Vers un droit commun de la preuve numérique ?

Alice Mornet

Vers un droit commun de la preuve numérique ?

Alice MORNET
Maître de conférences
Université d'Avignon

Mots-clés : « preuve » ; « preuve numérique » ; « numérique » ; « techniques d'enquête numériques » ; « procédure pénale » ; « enquête » ; « données » ; « données de connexion ».

Résumé : À la faveur de la loi du 24 janvier 2022, le législateur a autorisé le recours aux drones à des fins de police judiciaire, allongeant encore davantage la liste des techniques d'enquête numériques et offrant l'occasion de s'intéresser à leur régime. À l'étude, les garanties entourant ces mesures se révèlent profondément hétérogènes alors qu'elles fragilisent, toutes, les droits à la vie privée et à la protection des données. Un tel constat invite à s'interroger sur l'opportunité d'un droit commun des techniques d'enquête numériques se structurant à partir de leur objet : la donnée numérique.

À retenir : L'hétérogénéité de l'encadrement des techniques d'enquête numériques semble trouver sa source dans l'absence de définition concédée à leur objet : la preuve numérique. Partant, le recours à la notion de données numériques, plus claire, pourrait permettre de corriger cet état de fait. Véritable critère, la nature de la donnée en cause vient, en s'ajoutant au critère temporel, justifier une variation des garanties entourant les techniques d'enquête et dessiner, progressivement, un droit commun de la preuve numérique.

La preuve numérique apparaît être l'héroïne d'une saga dont les rebondissements feraient pâlir les plus grands scénaristes. Se trouvant au cœur de l'actualité législative[1] et jurisprudentielle[2], française comme européenne[3], elle attire toute l'attention. Significative, cette « *success story* » témoigne, en réalité, des difficultés qu'il y a à encadrer son recueil et son exploitation.

Volatile, évanescente, fuyante... Autant de qualificatifs ayant été attribués à la preuve numérique pour souligner les résistances de son appréhension pénale. En se dissimulant dans les sinuosités innombrables des réseaux informatiques, elle échappe à la maîtrise — tant physique qu'intellectuelle — des praticiens et de la doctrine. Cependant, en dépit de son ambiguïté, certaines certitudes existent, notamment quant aux mécanismes permettant de « capturer » cette insaisissable preuve.

La preuve numérique, en effet, peut être recueillie à l'occasion d'une enquête ou d'une instruction[4] et, plus précisément, à la faveur de la mise en œuvre des techniques d'enquête numériques. Celles-ci recouvrent l'« ensemble des mesures d'investigation susceptibles d'être employées par les autorités de police et justice via les réseaux de transmission électronique – satellitaires et terrestres, fixes et mobiles, dès lors qu'ils passent par des canaux numériques –, ou sur des appareils connectés à ces réseaux, afin de mettre à jour des infractions pénales et d'identifier leurs auteurs[5] ». Si l'objet résiste aux définitions, il n'en va donc pas ainsi de son

[1] En témoigne la réforme des réquisitions relatives aux données de connexion à la faveur de la loi n°2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire, JORF n°52 du 3 mars 2022.

[2] V. not. s'agissant des réquisitions de données de connexion : Cons. const., 3 déc. 2021, *M. Omar Y*, n°2021-952 DC – Gaz. Pal., 2022, 12, 5, obs. T. Douville ; LPA, 2022, 3, 53, comm. B. Guillaumin ; Gaz. Pal., 2022, 6, 55, obs. F. Fourment, Gaz. Pal., 2022, 2, 19, comm. B. Daligaux ; Lexbase Pénal, 2021, 44, obs. M. Audibert – Cons. const., 25 févr. 2022, *M. Youcef Z.*, n°2021-976/977 QPC – D. actu., 2022, obs. C. Evrard ; AJ Pénal, 2022, 220, obs. A. Archambault ; Dalloz IP/IT, 2022, 118, obs. C. Crichton ; Rev. sc. crim., 2022, 415, obs. A. Botton ; Lexbase, obs. A. Léon – Cons. const., 20 mai 2022, *M. Lofti H.*, n°2022-993 QPC – Gaz. Pal., 2022, 24, 16, obs. P. Collet ; Gaz. Pal., 2022, 40, 10, obs. C. Richaud ; Cass. crim., 12 juill. 2022, n°21-83.710, bull. Crim. n°769, n°21-83.820, bull. crim. n°771, n° 21-84.096, bull. crim. n°772, n°21-83.729, Inédit – JCP-G, 2022, 40, 1123, note O. Cahn ; Gaz. Pal., 2022, 31, obs. M. Bouchet ; Dalloz IP/IT, 2022, 408, obs. J. Eynard ; D. actu., 2022, obs. B. Nicaud ; AJ Pénal, 2022, 415, note M. Bendavid et C. Quendolo ; Lexbase Pénal, 2022, 52, obs. A. Léon – Cass. crim., 11 oct. 2022, n°22-81.244, Inédit – Gaz. Pal., 2022, 38, 16, obs. R. Mésa. S'agissant de l'accès aux données chiffrées : Cons. const., 8 avril 2022, *M. Saïd Z.*, n°2022-987 QPC – RTD Civ., 2022, 628, comm. H. Barbier ; D. actu., 2022, obs. M. Slimani ; Lexbase Pénal, 2022, 48, obs. L. Saenko ; Lexbase Pénal, 2022, 48, obs. A. Léon.

