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

SYNTHÈSE 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.

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

NOTE DE SYNTHESE

1/ Problématique retenue et objectifs de la recherche

Conçue en réponse à un appel à projets du GIP Mission de recherche Droit et Justice – devenu depuis Institut des études et de la recherche sur le droit et la justice – intitulé « L'appréhension des nouvelles technologies d'investigation et de surveillance par la procédure pénale », la recherche trouve son point de départ dans la tentative du législateur de systématiser l'encadrement des nouvelles technologies d'investigation et de surveillance (NTIS)[1] dans 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 créé par l'article 46 de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme de la justice. En répondant à l'appel d'offres puis en nous mettant à l'ouvrage après avoir obtenu le financement, nous étions loin de nous douter qu'à partir de cette curieuse catégorie, qui se présente formellement comme résiduelle (« autres ») et qui comprend le recueil des données techniques de connexion et des interceptions de correspondances émises par la voie électronique (art. 706-95-20 CPP), les sonorisations ou fixations d'images de certains lieux ou véhicules (art. 706-96 à 706-98 CPP), la captation de données informatiques (art. 706-102-1 à 706-102-5 CPP), nous voyagerions vers des contrées très différentes, les unes connues, les autres moins : les arcanes de ce qui est devenu le quotidien de l'enquête, à savoir un grand nombre de techniques d'investigation et de surveillance, nouvelles ou moins nouvelles, spéciales ou moins spéciales, numériques d'emblée ou mimant leurs sœurs du monde réel ; un vocabulaire à la fois technique et souvent imprécis ; les conséquences néfastes, pour toute la procédure pénale, de l'absence d'indépendance statutaire du Parquet ; la définition de ce qu'est une preuve (par rapport à une trace, un indice, une donnée brute, une information, une information contenue dans un fichier, etc.), le rôle du secteur privé dans la production de la preuve ; la place de la procédure pénale dans le champ de la surveillance, dont l'étude relève largement de la science politique, notamment la surveillance qualifiée, à tort ou à raison, de participative ; et, surtout, le continent du droit des données personnelles, dont l'exploration nous a *in fine* conduit à voir – et faire – émerger la catégorie de donnée numérique pénale.
L'ampleur du champ d'étude couvert par les NTIS était d'autant moins perceptible d'emblée que ce qui est apparu d'abord, ce sont les trois limites de la catégorie la plus simple à appréhender en première intention malgré son caractère résiduel, les techniques spéciales

[1] Ensemble indéterminé des « nouvelles technologies » introduites en droit français afin de « renforcer les outils de surveillance et d'investigation », Texte de l'appel à projets, 2020.

d'enquête (TSE) *stricto sensu* : elle touche à la procédure pénale dans ce que celle-ci a de particulier, voire d'exceptionnel, comme en témoigne l'adjectif « spécial » qui 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) puis semble par glissement qualifier l'enquête (ou plutôt la criminalité grave qui autorise le recours à des pouvoirs dérogatoires, *i.e.* spéciaux) ; elle ne couvre en réalité pas toutes les mesures qui pourraient être qualifiées de (nouvelles) technologies d'investigation et de surveillance ; 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, et, partant, réglementées par le Code de la sécurité intérieure. C'est cette relative porosité de deux champs – le renseignement et la procédure pénale – traditionnellement distincts, conjuguée au besoin de se repérer dans un environnement peuplé d'acteurs multiples et nombreux, qui a fait naître l'idée d'une cartographie des acteurs du recueil et de l'administration du renseignement et de la preuve numériques[2]. L'exercice, peu commun pour les juristes, s'est révélé offrir un instrument précieux d'accompagnement et d'orientation de la recherche ainsi que, nous l'espérons, un outil utile pour les futurs chercheurs. Mettre en carte qui est habilité à faire quoi à quelles fins, dans le monde du renseignement comme dans la procédure pénale, ainsi que les procédés de communication entre les deux sphères est ainsi une méthode fructueuse d'appréhension et de dévoilement de la scène sur laquelle opèrent les NTIS. Quant au résultat qui en découle, outre qu'il rend visibles et sensibles la variété des acteurs et de leurs relations et, ce faisant, la complexité du champ d'étude, il donne à voir par comparaison l'élaboration moindre du dispositif de l'enquête pénale.

