flagrance, 76 pour l'enquête préliminaire, 94 s. pour l'instruction et 706-88 s. en matière de criminalité organisée.
Si les données sont stockées à l'étranger, les enquêteurs doivent respecter les engagements internationaux (ex : conv. de Budapest), art. 57-1 al. 3.
Les OPJ et APJ peuvent requérir par tout moyen toute personne susceptible d'avoir connaissance des mesures protégeant les données ou de leur remettre les informations permettant d'y accéder.
Nota : le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni de 3750 euros d'amende

Infractions concernées
V. Régime applicable aux perquisitions judiciaires

Type de décision
Décision des OPJ ou, sous leur responsabilité APJ, au cours d'une perquisition prévue par le code de procédure pénale : enquête de flagrance ou préliminaire, instruction sur commission rogatoire.
Aucune forme spécifique exigée par l'art. 57-1.

Copies des données informatiques contenues dans des supports placés sous scellés

Définition
Réaliser une ou plusieurs copies des données informatiques ou procéder aux opérations techniques nécessaires à leur mise à la disposition des enquêteurs afin de permettre leur exploitation accélérée sans porter atteinte à leur intégrité. Concerne les données physiquement stockées sur le support et non les données stockées à distance.

Cadre légal
Enquête de flagrance
Réquisition par le procureur de la République, l'OPJ, l'APJ ou l'assistant d'enquête de toute personne qualifiée pour procéder à la copie (art. 60-3 al. 1er).
Enquête préliminaire
Réquisition de l'OPJ ou de l'APJ sur autorisation du procureur de la République (art. 77-1-3 al. 1er).
Instruction
Réquisition de l'OPJ, de l'APJ ou de l'assistant d'enquête sur autorisation expresse du JI (art. 99-5 al. 1er).

Infractions concernées
Toute infraction justifiant l'ouverture d'une enquête ou information.
S'agissant des données d'identification de la source de la connexion, d'identification des terminaux et de trafic ou de localisation, uniquement pour les crimes ou délits punis de 3 ans d'emprisonnement ou les délits punis d'1 an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques, lorsque dans ce cas les réquisitions ont pour seul objet d'identifier l'auteur de l'infraction (art. 60-1-2).

Type de décision
Réquisition à personne qualifiée inscrite sur une des listes prévues à l'article 157 ou ayant prêté par écrit le serment prévu à l'article 60 (art. 60-3 al. 1er).

Réquisitions judiciaires aux fins de mise à disposition de données informatiques

Définition
Mise à disposition par les organismes privés ou publics des informations utiles à la manifestation de la vérité, y compris de celles contenues dans les systèmes informatiques ou de traitement automatisés de données qu'ils administrent (FADET).

Cadre légal
Enquête de flagrance
Réquisition du procureur de la République ou de l'OPJ effectuée par tout moyen, y compris par voie télématique ou informatique (art. 60-1 al. 1er et 60-2 al. 1er).
Enquête préliminaire
Réquisition de l'OPJ sur autorisation du procureur de la République (art. 77-1-1 al. 1er et 77-1-2 al. 1er).
Instruction
Réquisition du JI ou de l'OPJ commis par lui (art. 99-3 al. 1er).

Infractions concernées
Toutes infractions pour les réquisitions des données issues d'un système informatique ou d'un traitement de données nominatives (ex : comptes bancaires), art. 60-1.
Crimes ou délits punis d'au moins 3 ans d'emprisonnement, délits punis d'au moins 1 an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques, art. 60-1-2 pour les réquisitions des données d'identification de la source de la connexion, des données d'identification des terminaux et des données de trafic et de localisation. Ces dernières réquisitions ont pour seul objet d'identifier l'auteur de l'infraction (art. 60-1-2).

Type de décision
Réquisitions transmises à la PNIJ (art. 230-45 CPP).
Nota : le fait de refuser de répondre aux réquisitions sans motif légitime est puni de 3750 euros d'amende

Conservation rapide des données informatiques stockées -

Définition
Mesure conservatoire et provisoire requérant des opérateurs de télécommunications de préserver les données informatiques traitées ou stockées par ces derniers.

Cadre légal
Le cadre légal des enquêtes de flagrance et préliminaire relatif à l'accès aux données conservées par les opérateurs à la suite d'une réquisition de conservation rapide a été jugé non conforme au droit de l'UE la Cour de cassation (Crim., 12 juillet 2022, n° 21-83.710).
Enquête de flagrance
OPJ sur réquisitions du procureur de la République après autorisation du JLD (art. 60-2 al. 2).
Enquête préliminaire
OPJ sur autorisation du JLD saisi par le procureur de la République (art. 77-1-2 al. 2).
Instruction
Réquisitions de l'OPJ après autorisation expresse du JI (art. 99-4 al. 2).

Infractions concernées
Crimes ou délits punis d'au moins 3 ans d'emprisonnement ; délits punis d'au moins 1 an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques (art. 60-1-2).

Type de décisions
Réquisitions judiciaires transmises à la PNIJ (art. 230-45). Elles ont pour seul objet d'identifier l'auteur de l'infraction.

Nota : le fait de refuser de répondre aux réquisitions sans motif légitime est puni de 3750 euros d'amende

Mise au clair des données chiffrées – 230-1

Définition
Opérations techniques réalisées par toute personne qualifiée permettant d'obtenir l'accès à ces informations, leur version en clair ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement.

Cadre légal
Enquête de flagrance, enquête préliminaire et instruction
Réquisition du procureur de la République, de la juridiction d'instruction, de l'OPJ sur autorisation du procureur de la République ou du juge d'instruction, de la juridiction de jugement (art. 230-1).

Infractions concernées
Toute infraction justifiant l'ouverture d'une enquête ou information.
En cas d'infraction punie d'au moins 2 ans d'emprisonnement, il est possible de solliciter le recours aux moyens de l'État soumis au secret de la défense nationale (art. 230-1 al. 3).
S'agissant des données d'identification de la source de la connexion, des terminaux et des données de trafic ou de localisation, uniquement pour les crimes ou délits punis de 3 ans d'emprisonnement ou les délits punis d'1 an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques, lorsque dans ce cas les réquisitions ont pour seul objet d'identifier l'auteur de l'infraction (art. 60-1-2).

Type de décision
Réquisition à toute personne qualifiée (art. 230-1 al. 1er).
En cas de recours aux moyens de l'État soumis au secret de la défense nationale, la réquisition est adressée à un organisme technique soumis au secret de la défense nationale avec le support physique contenant les données à mettre au clair ou une copie de celui-ci (art. 230-2 al. 1er).
La réquisition fixe le délai dans lequel les opérations de mise au clair doivent être réalisées (art. 230-2 al. 1er).
Les décisions n'ont pas de caractère juridictionnel et sont insusceptibles de recours (art. 230-4).

Géolocalisation – 230-32 et s.

Définition
Moyen technique (suivi dynamique d'un terminal de communication – ex : téléphone – ou pose d'une balise) destiné à la localisation en temps réel d'une personne à son insu ou d'un bien sans le consentement de son propriétaire ou possesseur.

Cadre légal
Enquête de flagrance et enquête préliminaire
Autorisation du procureur de la République pour 8 jours consécutifs (15 en matière de criminalité organisée et de procédures de recherches), puis renouvellement par le JLD à la requête du procureur pour une durée d'un mois renouvelable (art 230-33). En cas d'urgence, mise en place par un OPJ pour 24h, qui en informe immédiatement le procureur de la République qui décide de la poursuite ou non de l'opération (art. 230-35).
Instruction ou information pour recherche des causes de la mort
Autorisation par le juge d'instruction pour une durée de quatre mois, renouvelable.
Exécution de la peine
Si à l'issue de l'incarcération d'une personne condamnée pour une infraction punie d'au moins trois ans d'emprisonnement, celle-ci est soupçonnée de ne pas respecter ses obligations, le JAP peut ordonner (éventuellement saisi par le procureur) la mesure (art. 709-1-3).
Enquête de flagrance, enquête préliminaire et instruction
La durée totale de l'opération ne peut excéder un an ou en matière de criminalité organisée deux ans.
Autorisation par le PR ou le JI de l'introduction dans certains lieux privés ou dans un véhicule aux fins de mise en place du dispositif en dehors des heures de perquisitions légales (art. 230-34). Dans les autres lieux privés, l'opération n'est possible que pour recherches des causes de la mort, disparition ou personne en fuite et lorsque l'enquête ou l'instruction est relative à un crime ou à un délit puni d'au moins cinq ans d'emprisonnement (art. 230-34). S'il s'agit d'un lieu d'habitation, l'autorisation est délivrée par le JLD.
Infractions concernées
Infractions punies d'au moins 3 ans d'emprisonnement ; recherche des causes de la mort ou de la disparition ; recherche d'une personne (art. 230-32, 706-1-3).

Type de décision
Décision écrite, non juridictionnelle, insusceptible de recours (art. 230-33), transmise à la PNIJ (art. 230-45).

Enquête sous pseudonyme – 230-46 et s.

Définition
Procéder sous pseudonyme aux actes suivants sans en être pénalement responsables : participer à des échanges électroniques, y compris avec les personnes susceptibles d'être les auteurs de ces infractions ; extraire ou conserver par ce moyen les données sur les personnes susceptibles d'être les auteurs de ces infractions et tout élément de preuve ; acquérir tout contenu, produit, substance, prélèvement ou service, y compris illicite, ou transmettre en réponse à une demande expresse (« achat de confiance ») ; en vue de l'acquisition, de la transmission ou de la vente par les personnes susceptibles d'être les auteurs de ces infractions de tout contenu, produit, substance, prélèvement ou service, y compris illicite, mettre à la disposition de ces personnes des moyens juridiques ou financiers ainsi que des moyens de transport, de dépôt, d'hébergement, de conservation et de télécommunication (« coup d'achat »).

Cadre légal
Enquête de flagrance, enquête préliminaire et instruction
OPJ ou APJ, affectés dans un service spécialisé et spécialement habilités à cette fin, sous le contrôle du procureur de la République ou du juge d'instruction (art. 230-46).
Pour la pédo-criminalité, cadre légal spécifique aux articles D. 47-8 et D. 47-9 CPP

Infractions concernées
Crimes et les délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques (art. 230-46 CPP).

Type de décision
Actes définis par l'art. 230-46, réalisés par OPJ ou APJ spécialement habilités sous le contrôle du procureur de la République ou sur commission rogatoire.
Pour l'achat de confiance et le coup d'achat : autorisation par tout moyen du procureur de la République ou du JI, mentionnée et versée au dossier.

Interception des correspondances émises par la voie des communications électroniques – 706-95 et s.

Définition
Interception (enregistrement, transcription) de toute émission, transmission ou réception de signes, de signaux, d'écrits, d'images ou de sons, par câble, par la voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques (art. L. 32 CPCE) : correspondances émises par le biais de téléphones, tablettes, ordinateurs, à l'exclusion des applications de messageries.