[3] S'agissant de l'Union européenne : Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM(2018) 225 final, Strasbourg, 17 avril 2018. S'agissant du Conseil de l'Europe : Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, Strasbourg, 12 mai 2022.

[4] Nos propos se limiteront à l'étude de ces mesures dans le cadre de l'enquête, à l'exclusion de l'instruction.

[5] M. TOUILLIER, « Lumière sur un arsenal de lutte contre une délinquance tapie dans l'ombre », AJ Pénal, 2017, p. 312.

mode de recueil, lequel a, de surcroît, été consacré par la création, en 2017, de l'Agence Nationale des Techniques d'Enquête Numériques judiciaires (ANTEN)[6]. Mettant en œuvre la plate-forme nationale des interceptions judiciaires, l'agence est également compétente s'agissant des techniques d'enquête prévues aux articles 230-1 et suivants et 706-95-1 et suivants du Code de procédure pénale[7]. Au regard de ce champ de compétences, il faudrait conclure que la preuve numérique ne peut être recueillie qu'au moyen des techniques d'enquête prévues auxdits articles. Toutefois, ce serait oublier les réquisitions et les perquisitions qui, en raison de leur généralité, permettent également de l'obtenir. Volatile, la preuve numérique l'est donc aussi au sein du Code de procédure pénale tant les dispositions y afférentes y sont dispersées. Elle apparaît, en effet, aux articles relatifs à l'enquête et à l'instruction, à ceux communs aux deux cadres et, enfin, à ceux consacrés à la lutte contre la criminalité organisée. Une telle division, sans logique apparente, semble résulter des multiples interventions du législateur visant à combattre la cybercriminalité.

Dans un monde exponentiellement numérisé, il est en effet impérieux de lutter contre les infractions commises sur ou au moyen des réseaux[8], qu'il s'agisse d'incriminer de nouveaux comportements[9] ou d'adapter les techniques permettant de les déceler. Aussi, depuis la loi du 10 juillet 1991 relative aux écoutes téléphoniques[10] jusqu'à celle du 24 janvier 2022 autorisant l'usage des drones à des fins de police judiciaire[11], le législateur n'a cessé de créer ou d'étendre les mesures d'enquête numériques[12].

---

[6] Décret n°2017-614 du 24 avril 2017 portant création d'un service à compétence nationale dénommé « Agence nationale des techniques d'enquêtes numériques judiciaires » et d'un comité d'orientation des techniques d'enquêtes numériques judiciaires, JORF n°97 du 25 avril 2017.

[7] Art. 2, *Ibid*.

[8] Conformément à la définition de la cybercriminalité proposée par le Sénat selon laquelle celle-ci peut se concevoir comme « toute action illégale dont l'objet est de perpétrer des infractions sur ou au moyen d'un système informatique interconnecté à un réseau de télécommunications » : Sénat, Rapport d'information sur la lutte contre la cybercriminalité, n°613, 9 juill. 2020, p. 6.

[9] V. not. B. PEREIRA, « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », RIDE, n°3, 2016, pp. 387-409 ; M. QUÉMÉNER, « Pour une lutte plus efficace contre la cybercriminalité », Sécurité globale, n°15, 2018, pp. 5-16.

[10] Loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, JORF n°162 du 13 juill. 1991.

[11] Loi n°2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, JORF n°20 du 25 janv. 2022.

[12] Il en va ainsi, par exemple, de la loi n°2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité qui a permis les sonorisations et les fixations d'images ou encore 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 ayant étendu ces mesures à l'enquête, ayant créé l'accès aux correspondances stockées et permis le recours aux IMSI-Catcher.

S'il est plus que nécessaire d'appréhender la preuve numérique[13] — le Web ne devant pas être un sanctuaire pour les délinquants — la technique impressionniste du législateur interroge quant à l'existence d'une cohérence d'ensemble. En effet, au-delà de leur dispersion au sein du Code de procédure pénale, les mesures d'enquête numériques connaissent un encadrement variable et les différences existantes ne sont pas toujours évidentes. Regrettable, ce désordre l'est surtout en ce que ces méthodes d'investigation sont susceptibles de fragiliser les droits à la vie privée et à la protection des données à caractère personnel[14], évidemment, mais également le droit à un procès équitable. Ainsi, toute variation de garanties devrait être justifiée par la nature de l'ingérence portée à ces derniers. À cet égard, la proposition de règlement relatif aux injonctions de production et de conservation de preuves électroniques en matière pénale[15] laisse à penser, au regard de son titre, qu'il existerait, ou devrait exister, un droit commun de la preuve numérique. Or, à l'évidence, un tel droit est, pour l'heure, introuvable. Une telle absence pourrait trouver sa cause dans le manque d'égards concédé à l'objet, autrement dit à la preuve numérique. Faute d'acception précise de ce qu'elle recouvre, élaborer un régime cohérent semble, en effet, impossible[16].

Partant, la précision de la notion de preuve numérique (**I**) constitue la première pierre à l'édification d'un droit commun des techniques d'enquête numériques (**II**).

I. La révélation de la nature plurielle de la preuve numérique

Si la preuve numérique est évanescente au sein des réseaux, sa définition l'est tout autant et son acception ne fait l'objet d'aucun consensus, qu'il soit légal ou doctrinal (**A**). Pour autant, cette carence sémantique semble pouvoir être corrigée en recourant à une notion qui lui est proche, peut-être même identique : la donnée numérique (**B**).