A cette première difficulté tenant à la délimitation de l'objet et du champ s'ajoute celle qui résulte du vocabulaire employé pour le décrire, spécialisé mais souvent imprécis. On se contentera de trois exemples de la complexité de l'intégration d'une certaine technicité dans la langue du droit : d'un côté la loi recourt à des périphrases et des renvois complexes pour décrire certaines technologies, celle de l'*IMSI-catcher* par exemple[3], de l'autre elle continue à utiliser, pour désigner une écoute téléphonique, le vieux terme de « correspondance » que l'on associe spontanément plus volontiers à un écrit qu'à un message oral, enfin, depuis une dizaine d'années, les juges et la doctrine évoquent à longueur d'arrêts et d'articles la « conservation généralisée et indifférenciée » des données de connexion sans – ou si rarement – s'interroger sur ce qu'apporte un des adjectifs par rapport à l'autre. Pour franchir l'obstacle, il est utile de disposer d'un premier instrument de déchiffrement ou plus exactement de traduction de la langue juridico-technico-technologique. Tel est le but du glossaire proposé en annexe du rapport.

En l'absence d'un champ bien circonscrit et d'un vocabulaire fixé et accessible, on aurait alors pu imaginer pouvoir commencer à se repérer grâce aux questions que se pose tout enquêteur : qui ? Où ? Comment ? On aurait alors pu partir du type d'information recherchée pour sérier les mesures qui permettent de répondre à chacune de ces trois questions. Mais alors qu'on espérait ainsi ordonner les mesures, c'est un surcroît de désordre qui s'est dégagé. Ainsi la localisation des personnes ou des objets, qui peut être réalisée en temps réel ou *a posteriori*, est notamment permise par le recueil des données techniques de connexion (*i.e.* le recours à un

[2] Lien vers la version dynamique de la cartographie : https://miro.com/welcomeonboard/T3AwZllmeUNjYUNPdE5qVXY0WE96bHRLaFRGZTJjNHBUVFA5UEM5SFNNZDhPY25UN0VVY3RIalF1RmZlRXFQcnwzNDU4NzY0NTU3NjM5MjkwMTI3fDI=?share_link_id=444640732862

[3] Appareil qui simulant une fausse antenne-relais intercepte toutes les données de communication circulant dans un rayon donné.

IMSI-Catcher) 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 télécommunications) 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 », modalité à l'appellation mystérieuse et originale issue du droit international) des données conservées par les 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).

Pour aborder cet objet essentiellement fuyant, les chercheurs de l'équipe se sont dès lors fixé des objectifs modestes : saisir les ressorts de la construction de l'ensemble des NTIS 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. En réalité, tenter de répondre à ces questions nous a conduits beaucoup plus loin car 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*). L'hypothèse qui a alors été retenue est que, replacées dans le contexte de la mise en données du monde, les technologies d'investigation et de surveillance, nouvelles et moins nouvelles – la notion étant évidemment relative –, pourraient permettre de construire un pont entre les pratiques polymorphes et mouvantes de l'enquête et les grands principes de la procédure qui ont vocation à la stabilité et la généralité.

2/ Justification des choix méthodologiques effectués

L'équipe de recherche a en permanence mené l'analyse sur trois plans qui ont été distingués et entrelacés : l'un empirique, à partir des pratiques des divers acteurs, institutionnels ou privés, intervenant à divers titres dans l'enquête pénale, des usages et non-usages de ces technologies ; l'autre normatif s'attachant au cadre juridique national, européen et international de l'emploi des NTIS, celles-ci étant en outre étudiées une par une par l'équipe élargie (bases textuelles, historique de l'insertion de la mesure en droit français, moteurs ou facteurs d'introduction de la mesure, traits généraux, régimes et modes de justification, mise en œuvre, bibliographie) ; le dernier comparatif, dans une mesure qu'il a fallu recalibrer et qu'il convient de préciser. Si, de prime abord, il pouvait être tentant et utile de mener une véritable étude des NTIS en droit comparé puisque les services d'enquête étrangers y ont aussi recours, il est très vite apparu, sur les conseils des spécialistes étrangers consultés, que compte tenu de l'ampleur, de la complexité et de la fragmentation de l'objet de la recherche, l'apport de la comparaison devrait se limiter à des éclairages du droit français par la réception du droit européen dans les pays concernés (Italie, Belgique, Allemagne, Irlande). Cette façon de procéder a mis en exergue les réactions très variées à la jurisprudence de la Cour de justice de l'Union européenne (CJUE) mais aussi l'émergence d'outils qui pourraient s'avérer utiles à la réflexion française, comme le compte global de surveillance, concept échafaudé dès 2010 par la Cour constitutionnelle allemande et

qui alerte sur la nécessité de mesurer le degré de surveillance acceptable dans une société donnée.