Cadre légal
Enquête de flagrance et enquête préliminaire
Décision du JLD à la requête du procureur de la République pour une durée d'un mois, renouvelable une fois (art. 706-95).
Instruction
Décision du JI pour une durée de quatre mois, renouvelable sans excéder un an ou, s'il s'agit d'une infraction visée aux art. 706-73 et 706-73-1, deux ans. En cas d'information pour recherche des causes de la mort ou des causes d'une disparition, la durée est de deux mois, renouvelable (art. 80-4 al. 1er).
Exécution de la peine
Dans le cas où à l'issue de son incarcération, la personne condamnée pour une infraction prévue à l'article 100 al. 1er est soupçonnée de ne pas respecter certaines interdictions, les enquêteurs, agissant sur instruction du JAP saisi à cette fin par le procureur de la République, peuvent intercepter ses correspondances émises par la voie des télécommunications (art. 709-1-3).

Infractions concernées
Enquête de flagrance et préliminaire
Infractions visées par les art. 706-73 et 706-73-1 (art. 706-95) et 706-72.
Instruction

Crimes et délits punis d'au moins 3 d'emprisonnement (art. 100 al. 1er) ; délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques sur la ligne de la victime, l'interception peut également être autorisée, selon les mêmes modalités, si elle intervient sur cette ligne à la demande de la victime (art. 100 al. 3).

Type de décision
Décision écrite, non juridictionnelle, insusceptible de recours (art. 100 al. 2), transmise à la PNIJ (Art. 230-45) et motivée par référence aux éléments de fait et de droit justifiant que ces opérations sont nécessaires (art. 100-1). Elle comporte tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci (art. 100-1).

Accès à distance aux correspondances stockées – 706-95-1

Définition
Accès à distance, à l'insu de la personne visée, aux correspondances stockées par la voie de communications électroniques accessibles au moyen d'un identifiant informatique (historique des e-mails et autres messages échangés sur les réseaux sociaux) par l'intermédiaire des organismes publics ou exploitants privés de services de communication en ligne. 706-95-1 et s.
Possibilité de saisie, enregistrement ou copie des correspondances sur tout support.

Cadre légal
Enquête de flagrance et enquête préliminaire
Ordonnance du JLD à la requête du Procureur de la République (article 706-95-1 CPP).
Instruction
Ordonnance du JI (article 706-95-2 CPP).

Infractions concernées
Infractions visées aux articles 706-73, 706-73-1 et 706-72 CPP.

Type de décision
Ordonnance motivée mais non juridictionnelle, insusceptible de recours (706-95-1 à 706-95-3), puis commission rogatoire. Réquisitions transmises à la PNIJ (art. 230-45).
Nota : le fait de refuser de répondre aux réquisitions sans motif légitime est puni de 3750 euros d'amende

Recueil de données techniques de connexion au moyen d'une antenne-relais mobile factice (*IMSI-catcher*) – 706-95-20

Définition
Mise en place et utilisation d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal afin de recueillir les données techniques de connexion permettant l'identification d'un équipement terminal, le numéro d'abonnement de son utilisateur, les données relatives à la localisation d'un équipement terminal utilisé ainsi que les télécommunications émises ou reçues. Dans ce dernier cas, le dispositif permet de capter tous les échanges dans une zone déterminée.

Cadre légal
Enquête de flagrance et préliminaire
Ordonnance du JLD à la requête du procureur de la République qui autorise les OPJ à utiliser l'IMSI-catcher (art. 706-95-12 al. 2 ; art. 706-96-1 al. 1er). Durée : un mois renouvelable une fois pour l'accès aux données de connexion (art. 706-95-16 al. 1er) ; 48 heures renouvelable une fois pour l'interception des télécommunications (art. 706-95-20 al. 2)
Instruction
Ordonnance du JI après avis du procureur de la République qui autorise les OPJ à utiliser l'IMSI-catcher (art. 706-95-12 al. 3 ; art. 706-96-1 al. 2). Durée : 4 mois renouvelable 5 fois pour l'accès aux données de connexion (art. 706-95-16 al. 2) ; 48 heures renouvelable une fois pour l'interception des télécommunications (art. 706-95-20 al. 2).
Infractions concernées
Infractions visées aux art. 706-73 et 706-73-1 (art. 706-95-11 al. 2) et 706-72.

Type de décision
Ordonnance écrite et motivée, mais non juridictionnelle et insusceptible de recours (art. 706-95-13 al. 1er).

Sonorisation et fixation d'images de certains lieux ou véhicules – 706-96 et s.

Définition
Mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, la captation, la fixation, la transmission et l'enregistrement de paroles prononcées par une ou plusieurs personnes à titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics, ou de l'image d'une ou de plusieurs personnes se trouvant dans un lieu privé.

Cadre légal
Enquête préliminaire et de flagrance
Ordonnance du JLD à la requête du procureur de la République qui autorise les OPJ ou APJ (Art. 706-95-12 al. 2 ; Art. 706-96-1 al. 1er). Durée : un mois renouvelable une fois dans les mêmes conditions de forme et de durée (Art. 706-95-16 al. 1er).
Instruction
Ordonnance du JI après avis du procureur de la République (Art. 706-95-12 al. 3 ; Art. 706-96-1 al. 2). Durée : 4 mois renouvelable 5 fois dans les mêmes conditions de forme et de durée (Art. 706-95-16 al. 2).
Introduction dans des lieux
Ordonnance du JLD au cours de l'enquête et au cours de l'instruction si, dans ce cas, l'introduction a lieu dans un lieu d'habitation et hors des heures légales de perquisition de droit commun (art. 706-96-1).

Infractions concernées.
Infractions visées aux art. 706-73 et 706-73-1 (art. 706-95-11 al. 2) et 706-72.

Type de décision
Ordonnance écrite et motivée, non juridictionnelle et insusceptible de recours (art. 706-95-13 al. 1er).

Captation des données informatiques (cheval de Troie ou *key logger*) – 706-102-1

Définition
Mise en place d'un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de 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, même en dehors de toute activité relative à ces données. 706-102-1 et s.

Cadre légal
Enquête de flagrance et enquête préliminaire
Ordonnance du JLD écrite et motivée à la requête du procureur de la République, qui autorise les OPJ et APJ requis par le procureur.
L'autorisation est donnée pour une durée d'un mois, renouvelable une fois (art. 706-95-16 al. 1er).
Instruction
Ordonnance du JI écrite et motivée après avis du procureur de la République (art. 706-95-13 CPP).
L'autorisation est donnée pour une durée de quatre mois, renouvelable dans la limite de deux ans (art. 706-95-16 al. 2 CPP).
Enquête de flagrance, enquête préliminaire et instruction
Le procureur ou le JI peut désigner tout expert mentionnée sur une des listes de l'art. 157 pour effectuer les opérations techniques ou prescrire le recours aux moyens de l'État soumis au secret de la défense nationale (art. 706-102-1).
Le JLD, saisi par le JI ou le PR, peut autoriser l'introduction dans un véhicule ou lieu privé, y compris hors heures légales, pour assurer la mise en place ou la désinstallation.

Infractions concernées
Infractions visées aux art. 706-73 et 706-73-1 (cf. 706-95-11) et 706-72.

Type de décision
Ordonnance écrite et motivée, non juridictionnelle et insusceptible de recours (art. 706-95-13), précisant l'infraction qui motive le recours à ces opérations, la localisation exacte ou la description détaillée des systèmes de traitement informatisé.

Glossaire

Il s'agit ici de présenter au lecteur non spécialiste une liste des principaux termes utilisés dans le rapport.
Les définitions retenues, appliquées et contextuelles, ne sont elles-mêmes pas savantes et tentent d'éviter le piège de la technicité.
Résultant d'un croisement de sources différentes qui ont été à dessein simplifiées, elles ne sont pas attribuées à telle ou telle d'entre elles. Toutefois, lorsqu'un texte contient la mesure, il a été cité. Nous renvoyons également les lecteurs à la circulaire du 2 décembre 2016 de présentation des dispositions de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relative au renforcement du dispositif en matière de lutte contre la délinquance et la criminalité organisée (NOR : JUSD1635582C) ainsi qu'à la circulaire du 27 mai 2019 relative à la présentation des dispositions de procédure pénale de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice relatives à l'enquête et à l'instruction applicables au 1er juin 2019 (NOR : JUSD1915381C).

Accès distant : possibilité d'accéder à un appareil ou à un réseau depuis n'importe quel endroit. Il peut se faire sur le lieu de la perquisition où il y a du matériel informatique pour accéder par exemple à un stockage de type *Cloud* (art. 57-1 al. 1 CPP), depuis un service de police si les enquêteurs ont en leur possession les identifiants et mots de passe (art. 57-1 al. 2 CPP) ou encore à distance et l'insu de la personne concernée (art. 706-95-1 et art. 706-95-2 CPP).

Adresse IP *(Internet Protocol Address)* ***:*** suite de chiffres attribuée à chaque appareil connecté à un réseau informatique ou à Internet.

Analyse forensique numérique (ou *Forensic*) ***:*** identification, récupération et interprétation des données stockées ou transmises électroniquement. Son rôle est de reconstituer les événements après un incident (cyberattaque, fraude, etc.) en s'appuyant sur des preuves numériques.

Backdoor server (porte dérobée) ***:*** manière détournée de récupérer des données (utile par exemple pour la recherche d'une faille de sécurité)

Captation de données : dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder à distance à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles sont stockées dans un système informatique, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de 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. Cela correspond à une infiltration dans les matériels informatiques qui permet d'en capter les données avant qu'elles aient pu être chiffrées (art. 706-102-1 CPP).

Cheval de Troie ou Key Logger : programme informatique d'apparence inoffensive mais qui contient un logiciel malveillant installé par l'utilisateur à son insu. C'est le cas d'un fichier PDF transmis par courriel qui contiendrait un logiciel permettant la prise de contrôle à distance de l'ordinateur ciblé. Le cheval de Troie permet de capter des données.

Chiffrement (des données émises et reçues, des données du support) ***:*** opération informatique reposant sur un procédé cryptographique visant à rendre incompréhensibles une ou plusieurs données informatiques à toute personne ne disposant pas de la clé de déchiffrement.

Cloud computing (« informatique dans les nuages ») ***:*** utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (*cloud*) composé de nombreux serveurs distants interconnectés.

Conservation ciblée : Mesure conservatoire et provisoire pouvant être utilisée pour la lutte contre la criminalité et la délinquance grave, la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale, qui consiste en une injonction de conservation imposant aux opérateurs de communications électroniques la préservation pour une durée limitée des données de connexion dans certaines zones (aéroports par exemple) ou concernant certaines catégories de personnes pré-identifiées comme présentant des risques particuliers (par ex. : commission d'infractions graves). Cette mesure n'est pas prévue en droit français.

Conservation généralisée et indifférenciée : Obligation imposée aux opérateurs de communications électroniques de conserver les données de connexion de manière généralisée et indifférenciée (c'est-à-dire concernant tous les utilisateurs du service sans exiger qu'il existe à leur encontre des soupçons) pendant une durée d'an, après leur génération, si cette conservation est nécessaire pour la sauvegarde de la sécurité nationale. En droit français, cette obligation est prévue à l'article L. 34-1 III du CPCE.

Conservation rapide (Conservation *a posteriori*, gel immédiat, gel rapide, préservation rapide) ***:*** Mesure conservatoire et provisoire, utilisée pour la lutte contre la criminalité et la délinquance grave, la prévention des menaces graves contre la sécurité publique et la sauvegarde de la sécurité nationale. Elle vise à assurer sans retard la préservation de données informatiques existantes et futures en imposant aux opérateurs de communications électroniques de les conserver à compter de la date de l'injonction de conservation et pour une durée limitée. Établie par la Convention de Budapest sur la cybercriminalité (art. 16), la conservation rapide des données informatiques relève des articles 60-2 al. 2, 77-1-2 et 99-4 du CPP.