[13] M. QUÉMÉNER, F. DALLE, « L'accès à la preuve numérique, enjeu majeur de toute enquête pénale : pratique et perspectives », Dalloz IP/IT, 2018, p. 418.
[14] Sur la différence entre ces deux droits fondamentaux : A. MORNET, *Les fichiers pénaux de l'Union européenne. Contribution à l'étude de la protection des données à caractère personnel*, thèse dactylographiée, Université Toulouse I, 2020, n°17.
[15] Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, *op. cit*.
[16] J.-L. BERGEL, « Différence de nature (égale) différence de régime », RTD Civ., 1984, pp. 255-272.

A : L'absence de définition de la preuve numérique

La preuve numérique, ou preuve électronique[17], résiste à toute tentative de définition, qu'elle soit d'origine légale, jurisprudentielle ou doctrinale[18].

En droit interne, elle est seulement envisagée en droit civil, dans le cadre de la signature électronique[19]. Arlésienne pénale, elle demeure absente des dispositions du code pénal ou de procédure pénale, mais apparaît ici et là dans certains travaux du législateur, qu'il s'agisse de souligner son utilité en matière de répression[20] ou de préciser les modalités de sa collecte[21]. Le droit européen *lato sensu* utilise en revanche plus volontiers l'appellation de « preuve électronique »[22], laquelle figure dans les intitulés du protocole additionnel à la Convention de Budapest relatif « au renforcement de la coopération et de la divulgation des preuves électroniques[23] » et de la proposition de règlement de l'Union européenne relatif « aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale[24] ». Tandis que le premier texte se garde bien de définir ce que cette preuve recouvre, le second s'essaye à l'exercice en indiquant qu'il s'agit de la « preuve stockée sous forme électronique par un fournisseur de services ou en son nom au moment de la réception d'un certificat d'injonction de production ou de conservation, consistant en données stockées relatives aux abonnés, à l'accès, aux transactions et au contenu[25] ». Bienvenue, cette définition demeure cependant purement contextuelle, en étant seulement envisagée en référence aux

[17] En effet, les deux termes sont employés indifféremment par la doctrine.
[18] V. également en ce sens, E. VERGÈS, « La preuve numérique, entre continuité et changement de paradigme », *in Le traitement de la preuve numérique par les magistrats dans les procédures judiciaires civiles et pénales*, RJA, n°21, 2019, p. 16.
[19] Instruction de la Direction générale des systèmes d'information et de communication n°2003/DEF/DGSIC portant code de bon usage des systèmes d'information et de communication du ministère de la défense, 20 nov. 2008, p. 16.
[20] Le Sénat emploie effectivement l'expression « preuve numérique » en insistant sur son importance dans le cadre de la lutte contre la cybercriminalité : Sénat, Résolution européenne sur la lutte contre la cybercriminalité, JORF n°207 du 25 août 2020.
[21] En effet, la circulaire de présentation des dispositions de la loi n°2016-731 du 3 juin 2016 contient une fiche technique consacrée au « recueil de la preuve numérique » : Circulaire du Ministre de la justice 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, pp. 12 et s.
[22] En droit de l'Union européenne, le terme a été employé pour la première fois en matière de délinquance financière : Communication de la Commission au Conseil et au Parlement européen, Prévenir et combattre les malversations financières et pratiques irrégulières des sociétés, COM(2004) 611 final, Bruxelles, p. 13.
[23] Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, *op. cit*.
[24] Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, *op. cit*.
[25] Art. 2, 6), *Ibid*.

fournisseurs de services de communication en ligne. La définition jurisprudentielle de la preuve numérique — ou preuve électronique — n'est pas plus élaborée, loin de là. En effet, la Cour de justice de l'Union européenne n'utilise jamais ces expressions, lesquelles se font également très rares au sein des arrêts de son homologue strasbourgeoise[26]. S'agissant des juridictions françaises, seul le Conseil d'État évoque, parfois, la « preuve électronique » en matière pénale[27] lorsqu'il aborde les dispositions de la Convention de Budapest[28].

La doctrine pourrait combler cette imprécision notionnelle, mais, alors que de nombreux auteurs mentionnent la « preuve numérique »[29], peu d'entre eux se prêtent à l'exercice de définition. Soulignant l'hétérogénéité de la catégorie, certains estiment qu'il s'agit de la preuve recueillie au moyen des techniques d'enquête numériques[30], quand d'autres insistent davantage sur sa physionomie en énonçant qu'il s'agit « de toute information contenue dans un objet que l'homme n'est pas en mesure d'examiner par l'usage direct de ses sens[31] ». Faute de consensus doctrinal, il est difficile de cerner l'essence de cette preuve aux contours si particuliers, sauf à revenir aux fondamentaux c'est-à-dire aux définitions de ses composantes : la preuve, d'une part ; le numérique, d'autre part.

La preuve recouvre « Tout moyen permettant d'affirmer l'existence ou la non-existence d'un fait[32] » ou le « fait, témoignage, raisonnement susceptible d'établir de manière irréfutable

[26] La Cour européenne des droits de l'homme utilise l'expression « preuve électronique » dans un seul arrêt, pour désigner le contenu d'une messagerie électronique utilisée par une organisation criminelle : CEDH, 2ème sec., 22 nov. 2021, *Akgün c/ Turquie*, req. n°19699/18, §67.