3/ Terrains ou données ayant servi de support à la recherche dans une présentation anonymisée

Pour alimenter la partie empirique, l'équipe de recherche restreinte s'est entretenue, suivant la méthode des entretiens en sciences sociales (questions ouvertes sans réponse induite), 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 officier de police judiciaire, un investigateur en cybercriminalité, un gendarme spécialisé en nouvelles technologies, cinq magistrats (procureurs ou juges des libertés et de la détention (ci-après JLD), dont l'une qui fut avocate pendant de longues années), deux avocats, un personnel d'une entreprise de sécurité spécialisée dans les nouvelles technologies d'investigation, un officier de liaison cyber-gendarmerie, 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 parfois 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 la rencontre, l'enquêté recevait un questionnaire-type que nous avions élaboré et décliné en fonction de nos interlocuteurs et qui a pu être adapté au cours de l'entretien. Parfois celui-ci était enregistré, parfois non. Ils ont tous été transcrits mais nous n'avons pas fait figurer les transcriptions en annexe pour des raisons de confidentialité. Pour ces mêmes motifs, et en accord avec les enquêtés, leurs propos sont repris mais ne leur sont pas nominativement attribués. Seul a été mentionné le métier de chaque enquêté car il permet de situer le propos.
Ainsi pouvons-nous dire qu'au terme de ces presque quatre années de travail, 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 français et étrangers ayant participé aux séminaires qui ont émaillé le processus de recherche.

L'analyse normative a, elle, a été menée de façon classique par le repérage systématique, dans les différents textes concernés, nationaux et internationaux, des mesures objets de l'étude, qui relèvent soit du droit commun, soit de procédures dérogatoires. Quant au premier, figurent dans le livre premier du Code de procédure pénale, 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). Les secondes, nous l'avons vu, sont les « autres » TSE des articles 706-95-11 et suivants auxquelles il faut ajouter l'accès à distance aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique (article 706-95-1 CPP) qui est une technique spéciale d'enquête mais qui n'est pas soumise au régime des « autres » TSE.
Les normes sont rendues plus claires ou, du moins, moins absconses, d'une part, si l'on retrace, au moyen des outils classiques de l'analyse juridique, dont la lecture des travaux préparatoires et de la littérature grise, les méandres de la généalogie de mesures qui relèvent davantage de la technique du millefeuille que d'une systématique, d'autre part si on les confronte à l'épreuve de la jurisprudence, ô combien foisonnante ces dix dernières années, de la chambre criminelle de la Cour de cassation, du Conseil d'État, du Conseil constitutionnel, de la Cour européenne

des droits de l'homme et de la Cour de justice de l'Union européenne relativement à certaines des NTIS.

4/ Principales conclusions de la recherche

Autant nous avons vite su que la recherche comporterait une partie consacrée aux usages et une autre portant sur les normes, autant nous ignorions d'avance l'ordre d'exposition qui nous paraîtrait *in fine* le plus judicieux.
Après l'introduction, le rapport final fait entrer le lecteur de plain-pied dans les usages pour ensuite aborder les normes, et ce pour trois raisons principales.
Tout d'abord la pédagogie recommande d'aborder une matière ultra-technique par ce qui peut la rendre moins aride, à savoir les pratiques des acteurs confrontés aux NTIS, qu'ils les fabriquent, s'en servent, en contrôlent l'usage ou les contestent.
Ensuite, la généalogie des mesures a montré que celles-ci avaient quasiment toutes été utilisées par la pratique avant d'être consacrées par la loi.
Enfin, la réflexion que les acteurs mènent sur leurs propres pratiques met en lumière de façon crue ce que les normes révèlent, à savoir le fait que l'usage des NTIS est en quelque sorte inversement proportionnel à leur intelligibilité et leur cohérence. Autrement dit, nous avons affaire à un dispositif très utilisé en pratique, non moins encadré par des textes d'origine et de nature diverses, complétés par la jurisprudence du Conseil constitutionnel et de la Cour de cassation, d'abord éparse et qui s'emballe ces dernières années – mais dont la fragmentation et le manque de lisibilité et de cohérence sont soulignés par la plupart des praticiens. Les acteurs – policiers ou magistrats – ne connaissent qu'une partie de l'ensemble : l'enquêteur qui, une fois les auteurs de l'infraction identifiés, s'ils le sont, ne connaît pas l'issue de l'affaire, le JLD qui ne saisit pas l'ensemble du dossier (mais une partie à un moment particulier) ni ses suites, et de manière générale les instances diverses qui, à un moment ou un autre, autorisent ou contrôlent la mesure et n'en maîtrisent pas toujours les enjeux techniques, soit parce que ceux-ci sont cachés (secret défense par exemple), soit parce que les acteurs sont insuffisamment formés.