Copie de travail : Copie de données informatiques dont le support physique a été placé sous scellés (un disque dur externe par exemple) et qui est effectuée dans le but de permettre leur exploitation sans porter atteinte à leur intégrité (art. 60-3 CPP).

Cryptologie : science étudiant les mécanismes permettant d'assurer la confidentialité, l'authenticité d'un message ou encore l'intégrité des messages.

Darkweb : Le web est composé de trois grandes couches, la première, le *clearweb* est accessible par les moteurs de recherche classiques. Il s'agit de la couche que l'on utilise pour nos activités quotidiennes. La deuxième, le *deepweb* n'est pas accessible avec des moteurs de recherche traditionnels. Il faut utiliser un logiciel dédié, un mot de passe et un chiffrement des données pour s'y rendre. Les activités réalisées sur le *deepweb* sont essentiellement légales (dossiers médicaux, ressources militaires ou dossiers de recherche secrets par exemple). Enfin, la troisième est le *darkweb*, soit la partie la plus difficile d'accès d'internet à laquelle on accède par des navigateurs spéciaux. Volontairement cachés, certains sites hébergent des activités illégales.

Déchiffrement : processus de transformation des données rendues illisibles par la cryptographie. Déchiffrer un message consiste ainsi à ramener un fichier au format non crypté. Lors du déchiffrement, le système extrait et convertit les données illisibles en texte et en images facilement compréhensibles, non seulement par le lecteur, mais aussi par l'ordinateur en lui-même.

Données de connexion (métadonnées) : Données techniques produites par un appareil électronique (téléphone, tablette, ordinateur, objets connectés, etc.) lors de sa connexion au réseau de communications électroniques, qui sont traitées et puis conservées par les opérateurs de communications électroniques. Sans entrer explicitement dans un tel degré de

détail, l'article R. 10-13 du CPCE permet néanmoins de distinguer trois types des données de connexion :

-*les données d'identification* : Il s'agit des données qui permettent d'identifier l'utilisateur en connaissant l'identité civile liée à un numéro de téléphone, à une adresse mail, à une adresse IP, à un numéro d'abonné, à un numéro de carte SIM (IMSI) ou à un identifiant de téléphone (IMEI).

-*les données de trafic* (fadettes : facture/facturation détaillée) : Il s'agit des données qui portent sur l'acheminement des communications et concernent l'activité numérique et téléphonique de l'appareil, tels que l'adresse IP, la liste des contacts téléphoniques entrants et sortants, des SMS et courriels reçus et envoyés, des sites internet consultés, etc. ;

-*les données de localisation* : Il s'agit des données qui permettent la localisation d'un appareil dans une zone relativement précise – mais pas de manière aussi exacte que la géolocalisation - via l'identification de l'antenne-relais par laquelle ont transité les flux issus dudit appareil.

Données de contenu : Données informatiques qui portent sur un contenu (écrit, sonore, vidéo...), telles que le texte des messages (courriels, SMS, etc.) envoyés ou reçus, les images échangées, les propos tenus lors de conversations téléphoniques, le contenu des sites internet consultés. Elles sont le plus souvent déterminées par opposition aux autres données (de localisation et de trafic).

Données personnelles : Toute information relative à une personne physique susceptible d'être identifiée, directement, notamment par le biais de son nom, de son prénom ou de son image ou indirectement, par référence à des informations la concernant. Le recueil et l'utilisation des données personnelles est encadré par la loi informatique et libertés (articles 4-5) ainsi que par le RGPD (articles 4-7).

Données sensibles : Catégorie particulière de données personnelles, qui, directement ou indirectement, fait apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou qui est relative à la santé ou à la vie sexuelle des personnes. En principe, le recueil ou l'utilisation des données sensibles est interdit par la loi, mais sont également prévus des différents cas dans lesquels le traitement des données sensibles peut exceptionnellement avoir lieu. Les données sensibles sont définies et réglementées par l'article 6 de la loi Informatique et Libertés et l'article 9 du RGPD.

Géolocalisation : Procédé permettant de positionner un objet, une personne, une information, sur une carte à l'aide de ses coordonnées géographiques. Cette opération est réalisée à l'aide d'un terminal capable d'être localisé (grâce à un récepteur GPS ou à d'autres techniques) et de publier (en temps réel ou de façon différée) ses coordonnées géographiques (latitude/longitude). Les positions enregistrées peuvent être stockées au sein du terminal et être extraites postérieurement, ou être transmises en temps réel vers une plateforme logicielle de géolocalisation. Pour des enquêteurs, il s'agit d'une sorte de « filature virtuelle » (voir art. 230-32 et s. CPP).

IMSI-catcher : Littéralement intercepteur d'*IMSI* (*International Mobile Subscriber Identity)*, à savoir intercepteur du numéro unique à chaque téléphone portable qui permet de se connecter aux antennes relais et qui est contenu dans la carte SIM. L'*IMSI-catcher* est un appareil ou un dispositif technique utilisé dans le but de recueillir les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur, ainsi que les données relatives à la localisation d'un équipement terminal utilisé. Il s'agit d'un matériel de surveillance qui capte des données informatiques avant qu'elles ne soient chiffrées (voir art. 705-95-4 CPP).

Interception judiciaire des communications : branchement qui permet l'enregistrement et la conservation des messages par stratagème ou artifice. Ainsi une écoute téléphonique est-elle

une « interception ». Le droit français évoque les « interceptions de correspondances émises par la voie des communications électroniques » (art. 100 et s.CPP, art. 706-95 CPP).

International Mobile Equipment Identity (IMEI, littéralement « identité internationale d'équipement mobile ») : numéro qui permet à l'opérateur d'un réseau mobile d'identifier le mobile appelant et ainsi de l'autoriser, ou non, à se connecter. Il est utile par exemple en cas de perte ou de vol d'un téléphone portable.

Log (journal) : désigne en informatique un historique d'événements et par extension le fichier contenant cet historique. Fichier contenant des métadonnées pouvant servir à contextualiser un événement qui s'est produit à un moment donné. Les logs constituent un registre historique de tout ce qui se passe au sein d'un système.

Note blanche : fiche brève, d'une page le plus souvent, non signée ni datée ni sourcée, émanant généralement d'un service de renseignement et rédigée à l'attention de hauts responsables d'un gouvernement ou d'une administration à propos de la conduite d'un individu.

Objets connectés : Objets tels que des montres, des podomètres, des voitures, des appareils électroménagers qui permettent de recueillir des métadonnées de trafic, de localisation, de contenu et notamment des données personnelles sensibles (par exemple, relatives à la santé)

Pack Darwin : clé USB autonome qui, connectée à un ordinateur éteint, analyse son disque dur sans l'altérer (Outil OCLCTIC).

Perquisition à distance, perquisition immatérielle, perquisition numérique, télé-perquisition : Mesure d'enquête consistant en la recherche de données stockées sans détention matérielle du système ou du support via l'accès distant à ce système ou support. Mesure d'enquête prévue par l'art. 57-1 CPP (art. 19 de la convention de Budapest).

Recueil des données techniques de connexion : collecte des données permettant l'identification d'un équipement, l'identification d'un numéro d'abonnement, ou relatives à la localisation d'un équipement terminal utilisé. Prévu par l'art. 706-95-20, ce recueil est une modalité de l'emploi d'un *IMSI-catcher*.

Screen logger **:** dispositif technique ayant pour objet sans le consentement des intéressés d'observer une activité spontanée, grâce à l'accès, en tous lieux, à des données informatiques, telles qu'elles s'affichent sur un écran pour l'utilisateur du système ; relève de la mesure d'enquête de captation de données informatiques régie par les art. 706-102-1 et s. CPP.

Système de traitement automatisé de données (STAD) : Ensemble – qui fait système – protégé par des dispositifs de sécurité, composé d'une ou plusieurs unités de traitement, de mémoire, de logiciel, de données, d'organes d'entrées-sorties et de liaisons, qui concourent à un résultat déterminé (ex : ordinateur, programmes/logiciel, disque dur, site web, réseaux de communication)

Système informatique : Ensemble – qui fait système – des moyens informatiques et de télécommunication ayant pour finalité d'élaborer, traiter, stocker, acheminer, présenter ou détruire des données

Technique spéciale d'enquête : appellation d'origine internationale désignant certaines mesures d'enquête particulièrement intrusives mobilisables en matière de criminalité et de délinquance organisées qui comprend notamment selon le CPP (articles 706-95-11 à 706-102-5) le recueil des données techniques de connexion, l'interception de correspondances émises par la voie électronique, la sonorisations et la fixation d'images de certains lieux ou véhicules et la captation de données informatiques.

Technique d'enquête numérique (judiciaire) : Mesure d'enquête relevant de la compétence de l'Agence nationale des techniques d'enquêtes numériques judiciaires (ANTENJ).

Techniques de recueil de renseignement (soumises à autorisation) : Mesure administrative prévue par les articles L. L851-1 et s. CSI, contrôlée par la CNCTR, qui peut consister en l'accès administratif aux données de connexion, l'interception de sécurité, la sonorisation de

certains lieux et véhicules, la captation d'images et de données informatiques ainsi que la surveillance des communications électroniques internationales.

Bibliographie

I – OUVRAGES GENERAUX, MANUELS ET TRAITES

AMBROISE-CASTEROT Coralie, BONFILS Philippe, *Procédure pénale*, PUF, 5ème éd., 2024.

BOULOC Bernard, *Procédure pénale*, Dalloz, 29ème éd., 2023.

DOUVILLE, Thibault, *Droit des données à caractère personnel*, Paris, LGDJ, 2023.

DREYER Emmanuel, MOUYSSET Olivier, *Procédure pénale*, LGDJ, 5ème éd., 2023.

FOURMENT François, CAMOUS Eric, *Procédure pénale*, Bruylant, 17ème éd., 2024.

GARE Thierry, GINESTET Catherine, *Droit pénal. Procédure pénale*, Lefebvre Dalloz, 16ème éd., 2024.

GUINCHARD Serge, BUISSON Jacques, avec la participation de ASCENCI Lionel et BOUCHET Marthe, *Procédure pénale*, Lexisnexis, 17ème éd., 2024.

PARIZOT Raphaële, *Procédure pénale*, Lefebvre Dalloz, 2024.

ROUSSEL Gildas, ROUX-DEMARE François-Xavier, *Procédure pénale*, Vuibert, 13ème éd., 2022.

VERGÈS, Étienne, *Procédure pénale*, Paris, LexisNexis, 2020.

VERGES Etienne, LECLERC Olivier, VIAL Géraldine, *Droit de la preuve*, PUF, 2ème éd., 2022.

VERNY Edouard, *Procédure pénale*, Lefebvre Dalloz, 9ème éd., 2024.

II - OUVRAGES SPECIALISES, ESSAIS, MONOGRAPHIES

AÏM Olivier, *Les théories de la surveillance. Du panoptique aux 'Surveillances Studies'*, Armand Colin, 2020.

ALLEN Stephen, COSTELLOE Daniel, FITZMAURICE Malgosia, GRAGL Paul, GUNTRIP Edward, *The Oxford Handbook of Jurisdiction in International Law,* OUP, 2019,

BEAUVAIS Pascal, CHILSTEIN David, DREYER Emmanuel (dir.), *Le droit pénal de l'avenir*, Lefebvre Dalloz, 2024.