[27] Les juridictions civiles l'emploient, quant à elles, pour désigner l'écrit électronique de l'article 1366 du Code civil : CA, Versailles, 30 oct. 2014, n°13/00220. Quant à la Commission Nationale Informatique et Libertés (CNIL), elle utilise l'expression « preuve numérique » pour désigner les QR Codes Covid (CNIL, Délibération n°2021-067 du 7 juin 2021 portant avis sur le projet de décret portant application du II de l'article 1er de la loi n° 2021-689 du 31 mai 2021 relative à la gestion de la sortie de crise sanitaire) et le terme « preuve électronique » en matière civile (CNIL, Délibération relative au projet de décret modifiant le Titre II du décret n° 98-247 du 2 avril 1998 relatif à la qualification artisanale et au répertoire des métiers).

[28] CE, Ass., 21 avril 2021, n°393099.

[29] M. QUÉMÉNER, « Les spécificités juridiques de la preuve numérique », AJ Pénal, 2014, p. 63 ; C. MICHALSKI, « La recherche et la saisie des preuves électroniques », Gaz. Pal., 2014, n°42 ; C. CASTETS-RENARD, « Quelles nouveautés en matière de preuve numérique ? », Justice et Cassation, 2017, p. 23 ; M. QUÉMÉNER, F. DALLE, « L'accès à la preuve numérique, enjeu majeur de toute enquête pénale : pratique et perspectives », *op. cit*., p. 418.

[30] Ainsi, selon Mélanie Clément-Fontaine : « La preuve numérique est une modalité particulière d'établissement de la vérité qui consiste à avoir recours à des moyens numériques variés qui vont de l'étude des contenus dans la mémoire d'un disque dur, aux messages électroniques, en passant par l'enregistrement numérique » : « Définition et cadre juridique de la preuve numérique », *in La preuve numérique à l'épreuve du litige*, Actes de colloque du CNEJITA, 13 avril 2010, p. 11. V. également, E. VERGÈS, « La preuve numérique, entre continuité et changement de paradigme », *op. cit*., pp. 16-17.

[31] D. BENICHOU, « Le juge pénal, ses attentes, une preuve sûre et intelligible », *in La preuve numérique à l'épreuve du litige*, Actes de colloque du CNEJITA, 13 avril 2010, p. 58.

[32] R. MERLE, A. VITU, *Traité de droit criminel*, Cujas, 1979, p. 151.

la vérité ou la réalité[33] ». Elle renvoie donc, alternativement, à l'objet probant ou au moyen mis en œuvre pour le recueillir. Quant à l'adjectif « numérique », il correspond à ce « qui concerne des nombres, qui se présente sous la forme de nombres ou de chiffres, ou qui concerne des opérations sur des nombres[34] » ou encore à « la représentation de l'information ou de grandeurs physiques (images, sons) par un nombre fini de valeurs discrètes, le plus souvent représentées de manière binaire par une suite de 0 et de 1[35] ». À la lecture de ces définitions, il est donc possible d'avoir deux approches de la « preuve numérique » : l'une consistant à soutenir qu'il s'agit de la preuve qui se présente sous la forme de nombres ou de chiffres ; l'autre tendant davantage à qualifier la technique probatoire ayant permis de rendre lisible, pour tout un chacun, cette suite de chiffres.

En réalité, quelle que soit la définition privilégiée, la preuve numérique apparaît toujours, initialement, comme une suite de chiffres ou de nombres ce qui la rapproche d'une notion dont l'acception semble bien plus claire : la donnée.

B : La synonymie de la donnée et de la preuve numérique

La donnée peut se définir comme « la représentation de l'information ou de grandeurs physiques (par ex. images, sons) par un nombre fini de valeurs discrètes, le plus souvent représentées de manière binaire par une suite de 0 et de 1[36] »[37] et constitue alors une « information "valorisée" dont le traitement est facilité du fait de sa forme[38] ». À l'instar de la preuve, la donnée est donc, initialement, une simple information qui, comme la première, tire sa spécificité de sa forme[39]. L'étude des textes relatifs aux techniques d'enquête numériques ne fait que confirmer l'intuition selon laquelle toute preuve numérique est, fondamentalement, une donnée. En effet, si elles sont destinées à recueillir la preuve numérique, ces techniques portent

[33] V. « Preuve » : *TLFi : Trésor de la langue Française informatisé*, http://www.atilf.fr/tlfi, ATILF – CNRS & Université de Lorraine.
[34] V. « Numérique » : *TLFi : Trésor de la langue Française informatisé*, http://www.atilf.fr/tlfi, ATILF – CNRS & Université de Lorraine.
[35] Conseil d'État, *Le numérique et les droits fondamentaux*, La documentation française, 2014, p. 9.
[36] *Ibid*., p. 17.
[37] La Convention de Budapest utilise, quant à elle, l'expression « donnée informatique » qu'elle définit comme « 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 » : Art. 1, b), Convention sur la cybercriminalité, *op. cit*.
[38] A. DEBET, J. MASSOT, N. METALLINOS, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, L.G.D.J., coll. « Les intégrales », 2015, n°483. En italique dans le texte.
[39] L'article 60-1 du Code de procédure pénale confirme cette analyse en évoquant les « informations intéressant l'enquête » disponibles « sous forme numérique ».

toujours, en réalité, sur des données. Ainsi, pour qualifier leurs objets, le législateur utilise les termes de « données intéressant l'enquête[40] », « données saisies ou obtenues au cours de l'enquête[41] », « données de localisation[42] », « données de connexion[43] », « données informatiques[44] », « données techniques de connexion[45] » ou, plus directement, de « données[46] »[47]. Les décisions de justice adoptées sur la base de ces dispositions légales confirment l'assimilation de la preuve numérique et de la donnée, quelle que soit la mesure d'enquête étudiée[48].