Ici, donc, nous n'observons pas vraiment de discordance entre usages et normes, les deux se présentant comme les deux versants d'une même réalité, à savoir une procédure pénale profondément déstabilisée sous l'effet combiné de divers facteurs, dont une incorporation non réfléchie, au coup par coup, des outils techniques, les mutations de la criminalité, l'absence d'indépendance du Parquet, les nombreux pouvoirs du JLD à qui manque le temps nécessaire pour exercer ses missions correctement, un dialogue des juges internes et européens parfois heurté.

C'est alors que nous sommes parvenus au résultat inattendu de cette recherche : tandis que la jurisprudence déterminante secrétée depuis dix ans par les juges de la Cour de justice de l'Union européenne relativement aux données de connexion aurait pu faire craindre un engloutissement des NTIS dans l'aridité du droit des données personnelles, c'est précisément ce droit qui offre, par son regard d'ensemble, des perspectives de reconstruction de la place des NTIS dans la procédure pénale et, plus généralement, de la procédure pénale. Ce n'est pas à dire que ce droit soit simple d'accès, loin s'en faut, ou qu'il offre des solutions toutes prêtes – il est en pleine construction et sujet à d'intenses controverses. Mais par son objet transversal (la donnée personnelle) et sa source (le droit européen est ici moteur), il permet de jeter une lumière sur les grandes dynamiques qui travaillent la procédure pénale. En effet, les acteurs de celle-ci recourent déjà à des données personnelles de toutes natures (celles qui sont contenues dans les

fichiers ADN par exemple) mais les (nouvelles) technologies d'investigation et de surveillance en produisent d'autres en nombre qui sont détenues par des tiers et ne sont pas toujours pénales d'emblée (par exemple une facture détaillée d'un opérateur téléphonique). Les perspectives suggérées par le droit des données personnelles permettent non seulement de proposer une clé de compréhension des règles souvent déstructurées applicables aux NTIS mais aussi d'aider à faire advenir une procédure pénale à la hauteur des enjeux de notre temps : respectueuse des droits et libertés, à distance tant d'un solutionnisme technologique naïf que d'une phobie de la science et des techniques, tenant compte des bouleversements qui affectent le droit de la preuve, permettant la coopération internationale pour prévenir et réprimer les actes attentatoires aux normes sociales fondamentales.

Le rapport est dès lors construit tel une fusée à trois étages : usages, normes, perspectives, correspondant à trois parties qui, cohérentes dans la mesure où les mêmes éléments s'y retrouvent mais abordés sous des angles différents, sont aussi indépendantes, au sens où l'on peut lire l'une sans les autres.

La partie consacrée aux usages, fortement imprégnée des mots utilisés par les acteurs rencontrés, a mis en évidence trois constats.

Tout d'abord, ceux qui pratiquent quotidiennement les NTIS n'appréhendent pas cet ensemble avec certitude, qu'il s'agisse des mots mêmes ou des actes qui relèvent de la catégorie. D'après les réponses apportées aux trois questions suivantes : « Qu'évoque pour vous la formule "technologies ou techniques d'investigation et de surveillance" ? », « Avez-vous / êtes-vous amené 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 le syntagme « nouvelles technologies d'investigation et de surveillance » n'est pas utilisé en tant que tel par les praticiens, il est toujours évocateur pour eux. Ils les désignent par un vocabulaire qu'ils ont parfois adapté et ils deviennent prolixes à partir du moment où ils quittent le terrain des définitions pour aborder celui de l'énumération de ce qu'ils font et ne font pas en pratique.