BEAUVAIS Pascal et PARIZOT, Raphaële (éd.), *Les transformations de la preuve pénale,* Paris, LGDJ, 2018.

BERGEAUD-WETTERWALD Aurélie et SAINT-PEAU, Jean-Christophe, *La preuve pénale. Problèmes contemporains en droit comparé,* Paris, L'Harmattan, 2013.

BILLIS Emmanouil, KNUST Nandor, RUI Jon Petter*, Proportionality in Crime Control and Criminal Justice,* Hart publishing, 2021,

BURGUIERES Jean-Michel (dir.), *L'émergence d'un droit des données*, Dalloz, Thèmes et commentaires, 2023, 186p.

COLLET Philippe, *L'acte coercitif en procédure pénale*, Paris, Éditions Panthéon-Assas, 2018.

DAOUST, François, Sur les traces de la police technique et scientifique, Paris, PUF, 2020

DECIMA Olivier (éd.), *La juridictionnalisation de l'enquête pénale*, Paris, Cujas, « Actes et études », 2015.

DELMAS-MARTY Mireille, *Les grands systèmes de politique criminelle*, Paris, PUF, 1992.

DE KOSTER Philippe, *Terrorism: Special Investigation Techniques,* Strasbourg, Council of Europe Publishing, 2005.

DE RUE, Maité et DE VALKENEER Christian, *Les méthodes particulières de recherche et quelques autres méthodes d'enquête,* 2ème éd., Bruxelles, Larcier, Collection « Les dossiers du journal des tribunaux », 2008.

DUBBER Markus D., HÖRNLE Tatjana, *The Oxford Handbook of criminal law,* 2014,

FLORIDI Luciano, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality,* Oxford, Oxford University Press, 2014.

FORCADE Olivier et WARUSFELD Bertrand (éd.), *Le droit du renseignement*, Paris, La documentation française, 2020.

FORCESE Craig, *The limits of reasonableness: the failure of the conventional search and seizure paradigm in information-rich environments*, Ottawa, Office of the privacy commissioner of Canada, « Insights on privacy speaker series », 2011.

FOUCAULT, Michel, Sécurité, territoire et population, Cours au Collège de France (1977-1978), éd. Michel Senellart, Paris, Gallimard/Éditions du Seuil, 2004.

FRANSSEN, Vanessa et MASSET, Adrien (éd.), *Les droits du justiciable face à la justice pénale*, Liège, Anthémis, « Commission Université-Palais », 2017.

FRANSSEN, Vanessa et FLORE, Daniel (éd.), *Société numérique et droit pénal, Bruxelles,* Bruylant, « Pratique du droit européen », 2019,

GRAY David, HENDERSON Stephen E., (ed.), *The Cambridge Handbook of Surveillance Law*, Cambridge, Cambridge University Press, 2017,

HARCOURT Bernard E., *Against Prediction. Profiling, Policing and Punishing in an Actuarial Age*, Chicago, The University of Chicago Press, 2007.

HARCOURT Bernard E., *La Société d'exposition*, Paris, Seuil, « La Couleur des Idées », 2020,

KERR Orin, *The digital fourth amendment*, Oxford, Oxford University Press.

LIGETI Katalin (ed.), *Toward a Prosecutor for the European Union : Draft Rules of Procedure*, Oxford - Portland, Hart, Vol. 2, 2018.

MITSILEGAS Valsamis, VAVOULA Niovi (eds.), Surveillance and Privacy in the Digital Age, Hart Publishing, 2021.

PORCEDDA Maria Grazia, C*ybersecurity, privacy and data protection in EU law : a law, policy and technology analysis*, Hart Publishing, 2023.

RIBAUX Olivier, *De la police scientifique à la traçologie. Le renseignement par la trace*, Lausanne, EPFL Press, 2023.

ROSS Jacqueline E., THAMAN Stephen C., *Comparative criminal procedure, 2018,*

SIEBER Ulrich et von zur MÜHLEN Nicolas (éd.), *Access to telecommunication data in criminal justice: a comparative analysis of European legal orders,* Berlin, Duncker & Humbolt, «Schriftenreihe des Max-Planck-Instituts für Ausländisches und Internationales Strafrecht., Strafrechtliche Forschungsberichte », 2016.

SIMMONS, Ric, *Smart Surveillance - How to Interpret the Fourth Amendement in the Twenty-First century,*Cambridge, Cambridge University Press, 2019.

TOUILLIER Marc (dir.), *Le code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, Dalloz, Les sens du droit, 2017.

TOUILLIER Marc et SIZAIRE Vincent (dir.), *La simplification de la justice pénale. Derrière la promesse, quelle réalité juridique ?*, Dalloz, coll. « Les sens du droit », 2022.

VAILLY J. (dir.), *Sur la trace des suspects. L'incorporation de la preuve et de l'indice à l'ère de la génétique,* éditions de la MSH, 2021.

VAILLY Joëlle, *ADN policier*, PUF, 2024.

VERMEULEN, Gert and LIEVENS, Eva (ed), *Data protection and privacy under pressure. Transatlantic tensions, EU surveillance and big data,* Anvers - Apeldoorn - Portland, Maklu, 2017.

VOGEL Benjamin (ed.), *Secret Evidence in Criminal Proceedings*, Berlin, Duncker & Humblot, 2021.

VOGEL Benjamin, MAILLART Jean-Baptiste, *National and international anti-Money Laundering Law,* 2020.

WINTER, Lorena Bachmaier, RUGGERI, Stefano (eds.), Investigating and Preventing Crime in the Digital Era, Springer Cham, 2022.

ZUBIK, Marek Podkowik, JAN, Rybski Robert, European constitutional courts towards data retention laws, Springer Cham, 2021

RAPPORTS

Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, Paris, La documentation française.

Cour des comptes, *Les moyens affectés aux missions de police judiciaire*, Exercices 2017-2022.

SUPIOT Elsa, « Le procès pénal à l'épreuve de la génétique », Mission Droit et justice-ISJPS, juin 2017.

III – ENCLYCLOPEDIES

QUEMENER, Myriam, « Les techniques spéciales d'enquête », Encyclopédie Dalloz.

IV – THESES

AUDIBERT Matthieu, *Le recueil de la preuve numérique. Enjeux et perspectives en procédure pénale*, Université Paris Nanterre, 2024.

DEMARCHI Jean-Raphaël, *Les preuves scientifiques et le procès pénal*, LGDJ, 2012.

DEPAEPE T., *Le droit de la preuve face aux techniques numériques*, Thèse Paris-Saclay, (dir.) F Labarthe, 2023.

EL HAJJ Chehade Farah, *Les actes d'investigation*, Thèse de doctorat, Université du Maine, 2010.

JEAN-MEIRE, Caroline, *Les nouvelles technologies et la lutte contre la délinquance : regards croisés France/Royaume-Uni*, Thèse soutenue à l'Université Paris 1 Panthéon-Sorbonne, 2016.

LASSALLE Maxime, *L'accès extraterritorial aux données bancaires dans le cadre de l'enquête pénale. Perspective transatlantique*, Thèse de doctorat, Université Paris Nanterre et du Luxembourg, 2019, 800 p.

MORNET Alice, *Les fichiers pénaux de l'Union européenne. Contribution à l'étude de la protection des données à caractère personnel*, Mare&Martin, 2023.

MERMOZ Vincent, *Les indices en procédure pénale*, Thèse soutenue à l'Université Paris-Saclay (Sceaux), 2019.

ROBIN Jean-Nicolas, *La matière pénale à l'épreuve du numérique*, Thèse de doctorat, Université de Rennes 1, 2017, 681 p.

SONTAG KOENIG Sophie, *Technologies de l'information et de la communication et défense pénale*, Paris, Mare & Martin, « Bibliothèque des thèses », 2015, 744 p

VII - COLLOQUES ET JOURNEES D'ETUDES

Les données de connexion – Quel équilibre entre droits fondamentaux et lutte contre la criminalité à l'ère du numérique ?, Colloque université des Antilles, 16 janv. 2023, (dir.) F.-X. Millet : RFDA 2023, p. 634.

VIII - ARTICLES

DOSSIER : « L'accès et la conservation des données de connexion » *AJ pénal 2022*, 391.

« Justice et transformation numérique », *Revue Justice Actualités*, n° 26, accessible en ligne : https://www.enm.justice.fr/api/getFile/sites/default/files/actu-pdf/RJA_26.pdf

ALCARAZ Hubert, « Sonorisations et écoutes téléphoniques : la France se fait “tirer l’oreille”... : à propos des arrêts Vetter et Matheron de la Cour européenne des droits de l’homme », *Revue trimestrielle des droits de l’homme*, nº 66, 2006, pp. 217-235.

ARCHAMBAULT, Alexandre, « Accès aux données de connexion : quelles pistes pour une mise en conformité ? », *AJ Pénal*, n° 9, 2022, p. 400-405.

ARCHAMBAULT, Alexandre, « La conservation généralisée des données de connexion est contraire à la Constitution », *AJ Pénal*, n° 4, 2022, p. 220-222.

AUDIBERT Matthieu, « L'extraction et l'exploitation des données contenues dans des supports numériques », *AJ Pénal*, n° 3, 2023, p. 116-119.

AUDIBERT Matthieu, « Conservation des données de connexion, comment le Conseil d’État a sauvé la majorité des enquêtes judiciaires. Veille juridique », 2021, 96, pp.16-25.

AUDIBERT Matthieu, « Inconstitutionnalité différée des réquisitions de données informatiques par le procureur de la République dans le cadre de l’enquête préliminaire : le jour d’après », *Lexbase Pénal*, n° 44, 23 décembre 2021.

AUDIBERT Matthieu, « La conservation et l’accès aux métadonnées dans le cadre des enquêtes judiciaires : vers un bouleversement dans la procédure pénale française ? », *Lexbase Pénal*, n° 36, 25 mars 2021.

AUMAITRE Aurélie, LETOQUEUX Hervé, « Apprivoiser les preuves numériques : la réception française de l’OSINT », *Délibérée*, 2023/2, pp. 49-55.

AUROY Benoît, « La preuve numérique en procédure pénale : un système à (re)construire », *D.* 2023, p. 697.

BARLATIER Jérôme, « Le renseignement criminel au service de la lutte contre la cybercriminalité : l’exemple français de la gendarmerie nationale », *Rivista di Criminologia, Vittimologia e Sicurezza*, Vol. XVI – Numero Unico – Janvier-Décembre 2022, p. 91-115.

BARRACHE Samia, OLIVIER Antoine, « L’administration de la preuve pénale et les nouvelles technologies de l’information et de la communication », *in*, DE FROUVILLE, Olivier (dir.), *La preuve pénale*, Paris, La documentation française, 2007, p. 129-164.

BEAUVAIS Pascal, « La nouvelle surveillance pénale », in *Humanisme et justice, Mélanges en l’honneur de G. Giudicelli-Delage*, Dalloz, 2016, pp. 259-273.

BELLIVIER Florence, « La circulation de profils ADN dans le système Prüm » *in* Raphaële Parizot et Pascal Beauvais (dir.), *Les transformations de la preuve pénale*, Paris, L.G.D.J, 2018, pp. 119-123.

BELLOIR Philippe, « Perquisition et saisie en matière de lutte contre la cybercriminalité », *RLDI* 2010/60, N° 1995.