Initialement, la preuve numérique est donc toujours une donnée. Or, contrairement à la première, la seconde voit son régime progressivement dessiné, notamment lorsque se posent des questions relatives à sa conservation ou à sa communication à des fins pénales. En effet, dans ces derniers cas, les garanties juridiques fluctuent selon la sensibilité de l'information en cause. Partant, le recours à la notion de données — qui n'est pas unitaire — pourrait, éventuellement, expliquer les variations de garanties entourant l'ensemble des techniques d'enquête numériques.

---

[40] S'agissant des perquisitions et saisies informatiques : Art. 57-1 et 76-3, Code de procédure pénale.
[41] S'agissant de l'accès aux données chiffrées : Art. 230-1 et s., Code de procédure pénale.
[42] S'agissant de la géolocalisation : Art. 230-8, Code de procédure pénale.
[43] S'agissant des réquisitions : Art. 60-1-1 et 77-1-1, Code de procédure pénale. L'article 60-1-2 évoque, quant à lui, les « données techniques » et, s'agissant des réquisitions « générales », le législateur précise qu'il peut s'agir d'informations « sous forme numérique ». Enfin, les articles 60-2 et 77-1-2 vise les « informations utiles à la manifestation de la vérité (...) contenues dans le ou les systèmes informatiques ou traitements de données nominatives ».
[44] S'agissant de la captation de données informatiques : Art. 706-102-1, Code de procédure pénale.
[45] S'agissant des IMSI-Catcher : Art. 706-95-20, Code de procédure pénale.
[46] S'agissant des interceptions et transcriptions de correspondances stockées : Art. 706-95-1 et -2, Code de procédure pénale. Il en va de même pour les cyberpatrouilles et les drones : Art. 230-46 et 230-52, Code de procédure pénale.
[47] En réalité, seul l'article 706-96 du Code de procédure pénale relatif à la sonorisation et à la fixation d'images n'emploie pas ce terme. Pour autant, les informations révélées par le corps et fixées par le biais de dispositifs numériques sont des données et, plus précisément, des données à caractère personnel : CNIL, *Voix, image et protection des données personnelles*, La Documentation française, 1996, 119 p.
[48] Tous les arrêts ou décisions relatifs aux techniques d'enquête numériques utilisent, en effet, l'expression de « données ». V. par exemple, pour les réquisitions : Cons. const., 3 déc. 2021, *M. Omar Y.*, n°2021-952 QPC ; Cons. const., 17 juin 2022, *M. Ibrahim K*, n°2022-1000 QPC – D., 2022, 1540, obs. M. Lassalle ; D., 2022, 1487, obs. J.-B. Perrier – Cass. crim., 11 oct. 2022, n°22-81.244, Inédit. Pour les obligations de conservation de données : Cons. const., 25 févr. 2022, *M. Habib A. et autres*, n°2021-976/977 QPC. Pour la géolocalisation : Cons. const., 25 mars 2014, n°2014-693 DC ; Cons. const., 21 mars 2019, n°2019-778 DC – D. actu., 2014, obs. C. Fleuriot ; Gaz. Pal., 2014, 95, 14, obs. E. Dupic. Pour l'accès aux données chiffrées : Cons. const., 8 avril 2022, *M. Saïd Z.*, n°2022-987 QPC. Pour les cyberpatrouilles : Cons. const., 21 mars 2019, n°2019-778 DC. Pour l'interception de paroles : Cons. const., 4 déc. 2013, n°2013-679 DC ; Cons. const., 9 oct. 2014, *M. Maurice L. et autres*, n°2014-420/421 QPC – AJ Pénal, 2014, 574, obs. J.-B. Perrier ; D. actu., 2014, obs. M. Léna ; Dr. Pénal, 2014, 142, obs. A. Maron et M. Haas ; RFDC 2015. 206, obs. S. Anane. Pour la captation de données informatiques : Cons. const., 8 avril 2022, *M. Saïd Z.*, n°2022-987 QPC ; Cass. crim., 1 févr. 2022, n°21-85.148, Inédit – Dalloz IP/IT, 2022, 578, obs. X. Laurent ; Pour les IMSI-Catcher et pour l'accès aux correspondances stockées : Cons. const., 21 mars 2019, n°2019-778 DC.

Plusieurs catégories de données ont, en effet, été identifiées, bien que celles-ci diffèrent selon la juridiction ou le texte étudié. Tout d'abord, la Convention de Budapest distingue les données de contenu, les données de trafic et, enfin, les données relatives aux abonnés[49]. Quant au droit de l'Union européenne, ensuite, la proposition de révision de la directive commerce électronique[50] différencie les données de contenu des métadonnées de communications[51]. La proposition de règlement *e-evidence*, plus précise, identifie quatre catégories de données : celles

[49] Les données de trafic sont « toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent » : Art. 1, d), Convention sur la cybercriminalité, *op. cit*. Quant aux données relatives aux abonnés, il s'agit de « toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir: a) le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service; b) l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services; c) toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services » : Art. 18§3, Convention sur la cybercriminalité, *op. cit*.