Ensuite, les personnes interrogées sont allées plus loin en exprimant des points de vue qui ne convergeaient pas toujours. En effet, une fois l'objet et les usages sémantiques à peu près identifiés, nous sommes entrés dans le vif du sujet en interrogeant plus avant 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 ; mesure de l'utilité qu'elles procurent ; mesure des limites rencontrées dans la mise en œuvre des NTIS ; mesure d'une éventuelle démesure ou disproportion dans le recours aux NTIS.
S'agissant, en premier lieu, de mesurer la nouveauté des NTIS, celle-ci doit être relativisée. Certains acteurs proposent un tournant qui remonte déjà à 20 ans environ, tandis que d'autres soulignent une homologie entre monde réel et monde virtuel (par exemple entre la perquisition de documents papier dans un domicile et une perquisition informatique). Il reste que la nouveauté semble provenir du caractère toujours évolutif des mesures.
Quand il faut, en second lieu, mesurer l'utilité des mesures, sans surprise – car l'enquête pénale utilise depuis longtemps des moyens techniques et scientifiques comme la balistique, les empreintes digitales ou génétiques – les acteurs soulignent que le recours aux NTIS est fréquent, routinier, parallèle à l'avènement des technologies en général. C'est qu'elles répondent à des besoins et qu'elles sont efficaces, même si ce dernier point est parfois discuté.
En effet, en troisième lieu, 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 ; des repères vacillants sur les conditions du recours à l'une ou l'autre, ce qui peut faire peser un risque sur la procédure ; leur technicité ; la dépendance aux opérateurs privés ; la valeur probante des preuves obtenues par leur biais, preuves comme les autres mais plus difficiles à discuter dans l'arène judiciaire.
Finalement, en quatrième lieu, si l'on envisage cette fois la mesure de la mesure, à deux égards au moins les mesures NTIS sont mises à l'épreuve : 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, par exemple si un enquêteur veut saisir des informations stockées dans un *cloud* ; les acteurs 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, certains pensant que la fin justifie les moyens ou que la jurisprudence européenne est hors sol, tandis que d'autres voudraient pouvoir pied à pied discuter en justice les modes de preuve et les preuves obtenues par le recours à ces mesures, des positions hésitantes ou conciliatrices s'exprimant aussi.

De manière structurelle, 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 et de reconfiguration d'une communauté professionnelle. 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, parfois pour la regretter, 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 ». Outre la création ou l'activation de réseaux formels et informels rassurants pour discuter de la technicité de tel ou tel point et se sentir en confiance, ou encore pour se former, 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. En outre, le secteur privé joue un rôle croissant dans la conception et la mise en œuvre des NTIS, 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 réquisitions du juge d'instruction ou du procureur à la demande d'un officier de police judiciaire dans le cadre d'une enquête. L'intervention du secteur privé dans ce domaine soulève des questions liées à l'ouverture de l'accès (sources ouvertes ou fermées) et de lieu de stockage des données. Si la souveraineté numérique est considérée par certains comme un enjeu de taille, la concentration des acteurs vers laquelle elle tend pourrait s'avérer un facteur de vulnérabilité si les données rassemblées étaient collectées par des tiers malveillants ou l'objet d'un mésusage interne[4].

La partie portant sur les normes les appréhende au travers d'une généalogie, puis par l'étude des régimes.

[4] A. Canayer et P. Bonnecarrère, *Rapport d'information (n°110) sur les modalités d'investigation recourant aux données de connexion dans le cadre des enquêtes pénales*, Sénat, 15 novembre 2023.

En premier lieu, la généalogie des mesures NTIS révèle combien leur apparition comme leur évolution 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.
L'étude de l'apparition des mesures relativise leur caractère « nouveau » en ce que certaines ont été conçues et appliquées d'abord en dehors du numérique (par exemple une perquisition numérique qui a son double dans le monde réel), contrairement à d'autres qui sont « nées » dans le monde numérique, ainsi de la captation des données informatiques. Par-delà cette distinction relative au contexte d'apparition, la généalogie des mesures NTIS montre qu'elles sont presque toutes nées de la pratique, ce qui unifie en quelque sorte leurs histoires respectives.
L'événement marquant qui a obligé le législateur français à suivre 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 (ratifiée par la France le 1er mai 2006) que le législateur français a transposée, d'une part, en adaptant les mesures d'enquête existantes à la technologie numérique du moment et, d'autre part, en intégrant au fur et à mesure de l'avancement technologique des mesures d'enquête fondées sur des nouvelles technologies et techniques.
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. 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. Si les mesures ont été consacrées par le législateur au fil de l'eau, c'est aussi qu'elles étaient utilisées en pratique avant d'être introduites dans le droit positif. Leur intégration *ex post* 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, choisissant de reconnaître et « sécuriser » les possibilités ou besoins nouveaux issus des évolutions technologiques dans le domaine du numérique et éprouvés par la pratique.
Ainsi, chaque intervention du législateur pour valider une mesure déjà employée en pratique a eu un caractère ponctuel et aucune n'a procédé d'une approche globale, à la notable exception près – significative d'une prise de conscience du législateur lui-même – de l'introduction en droit français des (autres) « techniques spéciales d'enquête », effectuée par le biais d'une même loi et régies par les mêmes règles. Cela ne peut manquer de rejaillir sur le(s) régime(s) des NTIS.
L'analyse 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 : d'une part, l'adaptation sans grande prudence des mesures d'investigation « classiques » à l'univers numérique (ainsi, 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) ; d'autre part, l'extension progressive mais continue, de l'exceptionnel vers le droit commun, de la portée des mesures NTIS consacrées par le législateur.