BENDAVID, Michaël, QUENDOLO, Camilla, Conservation et accès aux données de connexion : la Cour de cassation prend position, *AJ Pénal*, n° 9, 2022, p. 415-418.

BÉNICHOU David, « Accès à un compte de données personnelles à l’insu de son titulaire : aspects techniques et juridiques », *AJ Pénal*, 2013, p. 451.

BERGEAUD-WETTERWALD Aurélie, « Les nouvelles techniques d’investigation face au principe de légalité de la preuve », in *La preuve pénale. Problèmes contemporains en droit comparé*, Paris,

L'Harmattan, 2013, pp. 9-22.

BERNAEERT Marie-Aude, « Le nouveau code de procédure pénale en projet : quelques lignes de force » *in* Vanessa Franssen et Adrien Masset (dir.), *Les droits du justiciable face à la justice pénale*, Liège, Anthémis, « Commission Université-Palais », 2017, pp. 133-186.

BIGO Didier, BONELLI Laurent, « Nous ne sommes pas un Big Brother ! », Cultures & Conflits [En ligne], 114-115, été/automne 2019, mis en ligne le 01 janvier 2023, URL : http://journals.openedition.org/conflits/21180

BONELLI Laurent, RAYNER Hervé et VOUTAT Bernard, « Contestations et (re)légitimations du renseignement en démocratie », Cultures & Conflits, n°, 114-115, 2019, 7-28.

BOSSAN Jérôme, « Les réquisitions judiciaires relatives aux données de connexion : suite… et fin ? », *Dr. pén.*, n° 7-8, *2022, étude 17.*

BOTTON Antoine, *Aperçu rapide, JCP G n° 38 du 26 septembre 2022.*

BRIGANT Jean-Marie, « Conservation généralisée des données de connexion : pas de traitement de faveur pour la lutte contre les abus de marché », *RSC*, n° 2, 2023, p. 337-362.

BRIGANT Jean-Marie, « Mesures d'investigation face au défi numérique en droit français » in Vanessa Franssen et Daniel Flore (dir.), *Société numérique et droit pénal*, Bruxelles, Bruylant, « Pratique du droit européen », 2019, pp. 217-244.

BUISSON Jacques, « La requête en annulation : le droit à un recours effectif quelque peu malmené ? », *Procédures*, 2022, n°11, étude 12.

BUISSON Jacques, « Données de connexion, conservation et accès : la primauté du droit de l'Union réaffirmée », *Procédures* n° 10, Octobre 2022, étude 11.

BUISSON Jacques, « Des écoutes téléphoniques aux interceptions de correspondances émises par la voie des télécommunications : un regard historique » in *Droit répressif au pluriel : droit interne, droit international, droit européen, droits de l'homme*, Paris, Anthemis, « Droit et justice », 2015, pp. 61-78.

CALO Ryan, « Privacy Law's Indeterminacy », *Theoretical Inquiries in Law*, Vol. 20, n° 33, 2019.

CAHN Olivier, « Données de connexion et enquêtes pénales : la chèvre et le chou malmenés », *JCP* G, n° 40, 10 octobre 2022, act. 1123.

CASAGRAN Cristina Blasi, « Surveillance in the European Union » *in* David Gray, Stephen E. Henderson (éd.), *The Cambridge Handbook of Surveillance Law*, Cambridge, Cambridge University Press, 2017, pp. 642-658.

CASILI Antonio, « Quatre thèses sur la surveillance numérique de masse et la négociation privée », Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle, La documentation française.

CATTARUZZA Amaël, « XXI. Prolégomènes à une stratégie critique de la donnée », Jean Baechler éd., Guerre et Technique. Hermann, 2017, pp. 309-322.

CHAMBON Pierre, « De la légalité des écoutes téléphoniques concernant un inculpé, ordonnées par le juge d'instruction », *JCP*, 1981. I. 3029.

CHAUVELOT Aurore, « Le contrôle, par la chambre de l'instruction, de l'accès des personnels habilités aux fichiers de police judiciaire », *RSC* 2024 p.407.

CHRISTODOULOU Hélène, « L'injonction de production et de conservation des preuves électroniques : prémices d'un acte d'investigation de l'UE », *JCP G 2023*, 1561.

COCQ Céline, GALLI Francesca, « The catalysing effect of serious crime on the use of surveillance technologies for prevention and investigation purposes », *New Journal of European Criminal Law*, Vol. 4, n° 3, 2013, p. 256-289.

COLLET Philippe, « Le droit au silence en procédure pénale », *RSC*, n° 4, 2023, p. 751-775.

COLLET Philippe, « L'insaisissable notion de surveillance en droit pénal », *RSC*, nº 3, 2019, p. 549.

CONTE Philippe, « Refus de transmettre une convention secrète de déchiffrement : le code de déverrouillage d'un téléphone peut être une convention secrète de déchiffrement », *Droit pénal* n° 12, Décembre 2022, comm. 195.

COVOLO Valentina, « Monnaies virtuelles, nouvelle frontière dans la lutte contre le blanchiment d'argent et le financement du terrorisme », in *Droit pénal et procédure pénale*, nº 1, 2019, pp. 3-10.

DAIEFF, G., « Cybercriminalité : « Il y a un enjeu de protection du pays et des acteurs économiques par le biais des peines » », *Dalloz actualité*, 12 septembre 2023, propos recueillis par G. Thierry, journaliste.

DAVIS Frederick T., GUNKA Charlotte, « Perquisitionner les nuages - CLOUD Act, souveraineté européenne et accès à la preuve dans l'espace pénal numérique », *Revue critique de droit international privé*, n° 1, 2021 p.43-66.

DE HERT Paul et MALGIERI Gianclaudio, « European human rights, criminal surveillance, and intelligence surveillance: towards "good enough" oversight, preferably but not necessarily by judges » *in* David C. Gray, Stephen Henderson (dir.), *Cambridge Handbook of Surveillance Law*, New York, Cambridge University Press, 2017, pp. 509-532.

DECIMA Olivier, « Du piratage informatique aux perquisitions et saisies numériques? », *AJ Pénal*, no 7-8, 2017, pp. 315-317.

DELAGE Pierre-Jérôme, « À propos de quelques évolutions de la procédure pénale issues de la loi « Justice » du 20 novembre 2023 (Loi n° 2023-1059 du 20 novembre 2023 d'orientation et de programmation du ministère de la Justice 2023-2027) », *RSC*, 2024, p. 633 et s.

DESFORGES Yves, « L'évolution de l'administration de la preuve pénale face aux défis scientifiques », *AJ Pénal*, n° 2, 2014, p. 56-57

DURAND-POINCLOUX M., PEISSEL J., BENDAVID M., « Le saviez-vous ? Chaque jour, vous cryptez vos correspondances ! », *Droit pénal 2022, étude 25*.

FLUMIAN Baptiste, FRANSSEN Vanessa, « Le nouveau cadre légal belge en matière de conservation des données de communications électroniques : "*Old Wine in New Bottles*" pour les autorités judiciaires ? », *in* FRANSSEN Vanessa, MASSET Adrien (dir.), *Le droit pénal et la procédure pénale en constante évolution*, Anthemis, 2023, vol. 217, p. 315-360.

FRANSSEN Vanessa, CORHAY Marine, « La fin de la saga Skype: les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger », *Revue de droit commercial belge*, nº 8, 2019, pp. 1014-1022.

FRANSSEN Vanessa, LEROUX Olivier, « Recherche policière et judiciaire sur internet: analyse

critique du nouveau cadre législatif belge » *in* Vanessa Franssen, Daniel Flore (dir.), *Société numérique et droit pénal*, Bruxelles, Larcier/Bruylant, « Pratique du droit européen », 2019, pp. 133-215.

GAVISON Ruth, « Privacy and the Limits of Law », *The Yale Law Journal*, nº 3, vol. 89, 1980, pp. 421-471.

GENTITHES Michael, « The end of Miller's time : how sensitivity can categorize third-party data after Carpenter », *Georgia Law Review*.

GERARDS Janneke, « How to improve the necessity test of the European Court of Human Rights », *International Journal of Constitutional Law*, nº 2, vol. 11, 2013, pp. 466-490.

GOGORZA Amane, « L'accès aux données de connexion : les affres du pluralisme normatif », *Droit pénal*, n° 10, *2022, étude 20*.

GUILLARD Antonin, « Sonorisation et fixation d'images au croisement de la procédure pénale et du renseignement », *AJ Pénal*, n° 11, 2023, p. 484-486.

GUILLARD Antonin et BELLIVIER Florence, « JOP 2024 : ne pas gâcher la fête ? », *Revue juridique de la Sorbonne*, décembre 2023, n° 8, p. 217 et s.

GUILLAUMIN, Béatrice, L'activation à distance des appareils électroniques en clair-obscur, *AJ Pénal*, n° 9, p. 389-391.

GUILLOU Nicolas, « Les nouveaux modèles de participation de la société civile en politique criminelle », *RSC* 2024, p. 695 et s.

HENDERSON Stephen E., « Beyond the (current) fourth amendment : protecting third-party information, third parties, and the rest of us too », *Pepperdine Law Review*, vol. 34, 2007, pp. 975-1026.

HERRAN Thomas, « La distinction entre police administrative et police judiciaire à l'aune de la loi relative au renseignement », *Montesquieu Law Review*, nº 4, 2016, pp. 1-8.

IMBERT-QUARETTA Mireille, « La plate-forme nationale des interceptions judiciaires », *AJ Pénal*, 2017, p. 318.

KEFFER Scott, « Too big to surveil: the fourth amendment illuminated by "modern lights" and shadowed by obsta principiis in a post-Carpenter world concerned with privacy », *Information & Communications Technology Law*, nº 2, vol. 28, 2019, pp. 161-185.

KERR Orin S., « Compelled Decryption and the Privilege Against Self-Incrimination », *Texas Law Review*, vol. 97, 2019, pp. 767-799.

KOERING-JOULIN Renée, « De l'art de faire l'économie d'une loi », *D*. 1990. Chron. 187.

LACROIX Bernard, « Retour sur 1848 : Le suffrage universel entre l'illusion du "jamais vu" et l'illusion du "toujours ainsi"», *Actes de la recherche en sciences sociales*, n° 140, 2001, pp.41-50.

LARONDE-CLÉRAC, Céline, « Dispositions de la loi Justice relatives à l'enquête : simplification et modernisation ?, *AJ Pénal*, n° 1, 2024, p. 8-12.

LASAGNI Giulia, « Tackling phone searches in Italy and the United States: proposals for a technological rethinking of procedural rights and freedoms », *New Journal of European Criminal Law*, nº 3, vol. 9, 2018, pp. 386-401.

LASSALE Alice, « De “Big Brother” à “Big Data”. L’avenir de la police administrative à l’ère de la vidéosurveillance intelligente », *RFDA* 2024, p. 955 et s.

LASSALLE Maxime, « La mue des réquisitions, signe avant-coureur d’une transformation plus large ? », *AJ Pénal*, 2023, n° 11, p. 491-492.

LASSALLE Maxime, « L'affaire EncroChat », *Recueil Dalloz*, n° 35, 2023, p. 1833-1838.

LASSALLE Maxime, « Conservation et réquisition des données relatives aux communications électroniques : un débat serein est-il enfin possible ? », *Recueil Dalloz*, n° 8, 2022, p. 1540-1547.