[50] La directive commerce électronique distingue, quant à elle, les données de trafic et les données de localisation. Une telle division est en voie d'être abandonnée car elle n'a pas de conséquences pratiques, ces deux catégories de données présentant le même degré de sensibilité : Art. 2, b) et c), 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), JO L 201 du 31 juillet 2002, p. 37.

[51] Les premières correspondent au « contenu échangé au moyen de services de communications électroniques, notamment sous forme de texte, de voix, de documents vidéo, d'images et de son » tandis que les secondes recouvrent « les données traitées dans un réseau de communications électroniques aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication » : Art. 4§3, l) et m), Proposition de règlement du parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement «vie privée et communications électroniques»), COM(2017) 10 final, Bruxelles, 10 juill. 2017.

relatives aux abonnés[52], celles relatives à l'accès[53], celles relatives aux transactions[54] et, enfin, celles relatives aux contenus[55]. Alors que les deux premières catégories sont jugées peu intrusives, les deux dernières font l'objet d'une protection accrue, s'agissant notamment de l'organe compétent pour émettre une injonction européenne de production les concernant[56]. Une telle catégorisation se retrouve, peu ou prou, au sein de la jurisprudence de la Cour de justice de l'Union européenne. En effet, celle-ci n'apprécie pas la proportionnalité de l'ingérence de la même manière selon la nature des données concernées. Ainsi, dans l'arrêt *Ministerio Fiscal,* elle affirma que les données relatives aux abonnés[57] ne permettaient pas d'obtenir des informations intrusives et, qu'ainsi, l'ingérence n'avait pas à se limiter aux infractions graves[58]. En outre, elle opère une distinction entre les données de trafic et de localisation et les données de contenu et, si elle considère que l'ingérence est plus importante

[52] Il s'agit de « toutes les données relatives à a) 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 le courriel fournis ; b) le type de service et sa durée, y compris les données techniques et les données identifiant les mesures techniques liées ou les interfaces utilisées ou fournies par l'abonné ou le client, 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 fournis par un utilisateur ou créés à la demande d'un utilisateur » : Art. 2, 7), Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, *op. cit*.

[53] Il s'agit des « les données relatives au début et à la fin d'une session d'accès utilisateur à un service, strictement nécessaires aux seules fins d'identification de l'utilisateur du service, telles que la date et l'heure d'utilisation, ou la connexion et la déconnexion du service, ainsi que l'adresse IP attribuée par le fournisseur de service d'accès à l'internet à l'utilisateur d'un service, les données identifiant l'interface utilisée et l'identifiant de l'utilisateur. Sont incluses les métadonnées de communications électroniques telles que définies à l'article 4, paragraphe 3, point g), du [règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques] » : Art. 2, 8), *Ibid*.

[54] Il s'agit des « 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, tel que la source et la destination d'un message ou d'un autre type d'interaction, les données sur l'emplacement du dispositif, la date, l'heure, la durée, la taille, le routage, le format, le protocole utilisé et le type de compression, sauf si ces données constituent des données relatives à l'accès. Sont incluses les métadonnées de communications électroniques telles que définies à l'article 4, paragraphe 3, point g), du [règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques] » : Art. 2, 9), *Ibid*.

[55] Il s'agit de « toutes les données stockées dans un format numérique tel que du texte, de la voix, des vidéos, des images et du son autres que les données relatives aux abonnés, les données relatives à l'accès ou les données relatives aux transactions » : Art. 2, 10), *Ibid*.

[56] En effet, pour ces deux catégories de données, l'injonction ne peut être émise que par un juge, une juridiction ou un juge d'instruction, à l'exclusion de toute autre autorité compétente en matière pénale : Art. 4§2, *Ibid*.

[57] Il s'agissait, en l'espèce, des numéros de téléphone et des noms, prénoms et adresses des titulaires de cartes SIM.

[58] CJUE, gde ch., 2 oct. 2018, *Ministerio Fiscal*, Aff. C-207/16, §§59-61 – D., 2018, obs. S. Fucini ; Comm. com. électr., 2018, 10, 79, obs. A. Fitzjean Ó Cobhthaigh. V. également en ce sens, CJUE, gde ch., 6 oct. 2020, *La Quadrature du Net e. a.*, Aff. Jtes. C-511/18, C-512/18 et C-520/18, §157 – Lexbase Pénal, 2020, 32, obs. W. Azoulay ; Lexbase, 2020, obs. A. Léon ; D., 2021, 406, obs. M. Lassalle ; Dalloz IP/IT, 2021, 46, obs. E. Daoud, I. Bello et O. Pecriaux ; Légipresse, 2020, 671, étude W. Maxwell ; Légipresse, 2021, 240, étude N. Mallet-Poujol ; RTD Eur., 2021, 175, obs. B. Bertrand ; RTD Eur., 2021, 973, obs. F. Benoît-Rohmer.

lorsque les secondes sont concernées[59], elle souligne tout de même la sensibilité des premières en ce qu'elles « sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles[60] »[61]. Enfin, parmi les données de trafic et de localisation, elle isole l'adresse IP qu'elle rapproche des données relatives à l'identité civile en ce qu'elle sert principalement à identifier la personne concernée[62]. À la lecture des arrêts de la juridiction de Luxembourg, il est donc possible de distinguer les données d'identité, comprenant l'adresse IP, les données de trafic et de localisation et, enfin, les données de contenu.