En second lieu, 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. Par-delà l'existence de certains traits communs, la

consécration des mesures NTIS en droit positif présente aussi d'importantes différences de sorte que le singulier doit céder la place au pluriel : ce sont trois régimes qui coexistent et non un seul pour l'ensemble des mesures NTIS.
Tout d'abord, 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. Il en va ainsi des perquisitions, des saisies et des réquisitions numériques qui suivent le régime de leurs homologues du monde réel, sans qu'une réflexion n'ait véritablement été menée sur la façon éventuellement différenciée dont ces mesures (réelles, virtuelles) affectent la vie privée.
Ensuite, 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. 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, des réquisitions de données informatiques stockées ainsi que de la conservation rapide des données informatiques, étant souligné que la distinction entre ces deux derniers types de mesure n'est pas clairement arrêtée. 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.
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. La *ratio legis* de l'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, ce qui a donné lieu à une jurisprudence très étoffée des deux cours européennes et à un processus de réception complexe en France.
Enfin, 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, le 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. Toutefois, les textes n'excluent pas le risque de relativisation de la notion d'infraction grave comme critère pour l'application de ces mesures NTIS, notion au cœur de la jurisprudence développée par les deux cours européennes à propos des données personnelles et de la mise en œuvre des mesures de surveillance non seulement dans le domaine pénal mais aussi dans celui du renseignement.

Fondées sur une règle logique selon laquelle plus un acte est intrusif dans la vie privée, plus il réglementé, ces différents régimes révèlent une hiérarchisation des mesures NTIS. Toutefois cette gradation reste implicite et insuffisante car la notion d'intrusion n'est pas définie. En outre, l'appréciation de l'intensité de l'intrusion dans la vie privée s'effectue à l'aune plutôt des moyens utilisés (accès en temps réel ou différé) que des résultats obtenus (catégorie des données

auxquelles l'accès a été donné). Dès lors, on 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 » et d'identification des critères permettant de la rendre opératoire émousse encore davantage les distinctions entre les différents régimes des mesures NTIS, les privant ainsi de la cohérence et de l'articulation internes souhaitables.

Dès lors la troisième partie de la recherche (Perspectives) s'efforce de ne pas en rester au constat du vacillement des repères qui, en tout état de cause, déborde et dépasse largement le champ de l'enquête pénale. En effet, 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, en particulier de prise en compte du phénomène de « dataisation », ou « datafication » selon le néologisme anglais plus élégant, qui désigne la « mise en données »[5] du monde. Cette lame de fond se produit à la faveur d'un autre processus qu'elle alimente en retour : la transnationalisation.
La dataisation aboutit à renommer les transformations numériques et notamment à repérer les fausses évidences liées à la prétendue neutralité d'un vocable comme celui d'« accès » ou encore à interroger les soubassements des expressions européennes de « preuve électronique » ou de « procédure pénale numérique ».
La transnationalisation invite quant à elle à prendre la mesure du dépassement du territoire par une réponse du droit et de la procédure pénale dont les contours et les limites sont profondément perturbés.
Mise en données et mise en réseaux, ces deux processus convergent vers une mise sous surveillance du monde, que favorisent les mécanismes d'anticipation, d'exception et la porosité entre le renseignement et la procédure pénale, notamment *via* la circulation entre ces deux sphères de données pouvant servir à produire des preuves, déclencher ou orienter une enquête.

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 encore provisoire et consciente de ses limites que la recherche a conduit à faire émerger et dont elle a commencé à vérifier la pertinence. 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. En effet, les données numériques apparaissent comme la cible ou le matériau commun des mesures d'enquête étudiées. Mais se pose alors la question de savoir comment sont « constituées » ces données pénales. 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. A cet égard, 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.

[5] Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, La documentation française, p. 9.