LASSALLE Maxime, « Transformation à venir de l’encadrement des réquisitions judiciaires de documents », *Droit pénal*, n° 6, 2021, p. 46-47.

LASSALLE Maxime, « Enquêtes administratives et protection des données personnelles : les limites de la jurisprudence constitutionnelle », *Dalloz*, 2020, p. 68.

LEBLOIS-HAPPE Jocelyne, « La réforme de l’enquête par la loi de programmation 2018-2022 revue par le Conseil constitutionnel », *AJ Pénal*, 2019, p. 180.

LEBORNE Jérôme, « La vidéojustice : la justice pénale à l’ère de la vidéo », *Cahiers droit, sciences & technologies,* n° 13/2021, p. 93-109.

LEBRETON, Thomas, « Constitutionnalité des réquisitions de métadonnées en flagrance », *AJ Pénal*, n° 7, 2022, p. 379-381.

LECLERC Olivier, VERGÈS Étienne, VIAL Géraldine, « Preuves scientifiques et technologies », *Cahiers Droit, Sciences & Technologies* [En ligne], 15, 2022, mis en ligne le 14 novembre 2022, consulté le 29 juin 2023. URL : http://journals.openedition.org/cdst/6883

LE DRÉAU Constance Ascione, « QPC dans l’affaire EncroChat : des jours heureux pour Big Brother ? », *AJ Pénal*, n° 7, 2022, p. 376-377.

LE MONNIER DE GOUVILLE Pauline, « Quel juge pour l’enquête ? » *in* Olivier Décima (éd.), *La juridictionnalisation de l’enquête pénale*, Paris, Cujas, « Actes et études », 2015, pp. 83-99.

LELIEUR Juliette, SAAS Claire et WEIGEND Thomas « Chronique de droit pénal constitutionnel allemand. Année 2010 », *RSC*, no. 3, 2011, pp. 690-701.

LÉNA Maud, « Tableau récapitulatif des techniques d’enquête numériques judiciaires », *AJ Pénal*, nº 7-8, 2017, pp. 327-329.

LIGETI Katalin, ROBINSON Gavin, « Cross-border access to electronic evidence: policy and legislative challenges » *in* Sergio Carrera, Valsamis Mitsilegas (éd.), *Constitutionalising the Security Union Effectiveness, rule of law and rights in countering terrorism and crime*, Bruxelles, Centre for European Policy Studies, 2017, pp. 99-111

LOPEZ, Xesus Pérez, « La géolocalisation et la preuve pénale », *AJ Pénal*, n° 2, 2014, p. 67-70.

LYON David, « La surveillance globale dans un monde post-Snowden », *Communiquer*, 20, 2017, 49-65.

MASSON F., « Quel “modèle propriétaire” pour les données personnelles ? », *RTDCiv*. 2022, p. 777 et s.

MAZEAUD Vincent, « La constitutionnalisation du droit au respect de la vie privée », *Les nouveaux cahiers du Conseil constitutionnel*, n° 48, 2015, p. 7-20.

MESA Rodolphe, « Conservation et exploitation des données électroniques dans l'enquête et l'instruction / droit de l'Union européenne », Gazette du Palais, 2022, n° 38, p. 16-19.

MOONEN Toon, « Special investigation techniques, data processing and privacy protection in the jurisprudence of the European court of human rights », *Pace International Law Review Online Companion*, nº 9, vol. 1, 2010, pp. 97-136.

MORNET Alice, « Vers un droit commun de la preuve numérique ? », *Lexbase Pénal*, n° 57, 23 février 2023.

NILSSON H.G., « Special Investigation techniques and Developments in Mutual Legal Assistance – The Crossroads between police cooperation and judicial cooperation », disponible à https://www.unafei.or.jp/publications/pdf/RS_No65/No65_07VE_Nilsson2.pdf

OHM Paul, « The many revolutions of Carpenter », *Harvard Journal of Law and Technology*, nº 2, vol. 32, 2019, pp. 357-416.

OLLARD Romain, « Un an de droit pénal numérique - (octobre 2021 - octobre 2022) », *Droit pénal* n° 12, Décembre 2022, chron. 12.

PAMART David, « La PNIJ, consulte-la si tu peux », *AJ Pénal*, n° 9, 2023, p. 392-394.

PAMART David, note sous Crim., 8 novembre 2023, n° 23-81.636, *AJ Pénal*, n° 12, 2023, p. 560-561.

PARIZOT Raphaële, « Qu'est-ce qu'un téléphone portable ? », *RSC*, n° 1, 2021, p. 128-129.

PARIZOT Raphaële, « Les (autres) techniques spéciales d'enquête, une non catégorie juridique », *in* Sébastien Pellé, *Quelles mutations pour la justice pénale du XXIe siècle*, Paris, Dalloz, 2020, p. 71-81.

PARIZOT Raphaële, « La distinction entre police administrative et police judiciaire est-elle dépassé ? » *in* Marc Touillier (dir.), *Le Code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre ?*, Paris, Dalloz, 2017, pp. 133-145.

PARIZOT Raphaële, « Surveiller et prévenir... à quel prix ? Loi n° 2015-912 du 24 juillet 2015 relative au renseignement », JCP G n° 41, 5 octobre 2015, doctr. 1077.

PIN Xavier, « Le Code de la sécurité intérieure substitut du Code de procédure pénale ? », *in* BEAUVAIS Pascal, CHILSTEIN David, DREYER Emmanuel (dir.), *Le droit pénal de l'avenir*, Lefebvre Dalloz, 2024, pp. 205-220.

PRADEL Jean, « De l'enquête pénale proactive : suggestions pour un statut légal », *Recueil Dalloz*, 1998, p. 57.

PRADEL Jean, « Écoutes téléphoniques et Convention européenne des droits de l'homme, (à propos de Cass., Ass. plén., 24 novembre 1989, affaire Baribeau », D. 1990.34), *Recueil Dalloz*, 1990, Chronique, p. 15-20.

QUEMENER Myriam, « Les spécificités juridiques de la preuve numérique », *AJ Pénal*, n° 2, 2014, p. 63-66.

REDON Michel, « Article 77-1 du Code de procédure pénale : un salutaire rappel des principes », *D.*

2001, p. 1128.

ROZENSHTEIN Alan Z, « Surveillance Intermediaries », *Stanford Law Review*, vol. 70, 2018, pp. 99-189.

RUMOLD Mark, « Regulating surveillance through litigation: some thoughts from the trenches » *in* David Gray et Stephen E. Henderson (éd.), *The Cambridge Handbook of Surveillance Law*, Cambridge, Cambridge University Press, 2017, pp. 579-596.

SACHAROFF Laurent, « Unlocking the fifth amendment: passwords and encrypted devices », *Fordham Law Review*, nº 1, vol. 87, 2018, pp. 203-251.

SAINT-PAU Jean-Christophe, « Les investigations numériques et le droit au respect de la vie privée », *AJ Pénal,* n° 7-8, 2017, p. 321-324.

SCHERER Théo, « Consécration de la dualité des régimes de géolocalisation par la chambre criminelle », *Dalloz Actu*, 6 mars 2024.

SCHERER Théo, « Viser n'est pas motiver, tant pour le procureur que pour le JLD », Dalloz Actu, 9 octobre 2024.

SIZAIRE Vincent, « L'art du trompe-l'œil », *La Revue des droits de l'homme* [Online], Actualités Droits- Libertés, Online since 20 September 2021, connection on 22 September 2021. URL: http://journals.openedition.org/revdh/12968

SONTAG KOENIG Sophie, « La transformation des actes d'enquête : de la perquisition (informatique) aux autres techniques de captation », *AJ Pénal*, n° 11, 2023, p. 486-490.

SONTAG-KOENING Sophie, « Sonorisation et fixation d'images : que reste-t-il de la vie privée ? », *AJ Pénal*, n° 1, 2023, p. 27-32.

SONTAG KOENIG Sophie, « "Silence, on tourne !" L'essor des caméras mobiles : le clair-obscur de la transparence », *Droit pénal*, nº 4, 2018.

SONTAG KOENIG Sophie, « Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel », *AJ Pénal*, 2016, p. 238.

STARR Sonja B., « Evidence-Based Sentencing and the Scientific Rationalization of Discrimination », *Stanford Law Review*, nº 4, vol. 66, 2014, pp. 803-821.

SUPIOT Elsa et SIMON Anne (dir.), « Le procès pénal à l'épreuve de la génétique », *Cahiers droit, sciences & technologies, n°* 9, 2019, dossier, p. 19-104.

SURREL Hélène, « La protection des données à caractère personnel, domaine emblématique des interactions jurisprudentielles entre cours européennes et Conseil constitutionnel », *Titre VII*, n°2, 2019.

TEYSSEDRE Julie, « Strictly regulated retention and access regimes for metadata: Commissioner of An Garda Síochána », *Common Market Law Review*, Vol. 60, n° 2, 2023, p. 569-588.

THIERRY Gabriel, « Robin Binsard et Guillaume Martine : ces avocats qui ferraillent contre la procédure Encrochat », *Dalloz actualité*, 19 janvier 2024.

TINIERE Romain, « Protection des données à caractère personnel », *in* PICOD Fabrice, RIZCALLAH Cecilia, VAN DROOGHENBROECK Sébastien (dir.), *Charte des droits fondamentaux de l'Union européenne, Commentaire article par article*, Bruylant, 2ème éd., 2019.

TOSZA Stanislaw, « Vers une justice pénale numérique ? A propos du rôle singulier des fournisseurs de services numériques dans la procédure pénale », *in* BEAUVAIS Pascal, CHILSTEIN David, DREYER Emmanuel (dir.), *Le droit pénal de l'avenir*, Lefebvre Dalloz, 2024, pp. 45-55.

TOUILLIER Marc, « Lumière sur un arsenal de lutte contre une délinquance tapie dans l'ombre », *AJ Pénal,* n° 7-8, 2017, p. 312-315.

TRICOT Juliette, NIETO MARTIN Adan, « Monitoring of Banking Transactions and Traffic Data » *in* Katalin Ligeti (éd.), *Toward a Prosecutor for the European Union : Draft Rules of Procedure*, Oxford - Portland, Hart, à paraître, vol. 2/2.

TURPIN Dominique, « Les drones, dangers pour la sécurité et pour les libertés », *RFDA* 2024, p. 923 et s.

VERGES Etienne, « Géolocalisation en temps réel d'un téléphone : sauvetage d'une preuve illicite », *AJ Pénal*, 2024, p. 208 et s.

VERGES Etienne, « Quel juge pour contrôler les atteintes aux libertés ? », *Droit pénal* n° 5, Mai 2023, dossier 6.

VERGES Etienne, « La preuve par l'image : symptôme d'un mal aigu. (Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure) », *RSC* 2023, p. 159.

VERGES Etienne, « La procédure pénale technicienne (ou l'asphyxie procédurale), Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice », *RSC* 2019 p. 667.

VERGES Etienne, « L'outil procédural au service de l'efficacité (à propos de la lutte contre la fraude) », *RSC* 2019, p. 155.

VERGES Etienne, « Réforme de la procédure pénale : une loi fleuve, pour une justice au gré des courants - À propos de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la Justice », *Droit pénal* n° 5, Mai 2019, étude 12.

VERGES Etienne, « La procédure pénale au temps des confluences. À propos des visites domiciliaires et saisies instituées par la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme », *RSC* 2018, p.153.