L'autorité de la Cour de justice a conduit le législateur français à modifier l'article L.34-1 du Code des postes et des communications relatif aux obligations de conservation de données s'imposant aux opérateurs de communications électroniques[63]. Sont désormais distinguées les informations relatives à l'identité civile, les informations relatives à la souscription d'un contrat et au paiement, les données techniques permettant d'identifier la source de la connexion ou relatives aux équipements terminaux utilisés, les autres données de trafic et, enfin, celles relatives aux communications électroniques. À y regarder de plus près, le législateur s'est fortement inspiré de la classification élaborée par la Cour de justice, les trois premières

[59] CJUE, gde ch., 21 déc. 2016, *Tele2 Sverige AB c/ Post-och telestyrelsen et Secretary of State for the Home Department c/ Tom Watson e. a.,* Aff. Jtes C-203/15 et C-698/15, §101 – Europe, 2017, 2, 48, comm. F. Gazin ; JCP G, 2017, 3, 59, obs. D. Berlin ; AJDA, 2017, 73, obs. F.-X. Brechot ; RUE, 2017, 178, obs. F.-X. Brechot; Dalloz IP/TP, 2017, 230, obs. D. Fores.

[60] CJUE, gde ch., 6 oct. 2020, *La Quadrature du Net e. a.*, Aff. Jtes. C-511/18, C-512/18 et C-520/18, §117 ; CJUE, gde ch., 6 oct. 2020, *Privacy International c/ Secretary of State for Foreign and Commonwealth Affairs e.a.,* Aff. C- 623/17,§71 ; CJUE, gde ch., 5 avr. 2022, *G.D. c/ Commissioner of An Garda Síochána e. a.,* Aff. C-140/20, §45 – D. actu., 2022, obs. C. Crichton ; D., 2022, 1487, obs. J.-B. Perrier.

[61] La Cour européenne des droits de l'homme adopte une lecture similaire en permettant aux États parties de ne pas soumettre aux mêmes garanties les traitements de données de contenu et ceux de métadonnées, tout en soulignant la sensibilité des secondes : CEDH, gde ch., 25 mai 2021, *Big Brother Watch et autres c/ Royaume-Uni*, req. n°58170/13, 62322/14 et 24960/15, §368 – D., 2021, 1082, obs. M.-C. de Montecler ; Légipresse, 2022, 253, obs. N. Mallet-Poujol ; Gaz. Pal., 2021, 25, 25, obs. J. Andriantsimbazovina – CEDH, gde ch., 25 mai 2021, *Centrum för Rättvisa c/ Suède*, req. n°35252/08, §256 et §§277-278 – Légipresse, 2022, 253, obs. N. Mallet-Poujol. V. pour un commentaire des deux arrêts, J.-P. MARGUÉNAUD, « La protection de la vie privée contre l'interception en masse des communications transfrontières », RTD Civ., 2021, p. 843.

[62] CJUE, gde ch., 5 avr. 2022, *G.D. c/ Commissioner of An Garda Síochána e. a.,* Aff. C-140/20, §73 ; CJUE, gde ch., 6 oct. 2020, *La Quadrature du Net e. a.*, Aff. Jtes. C-511/18, C-512/18 et C-520/18, §154.

[63] À la faveur de l'arrêt rendu par le Conseil d'État dans l'affaire *La Quadrature du Net :* CE, Ass., 21 avril 2021, n°393099, 397844, 397852, 424717 et 424718, *French Data Network* – Comm. com. électr., 2021, 56, comm. N. Belkacem ; D., 2021, 1268, note T. Douville, H. Gaudin ; JCP G, 2021, 659, obs. A. Iliopoulou-Peno.

catégories pouvant être regroupées sous l'appellation « données d'identité », jugées peu sensibles[64].

Finalement, la « preuve numérique » semble englober trois catégories de données qui, au regard de leur sensibilité, méritent d'être distinguées[65] : les données relatives à l'état civil, au contrat, à la facturation, ainsi que l'adresse IP (données d'identité) ; les données de trafic et de localisation[66] et, enfin, les données de contenu, recoupant celles qui concernent les échanges écrits ou oraux tenus entre plusieurs protagonistes, mais également l'image de ces derniers ou le simple son de leurs voix. La classification proposée ressemble à celle retenue par la Cour de justice, au terme d'une jurisprudence riche et dense, ou encore à celle arrêtée par le législateur au sein de l'article L.34-1 du Code des postes et des communications. Cependant, si elle semble, de prime abord, n'avoir d'intérêt que dans le cadre du contentieux relatif aux obligations de conservation et de communication des données de connexion, elle pourrait, en réalité, permettre l'édification d'un droit commun de la preuve numérique.

II. La construction d'un régime unifié de la preuve numérique

Les techniques d'enquête numériques se sont développées au fil des interventions impressionnistes du législateur. En apparence, elles semblent identiques, tant du point de vue de l'atteinte portée aux droits à la vie privée et à la protection des données à caractère personnel que de celui de leur objet, la preuve numérique. Pourtant, à y regarder de plus près, les garanties entourant la mise en œuvre de ces techniques diffèrent amplement selon la mesure d'investigation étudiée (**A**). Regrettable, cet encadrement anarchique semble pouvoir être

[64] De telles catégories se retrouvent désormais au sein des arrêts de la Chambre criminelle de la Cour de cassation : Cass. crim., 12 juill. 2022, n°21-83.820, bull. crim. n°771, n°21-84.096, bull. crim. n°772, n°21-83.729, Inédit. De même, le Conseil constitutionnel isole la catégorie des données de connexion, en raison de leur sensibilité : Cons. const., 3 déc. 2021, *M. Omar Y.*, n°2021-952 QPC, §11 ; Cons. const., 20 mai 2022, *M. Lofti H.*, n°2022-993 QPC, §10 ; Cons. const., 17 juin 2022, *M. Ibrahim K.*, n°2022-1000 QPC, §11 ; Cons. const., 25 févr. 2022, *M. Habib A. et autres*, n°2021-976/977 QPC, §11.