Plus encore, la construction juridique de la donnée pénale semble aujourd'hui indissociable d'une rencontre nouvelle, difficile et délicate de la procédure 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 sous leurs diverses déclinaisons, dont le droit de ne pas s'auto-incriminer) ou nouveaux (le droit à la protection des données personnelles). Or l'hypothèse principale est que ce dernier corpus, devenu foisonnant, 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. 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. Parmi les sources organisant le droit à la protection des données personnelles et à la vie privée, le droit de l'Union européenne occupe, en effet, la première place, 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 qui invite à distinguer les données pénales par nature des données pénales par destination, toutes soumises au droit des données personnelles. Ainsi, l'objectif de recherche des auteurs d'infractions – au cœur de la procédure pénale – se trouve en quelque sorte relégué au rang de dérogation à la protection due aux droits fondamentaux. Il en résulterait une centralité nouvelle de la problématique de la conservation des données aux fins de mise en œuvre des règles relatives à l'enquête pénale ainsi qu'une compréhension renouvelée des conditions de leur collecte, qu'elle s'opère directement ou indirectement par l'intermédiaire de tiers.

5/ Pistes de réflexions ouvertes, reformulations opérées

Pensé et rédigé au moment où la réflexion au sujet des NTIS s'emballe, ce travail se présente avant tout comme une œuvre de dépliement et de clarification.
Les entretiens avec les acteurs ont ainsi permis de dégager, à partir des besoins exprimés par eux, plusieurs recommandations touchant essentiellement à la confection et à la réception des normes pénales relatives aux NTIS : associer les professionnels spécialisés à l'élaboration des textes, confectionner des guides à usage des professionnels et qui partent d'exemples du terrain, désigner dans chaque tribunal un référent « cyber » qui permette de faire le lien entre les acteurs et d'expliquer les techniques utilisées ou envisagées ; mieux motiver les actes demandant une NTIS ou la refusant ; disposer d'instruments de mesure statistique.
L'analyse normative montre, quant à elle, la nécessité de systématiser la présentation des preuves par NTIS (et plus généralement de la preuve scientifique) dans le Code de procédure pénale, en soulignant non seulement son absence, y compris là où a pourtant été réalisé un effort du législateur en ce sens, mais aussi les effets induits, contreproductifs pour l'efficacité des enquêtes et de la procédure pénale et délétères pour la protection des droits et garanties individuels d'une telle lacune.
Ensemble, approche empirique et analyse normative ont appelé et nourri le travail de mise en perspective visant à répondre aux interrogations soulevées par les acteurs eux-mêmes ou l'observation de leurs pratiques et aux insuffisances du cadre juridique applicable.
Il débouche sur la reformulation principale que nous avons opérée. Elle concerne la donnée numérique pénale dont nous avons caractérisé l'émergence et qui nous semble pouvoir contribuer à repenser les phases de l'obtention de la preuve. En effet, la donnée est susceptible tout à la fois d'orienter ou alimenter l'enquête (donc de déterminer l'action des enquêteurs) et

de constituer le résultat de cette action (la preuve). Dès lors son rôle et sa place varient, en particulier en fonction de la disponibilité d'autres éléments pouvant remplir les mêmes fonctions ou fins. On pourrait alors dégager trois phases – et non plus seulement deux, le recueil et l'emploi– dans la construction de la preuve pénale : la phase de conservation qui commande la disponibilité des données potentiellement susceptibles de constituer des éléments de preuve, la phase d'accès qui détermine leur mise à disposition, leur recueil, et la phase d'exploitation qui conditionne leur utilisation ès-qualité (en tant que preuve).

Chacune de ces trois phases est configurée d'abord à l'aune des principes du droit des données personnelles qui concrétise directement ou indirectement les garanties de la Charte des droits fondamentaux de l'Union européenne, puis au regard et dans la mesure de la conciliation entre ces principes et l'objectif de lutte contre la criminalité. Autant dire qu'une telle (re)-configuration suppose une typologie des données qui toutes n'engagent pas les (mêmes) droits fondamentaux avec la même intensité. Ainsi, entre les données qui concernent l'identité civile, la vie sociale ou l'intimité, certaines sont sensibles, d'autres non, certaines permettent de tirer des conclusions très précises sur la vie privée, d'autres moins et encore faut-il distinguer selon que la donnée a déjà été stockée ou fera l'objet d'un recueil en temps réel ou encore selon qu'elle renseigne à la fois sur l'identité ou la localisation (comme l'adresse IP).