VERGES Etienne, « La procédure pénale à son point d'équilibre (À propos de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale) », *RSC* 2016, p. 551.

VERGES Etienne, « La réforme par transposition : la nouvelle voie de la procédure pénale. Loi n° 2015-993 du 17 août 2015 portant adaptation de la procédure pénale au droit de l'Union européenne », *RSC* 2015 p. 683.

VERGES Etienne, « Construire la norme en procédure pénale : une étude des techniques juridiques à travers un cas symptomatique, la géolocalisation », *RSC* 2014, p. 599.

VERGÈS Étienne, « Le contrôle graduel des preuves technologiques », *Revue pénitentiaire et de droit pénal*, nº 4, 2013, p. 897.

VERGES Etienne, « Émergence européenne d'un régime juridique du suspect, une nouvelle rationalité juridique », *RSC* 2012, p. 635.

VERGÈS Étienne, « La notion de “renseignement” et sa fonction en procédure pénale (à propos d’une dénonciation anonyme) », *Revue pénitentiaire et de droit pénal*, nº 4, 2011, pp. 885-888.

VERMEULEN Mathias, « Secrecy trumps location: a short paper on establishing the gravity of privacy interferences posed by detection technologies », in *Privacy and new technologies*, Madrid, ATI, 2013, pp. 23-25.

VERNY Édouard, « Des surveillances nouvelles en droit pénal », *Les droits et le droit, Mélanges dédiés à Bernard Bouloc*, Dalloz, 2007 p. 1141.

VERVAELE John A. E., « Mesures de procédure spéciales et respect des droits de l’homme - Rapport général », *Utrecht Law Review*, nº 2, vol. 5, 2009, pp. 110-152.

VIOLEAU Olivier, « Les techniques d'investigations numériques : entre insécurité juridique et limites pratiques », *AJ Pénal*, n° 7, 2017, p. 324-326.

WIEWIOROWSKI Wojciech R., « Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy » *in* Gert Vermeulen, Eva Lievens (éd.), *Data protection and privacy under pressure. Transatlantic tensions, EU surveillance and big data*, Anvers - Apeldoorn - Portland, Maklu, 2017, pp. 171-192.

ZIENTARA-LOGEAY Sandrine, « Open data des décisions des tribunaux judiciaires : une nouvelle étape novatrice », *Dalloz Actualité*, 11 janvier 2024.

IX – TEXTES, DOCUMENTS ET PUBLICATIONS OFFICIELLES

A- PUBLICATIONS OFFICIELLES

CANAYER Agnès, BONNECARRÈRE Philippe, *Rapport d’information fait au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d’administration générale (1) sur les modalités d’investigation recourant aux données de connexion dans le cadre des enquêtes pénales*, enregistré à la Présidence du Sénat le 15 novembre 2023.

ESTROSI Christian, *Rapport fait au nom de la Commission des lois constitutionnelles, de la législation et de l’administration générale de la République sur le projet de loi, adopté par le Sénat après déclaration d’urgence (n°381), pour la sécurité intérieure*, enregistré à la Présidence de l'Assemblée nationale le 18 décembre 2002.

FAUCHON Pierre, *Rapport n°486 (97-98), Commission des lois, « Alternative aux poursuites, renfort de l’efficacité de la procédure pénale et délégation aux greffiers des attributions dévolues par la loi aux greffiers en chef ».*

RUDLOFF Marcel, MARCHAND Philippe, *Rapport n° 408, fait au nom de la commission mixte paritaire chargée de proposer un texte sur les dispositions restant en discussion du projet de loi modifiant le code de procédure pénale et relatif à la détention provisoire*, déposé au Sénat le 22 juin 1998.

KERVRAN, Loïc et MIS, Jean-Michel, Rapport d’information par la mission d’information commune sur l’évaluation de la loi du 24 juillet 2015 relative au renseignement (n° 3069), enregistré à la Présidence de l’Assemblée nationale le 10 juin 2020.

Rapport n° 508 enregistré à la Présidence de l'Assemblée nationale le 18 déc. 2002 fait au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi, adopté par le Sénat après déclaration d'urgence, pour la sécurité intérieure.

WARSMAN Jean-Luc, *Rapport fait au nom de la Commission des lois sur le projet de loi (n°784) portant adaptation de la justice aux évolutions de la criminalité, déposé le 20 mai 2003.*

B- LOIS

Loi n° 2023-1059 du 20 novembre 2023 d'orientation et de programmation du ministère de la justice 2023-2027.

Loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire.

Loi n° 2021-1017 du 2 août 2021 relative à la loi de bioéthique.

Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

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.

Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation.

Loi n° 2013-1117 du 6 décembre 2013 relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière.

Loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance.

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.

Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques.

Loi n° 85-1407 du 30 décembre 1985 portant diverses dispositions de procédure pénale et de droit pénal.

C- CIRCULAIRES

Circulaire du 2 décembre 2016 de présentation des dispositions de la loi n° 2016-73 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relative au renforcement du dispositif en matière de lutte contre la délinquance et la criminalité organisée, NOR : JUSD1635582C.

Circulaire du 27 mai 2019 relative à la présentation des dispositions de procédure pénale de la loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice relatives à l'enquête et à l'instruction applicables au 1er juin 2019, NOR : JUSD1915381C

D- TEXTES INTERNATIONAUX ET EUROPÉENS

1- Conseil de l'Europe

Convention sur la cybercriminalité signée à Budapest, le 23 novembre 2001.

Livre blanc sur le crime organisé transnational, Conseil de l'Europe, 2014.

Comité de la Convention sur la cybercriminalité (T-CY), Rapport d'évaluation, Mise en oeuvre des dispositions de la Convention de Budapest en matière de préservation des données, Strasbourg, 25 janvier 2013, (2012) 10 REV.

2- Union européenne

Règlement 2023/1543 du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale.

Directive (UE) 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données (directive « police-justice »).

Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE *(abrogée)*.

Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; abrogée par le Règlement (UE) 2016/679 général sur la protection des données du 27 avril 2016 (RGPD).

Directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications ; abrogée par la directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

Résolution du Parlement européen du 11 juin 2013 notamment (2012/2117 (INI)).

X - JURISPRUDENCE

A- Française

1- Administrative

CE, assemblée, 21 avril 2021, *French data network,* req. n° 393099,.

2- Constitutionnelle

Conseil constitutionnel, décision du 17 juin 2022, n° 2022-1000 QPC.

Conseil constitutionnel, décision du 20 mai 2022, n° 2022-993 QPC.

Conseil constitutionnel, décision du 8 avril 2022, n° 2022-987 QPC.

Conseil constitutionnel, décision du 3 décembre 2021, n° 2021-952 QPC.

Conseil constitutionnel, 21 mars 2019, n° 2019-778 DC.

3- Judiciaire

Crim., 1er octobre 2024, n° 24-80.363.

Crim., 28 mai 2024, n°23-86.390.

Crim., 27 février 2024, n° 23-81.061.

Crim., 8 novembre 2023, n° 23-81.636.

Crim., 10 mai 2023, n° 22-84.475.

Cass., ass. plén., 7 novembre 2022, n° 21-83.146.

Crim., 25 octobre 2022, n° 21-85.763.

Crim., 11 octobre 2022, n° 21-85.148.

Crim. 12 juillet 2022, n° 21-86.652.

Crim. 12 juillet 2022, n° 21-84.096.

Crim. 12 juillet 2022, n° 21-83.820.

Crim. 12 juillet 2022, n° 21-83.710.

Crim. 12 janvier 2021, n° 20-84.045.

Crim. 13 oct. 2020, n° 20-80.150.

Crim., 9 mai 2018, n° 17-86.558.

Crim., 19 mars 2014 n°10-88725 et 13-88616.

Crim., 8 août 2007, n° 07-84.252 : Bull. crim., 2007, n° 188.

Crim., 8 novembre 2005, n°05-84822.

Crim., 14 septembre 2005, 05-84.021.

Crim., 17 décembre 2002, n° 02-83.679 : Bull. crim., 2002, n° 231.

Crim., 24 octobre 2001, n°00-86.440.

Crim., 19 mars 1991, n° 90-86.987, Bull. crim., 1991, n° 401.

Crim. 26 novembre 1990, Bull. crim., 1990, n° 401.

Crim. 15 mai 1990, n° 90-80.827.

Cass., ass. plén., 24 novembre 1989 n° 89-84.439, Bull. civ., 1989, n° 2.

Crim. 13 juin 1989 (Derrien), n° 89-81.388, 89-81.709 Bull. crim., 1989, n° 254.

Crim. 23 juillet 1985, Bull. crim., 1985, n° 275.

Crim. 24 avril 1984, n° 83-90.752, Bull. crim., 1984, n° 142.

Crim. 23 avril 1981, Bull. crim., 1981, n° 117.

Crim. 9 octobre 1980, n° 80-93.140, Bull. crim., 1980, n° 255.

Crim. 12 juin 1952 (Imbert), Bull. crim. n° 153.

B- Étrangère

1-Allemande

BVerGericht Census Acte case,15 décembre 1983.

BVerGericht Décis. 2 BvR 2101/09, 9 novembre 2010.

BVerGericht 1er octobre 2024, 1 BvR 1160/19.

2- Belge

Cour constitutionnelle, arrêt n° 57/2021 du 22 avril 2021.

2- Italienne

Cassazione Penale, Sez. VI, 2 novembre 2023, n. 44154/23.

Cassazione Penale, Sez. IV, 15 luglio 2022, n° 32915/22.

C- Européenne

1- CEDH

CEDH, 17 octobre 2024, *A.L. et E.J. c. France*, n° 44715/20 et 47930/21.

CEDH, 15 février 2024, *Škoberne c. Slovénie*, n° 19920/20.

CEDH (GC), 25 mai 2021, *Big Brother Watch e.a. c. Royaume-Uni*, n° 58170/13, 62322/14 et 24960/15.

CEDH (GC), 25 mai 2021, *Centrum för Rättvisa c. Suède*, n° 35252/08.

CEDH, 8 février 2018, *Ben Faiza c. France*, n° 31446/12.

CEDH (GC), 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06.

CEDH, 2 septembre 2010, *Uzun c. Allemagne*, n° 35623/05.

CEDH, 2 décembre 2008, *K.U. C. Finlande*, n° 2872/02.

CEDH, 25 mars 1999, *Pélissier et Sassi c. France*, n° 25444/94.

CEDH, 18 mars 1997, *Mantovanelli c. France*, n° 21497/93.

CEDH, 24 avril 1990, *Kruslin et époux Huvig c. France*, n° 11801/85 et 11105/84.

2- CJUE

CJUE (grande chambre) 4 octobre 2024, *CG contre Bezirkshauptmannschaft Landeck*, C-548-21.

CJUE (dixième chambre) 13 juin 2024, *Procédure pénale contre HYA e.a.*, C- C-229/23.

CJUE (grande chambre), 30 avril 2024, *Procédure pénale contre M.N.*, C-670/22 (Encrochat).

CJUE (Assemblée Plénière), 30 avril 2024, *QDN e.a.*, C-470/21 (Hadopi).

CJUE (grande chambre) 30 avril 2024, *Procédures pénales contre Inconnus*, C-178/22.

CJUE, 7 mars 2024, (sixième chambre) 7 mars 2024, *Endemol Shine Finland Oy*, C-740/22.

CJUE (grande chambre), 30 janvier 2024, *NG contre Direktor na Glavna direktsia « Natsionalna politsia » pri Ministerstvo na vatreshnite raboti – Sofia*, C-118/22.

CJUE, 7 septembre 2023, *A.G.*, C-162/22.

CJUE, 17 novembre 2022, *Spetisalizirana prokuratura*, aff. C-350/21.

CJUE (grande chambre), 20 septembre 2022, *Spacenet*, C-793/19.

CJUE (grande chambre), 5 avril 2022, *Commissionner of An Garda Siochàna*, C-140/20.

CJUE, 16 décembre 2021, *Spetsializirina prokuratura*, C-724/19 (Données rela tives au trafic et à la localisation).

CJUE (grande chambre), 2 mars 2021, *Prokuratuur*, C-746/18 (conditions d'accès aux données relatives aux communications électroniques).

CJUE (grande chambre), 6 octobre 2020, *La Quadrature du Net*, C-511/18.

CJUE (grande chambre), 2 octobre 2018, *Ministerio Fiscal*, C-207/16.

CJUE (grande chambre), 21 décembre 2016, *Télé2-Sverige*, C-203/15.

CJUE (grande chambre), 8 avril 2014, *Digital Rights Ireland*, C-293/12 et C-594/12.

XI - ARTICLES DE PRESSE

STROOBANTS, Jean-Pierre, Criminalité organisée : le démantèlement de la messagerie EncroChat a permis d'arrêter plus de 6 500 personnes, *Le monde*, 27 juin 2023.

UNTERSINGER Martin, « Que sont les IMSI-catchers, ces valises qui espionnent les téléphones portables ? », *Le monde*, 31 mars 2015.

XII - PODCASTS

Esprit de justice, « Qu'est-ce que la sécuritisation ? », *France culture*, 3 mars 2021 (https://www.radiofrance.fr/franceculture/podcasts/esprit-de-justice/qu-est-ce-que-la-securitisation-6478211)

Table des matières

SOMMAIRE **7**

INTRODUCTION **9**

PREMIERE PARTIE : USAGES **19**

SECTION 1 : L'USAGE DES NTIS, DES MOTS AUX ACTES 20
§1.- Les mots et les définitions *21*
§2.- Les actes : une énumération ouverte et opératoire *21*
SECTION 2 : UNE QUESTION DE MESURE(S) 23
§1.- Mesure de la nouveauté *23*
I.- Le tournant 23
II.- Les NTIS entre monde réel et monde virtuel 24
III.- Une perpétuelle nouveauté 25
§2.- Mesure de l'utilité *26*
I.- Un besoin 26
II.- Efficacité 28
§3.- Mesure des limites *28*
I.- Instrument de mesure 28
A.- Mesure de l'activité 28
B.- Mesure de l'impact 29
II.- Des repères vacillants 30
III.- Technicité des mesures 31
A.- Difficultés techniques pour les spécialistes 32
B.- Incompréhension pour les profanes 32
C.- La tentation du contournement ? 33
IV.- Dépendance aux opérateurs 34
V.- Valeur de la preuve obtenue par une mesure NTIS 35
A.- Un élément de preuve parmi d'autres 35
B.- Une preuve technique difficile à discuter judiciairement 36
§4.- Mesure ou démesure *37*
I.- Ubiquité des données et coopération internationale 37
II.- Question de la proportionnalité des mesures à l'atteinte aux droits fondamentaux 39
SECTION 3 : COMMUNAUTES PROFESSIONNELLES 41
§1.- Une communauté soudée *41*
§2.- Nouveaux métiers et nouvelle configuration du secteur privé *42*
I.- Nouveaux métiers 42
A.- Les experts en informatique : une fonction en appui des missions de police judiciaire 42
1) Les spécialistes de la technologie numérique de la gendarmerie : constater sans agir 43
2) Les spécialistes de la technologie numérique de la police nationale : investiguer sans enquêter 45
B.- Les référents cyber auprès des magistrats : une fonction de communication des enjeux techniques 46
II.- Rôle du secteur privé 47
CARTOGRAPHIE DES ACTEURS DU RECUEIL ET DE L'ADMINISTRATION DU RENSEIGNEMENT ET DE LA PREUVE NUMERIQUES 51
Lien vers la cartographie en ligne *51*
Note explicative : *51*
I.- Présentation de la cartographie 51
II.- Méthodologie de confection de la cartographie 53
DEUXIEME PARTIE : NORMES **57**
SECTION 1 : GENEALOGIE DES MESURES NTIS 57
§1.- L'apparition des mesures NTIS *57*
I.- La distinction entre ancien et nouveau 58
II.- De la pratique à la loi 60
§2.- L'évolution des mesures NTIS *64*
I. - Du tangible au cybermonde : l'adaptation heurtée des outils de l'enquête 64
II.- De l'exceptionnel au droit commun 67
SECTION 2 : REGIMES DES MESURES NTIS 69
§1.- Le régime ordinaire des mesures NTIS *70*
§2.- Le régime spécifique des mesures NTIS *72*

§3.- Le régime dérogatoire des mesures NTIS *78*
Conclusion *80*
TROISIEME PARTIE : PERSPECTIVES **83**
SECTION 1 : DESTABILISATION DES REPERES DE LA PROCEDURE PENALE 83
§1.- La « dataisation » ou la mise en données du monde *83*
I.- Décrire la bascule numérique 84
A.- Le moment numérique 84
B.- La source numérique : la donnée 85
C.- Des ressources numériques pour la procédure pénale 86
II.- Nommer les transformations numériques 88
§2.- La transnationalisation ou la mise en réseaux du monde *92*
I.- Brouillage des « frontières » 92
II.- Dépassement du territoire 93
§3.- La « sécurisation » ou la mise sous surveillance du monde *94*
I.- Essor de la sécurité 94
II.- Promotion du renseignement 94
SECTION 2 : RECONFIGURATION DE L'ENQUETE PENALE 96
§1.- Émergence de la donnée numérique pénale *96*
I.- La construction extra-juridique de la donnée numérique pénale 97
II.- La construction juridique de la donnée numérique pénale 98
A.- Paramètres d'une nouvelle configuration 98
1) Typologie des données : la formation d'un nouveau référentiel 104
a) Classification tripartite 104
b) Distinctions supplémentaires 105
L'exemple des adresses IP 105
La variable du facteur temporel 107
2) Disponibilité des données : le préalable de la conservation 107
a) Conditions de licéité de la conservation obligatoire 108
(a1) Classification des modes de conservation 108
(a2) Possibilités et limites de la conservation généralisée et indifférenciée 110
Les données de trafic et de localisation 110
Les seules adresses IP attribuées à la source 111
Les seules données d'identité 112
(a3) Alternatives à la conservation généralisée et indifférenciée : l'enjeu des données de trafic et de localisation 112
Conservation ciblée 112
Conservation rapide 113
Analyse automatisée et recueil en temps réel (pour le compte ou par les services de renseignement) 114
b) Conditions de licéité de la conservation facultative 114
3) Accessibilité des données : les possibilités d'accès 115
a) Principe de séparation des régimes de conservation et d'accès 115
b) Régime propre de l'accès 116
Objectifs légitimes 116
Exigence générale de proportionnalité 118
Condition de stricte nécessité 119
Exigences complémentaires de garantie judiciaire et de droit à l'information. 120
Champs et portée différenciée 121
4) Exploitabilité des données : les conditions d'utilisation 123
a) Principe d'équivalence 124
b) Principe d'effectivité 124
B.- Préférences de la nouvelle configuration 125
1) Marges 125
2) Variables (constitutionnelles) 126
a) L'option de la conservation ciblée 127
b) La préférence pour la conservation rapide 127
§2.- Au-delà de la donnée numérique pénale 129
I.- La proportionnalité de l'accès aux éléments de preuve 130
II.- Le contrôle préalable de l'accès aux éléments de preuve 132
III.- La sanction d'un accès irrégulier aux éléments de preuve 133
IV.- L'information sur l'accès aux éléments de preuve 135
CONCLUSIONS **137**
ANNEXES **141**
Liste des entretiens 142
Questionnaire type 144
Journées d'études 147
Glossaire 156
BIBLIOGRAPHIE **162**

À l'origine de la recherche, on trouve la tentative du législateur de systématiser l'encadrement des nouvelles technologies d'investigation et de surveillance (NTIS) dans le contexte de l'enquête pénale par l'élaboration de la catégorie des « autres techniques spéciales d'enquête » de l'article 706-95-11 du Code de procédure pénale. Pourtant, en tirant ce mince fil, est d'emblée apparu un double obstacle : la catégorie ne couvre pas toutes les mesures qui pourraient être qualifiées de NTIS ; elle ne prend pas en compte le fait que ces technologies sont également utilisées à l'extérieur de la procédure pénale, à des fins de protection de la sécurité nationale.

Pour aborder cet objet fuyant, il convenait de se fixer des objectifs modestes : saisir les ressorts de la construction de la catégorie dans ce maquis de textes d'origine et de nature diverses qu'est devenue la procédure pénale, interroger les acteurs qui, tout au long de la procédure qui fait vivre les textes, s'y confrontent ; mesurer les innovations et les continuités avec les techniques plus traditionnelles d'enquête ; apprécier une éventuelle distorsion entre les nouvelles technologies d'investigation et de surveillance et les grands principes qui gouvernent la procédure pénale. Rapidement il est apparu que les usages comme les normes relatives aux nouvelles technologies d'investigation et de surveillance sont à la fois révélateurs et moteurs de mutations profondes qui affectent l'enquête pénale depuis une trentaine d'années, qui plus est dans un monde pris dans le tourbillon de la production, de la conservation et de l'utilisation des « données » (data) et dans la dynamique d'une surveillance toujours plus poussée. Replacées dans ce contexte, les nouvelles technologies, utilisées sous la forme actuelle ou sous une autre, ne pourraient-elles pas permettre de faire levier entre les pratiques polymorphes et mouvantes de l'enquête et les principes de la procédure qui ont vocation à la stabilité et la généralité ? C'est à cette question que répond le rapport qui examine successivement les usages dont font l'objet les NTIS, les normes qui les encadrent puis les perspectives qu'ouvre la confrontation des usages et des normes. Il en résulte que les acteurs de la procédure pénale se sont résolument emparés des nouvelles technologies d'investigation et de surveillance, qu'ils les mettent en œuvre avec un grand sérieux et, partant, beaucoup de questionnements, que les NTIS mettent en lumière plus que jamais le besoin de coopération entre les acteurs de la chaîne pénale, que les normes en la matière sont touffues et que les NTIS sont loin d'obéir à un régime unique et homogène. Au final, la construction de la preuve pénale, qui est le but du recours aux NTIS, apparaît largement imprégnée par le droit des données personnelles. Trois phases se dégagent : la conservation qui commande la disponibilité des données potentiellement susceptibles de constituer des éléments de preuve, l'accès qui détermine leur mise à disposition, leur recueil et la phase d'exploitation qui conditionnent leur utilisation.

Florence BELLIVIER, Professeure à l'Université Paris 1 Panthéon Sorbonne

Juliette TRICOT, Maîtresse de conférences à l'Université Paris Nanterre

cd·pc CENTRE DE DROIT PENAL ET DE CRIMINOLOGIE

Université Paris Nanterre

Institut des Études et de la Recherche sur le Droit et la Justice