Si l'on fait abstraction des hypothèses d'accès direct, c'est donc la conservation qui commande la disponibilité de la donnée. Cette étape est par conséquent fondamentale tant elle conditionne l'existence et le volume du « réservoir » de preuves que constituent les données stockées et en circulation. Or, le régime de la conservation varie selon qu'elle est imposée (à des opérateurs de communication ou des banques par exemple) ou facultative (lorsque les particuliers y « consentent » ou selon les politiques commerciales des opérateurs). De l'ensemble textuel et jurisprudentiel européen résulte notamment un encadrement apparemment serré de la conservation obligatoire qui fixe comme borne la conservation dite « généralisée et indifférenciée » des données de trafic ou de localisation. Celle-ci est strictement limitée à la seule sauvegarde de la sécurité nationale. Toutefois, outre la conservation ciblée, la conservation dite rapide, empruntée à la Convention de Budapest, peut permettre d'enjoindre aux opérateurs de télécommunications de conserver également ces données aux fins de lutte contre la criminalité grave. On peut alors formuler l'hypothèse que la conservation rapide peut tenir lieu de chaînon manquant entre la conservation préventive (*i.e.* généralisée et indifférenciée aux fins de sauvegarde de la sécurité nationale) et la conservation répressive (*i.e.* rapide aux fins de lutte contre la criminalité grave).

Le réservoir des données abondé, son contenu n'est accessible qu'à certaines conditions spécifiques mais supposées conçues en cohérence avec celles qui déterminent la conservation ; conservation et accès constituant des ingérences distinctes dans les droits fondamentaux. Aussi bien, l'accès ne saurait être autorisé pour des motifs d'une importance moindre de ceux qui ont valablement permis la conservation. Le régime de l'accès ne saurait compenser ou corriger les insuffisances des conditions de conservation des données.

En tant que dérogation au principe de confidentialité ou limitation au droit à la protection des données personnelles, accès indirect et accès direct doivent obéir aux conditions de légitimité des objectifs, de proportionnalité, de stricte nécessité, de garantie judiciaire et du droit à l'information, qui varient selon la gravité (abstraite et concrète) de la criminalité en cause et les nécessités de l'enquête.

S'agissant, enfin, de l'exploitabilité des données en vue de leur utilisation probatoire, si elle relève encore principalement de la compétence des droits nationaux, elle doit satisfaire les exigences européennes d'équivalence et d'effectivité, qui, bien que de manière encore très lâche, encadrent la question de la sanction d'un accès irrégulier aux éléments de preuve.

C'est dire si au fil de typologies nouvelles – des données, des modes de conservation ou d'accès, des limites à l'exploitabilité – se construit un cadre juridique où la contrainte européenne est

forte (certaines voies sont exclues, d'autres sont étroitement réservées) mais où les marges nationales n'ont pas disparu (là où le curseur -tel que celui qui fixe ce qui relève ou non de la criminalité grave, ce qui est ou n'est pas exploitable- demeure du ressort des ordres internes).
Surtout, dans cette « négociation » entre contraintes et marges suscitée par la construction de la donnée numérique pénale, se dévoilent aussi les limites, faiblesses ou fragilités des procédures pénales nationales qui pourraient trouver dans la nouvelle configuration en cours d'élaboration les instruments ou leviers de leur dépassement.
Au-delà de cette proposition de reformulation centrée sur la donnée pénale numérique (conservation, accès, exploitation), le travail ouvre des pistes d'approfondissement : sans doute faudrait-il élargir le champ des enquêtés et mener des enquêtes de grande ampleur afin 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*) ; assurément la question des rapports entre monde réel et monde virtuel gagnerait-elle à être approfondie pour déterminer l'effet de substitution (obsolescence) des NTIS aux mesures d'enquête plus traditionnelles, ou encore la ventilation et l'articulation de leurs usages respectifs ; il serait fécond de mener une analyse comparée du recours aux NTIS et à d'autres techniques permettant d'obtenir des preuves afin de mettre en exergue ou au contraire de nuancer la spécificité des NTIS ; enfin la recherche ouvre la voie à un véritable travail de droit comparé.

Nous espérons que par les instruments et analyses proposés – cartographie, glossaire, observations empiriques, généalogie et comparaisons normatives, perspectives et mise en contexte – cette recherche permettra à chacun et chacune de contribuer à dégager les conditions ou coordonnées systémiques d'une mise en cohérence d'ensemble, par un travail concerté dont la réforme annoncée du Code de procédure pénale pourrait être l'occasion.

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