[65] V. pour une catégorisation proche, J. BOSSAN, « Les réquisitions judiciaires relatives aux données de connexion : suite... et fin ? », Droit pénal, n°7-8, 2022, 17. L'auteur distingue, en effet, les données administratives, qui correspondent à l'identité de l'utilisateur ainsi qu'aux informations relatives au paiement, des données techniques, plus sensibles. Certains auteurs ont proposé d'autres catégories : G. HAAS, A. DUBARY, « Cybercriminalité : mais que fait la justice ? », Lamy Droit des affaires, n°168, 2021 ; M. BOUCHET, « Conservation et accès aux données de connexion dans le cadre des enquêtes pénales : mode d'emploi », Gaz. Pal., n°31, 2022.

[66] Les deux premières catégories recouvrent, en réalité, celle, plus large, des données de connexion. V. également en ce sens, M. AUDIBERT, « L'accès aux données de trafic et de localisation dans le cadre d'une enquête judiciaire », Lexbase, Procédure pénale, 2022.

reconstruit autour de la notion de donnée, pour laisser entrevoir un droit commun de la preuve numérique (**B**).

A : L'éclatement regrettable du régime de la preuve numérique

En portant sur le même objet — la donnée —, toutes les techniques d'enquête numériques devraient être soumises aux mêmes garanties légales. Pourtant, nombreux sont les auteurs à avoir souligné une absence de cohérence[67], relevant même l'existence d'« un encadrement à géométrie variable[68] ». Pour se convaincre de ces disparités, il convient de s'intéresser plus avant au régime de ces mesures. Traditionnellement, en droit interne, elles sont soumises à trois conditions dont l'objectif est de garantir la protection des droits des personnes mises en cause et qui tiennent à la gravité de l'infraction concernée, à la durée de la mesure ainsi qu'à l'organe chargé de l'autoriser.

La condition tenant à la gravité de l'infraction concernée, d'abord, permet de s'assurer de la proportionnalité du recours aux techniques d'enquête numériques et devrait, dès lors, s'imposer pour chacune d'elles. Pourtant, elle est absente s'agissant des perquisitions informatiques[69] et des mises au clair de données chiffrées[70]. En revanche, la peine encourue doit être d'au moins trois ans d'emprisonnement lorsqu'il s'agit de recourir aux drones[71] ou à une géolocalisation[72] et, s'agissant des opérations de cyberpatrouilles, elles sont limitées aux crimes et délits punis d'une peine d'emprisonnement commis par la voie des communications électroniques[73]. Les techniques d'enquête numériques prévues aux articles 706-95 et suivants du code de procédure pénale[74], quant à elles, ne concernent que les infractions relevant de la

---

[67] J.-C. SAINT-PAU, « Les investigations numériques et le droit au respect de la vie privée », AJ Pénal, 2017, p. 321 ; O. DÉCIMA, « Du piratage informatique aux perquisitions et saisies numériques ? », AJ Pénal, 2017, p. 315.
[68] M. TOUILLIER, « Lumière sur un arsenal de lutte contre une délinquance tapie dans l'ombre », *op. cit*.
[69] Toutefois, sauf s'ils agissent dans le cadre de l'enquête de flagrance, les enquêteurs doivent obtenir le consentement de la personne concernée : Art. 57-1, Code de procédure pénale.
[70] Il faut noter que l'article 230-1 *in fine* permet de recourir aux moyens de l'État soumis au secret de la défense nationale afin d'obtenir les données en clair, mais, cette fois, seulement lorsque la peine encourue est égale ou supérieure à deux ans d'emprisonnement.
[71] Art. 230-47, Code de procédure pénale.
[72] Art. 230-32, Code de procédure pénale. En revanche, lorsque le moyen technique permettant la géolocalisation doit être introduit dans un lieu privé qui n'est pas destiné ou utilisé à l'entrepôt de véhicules, fonds, valeurs, marchandises ou matériel ou qui n'est pas un véhicule situé sur la voie publique ou dans de tels lieux, la peine encourue doit être au moins égale à cinq ans : Art. 230-34, al. 2, Code de procédure pénale.
[73] Art. 230-46, Code de procédure pénale.
[74] Il s'agit de l'interception de paroles (Art. 706-96, Code de procédure pénale), de la captation de données informatiques (Art. 706-102-1, Code de procédure pénale), du recours aux IMSI-Catcher (Art. 706-95-20, Code de procédure pénale), de l'accès aux correspondances stockées (Art. 706-95-1, Code de procédure pénale) et des interceptions de communications (Art. 706-95-1, Code de procédure pénale).

criminalité organisée énoncées aux articles 706-73 et 706-73-1 du même code, lesquelles sont, à tout le moins, punies de trois ans d'emprisonnement. S'agissant, enfin, des réquisitions, elles ne sont, en principe, soumises à aucune condition de gravité[75]. Toutefois, lorsque sont concernées des données de connexion, l'infraction en cause doit être punie de trois ans d'emprisonnement ou, si la mesure a pour seul objet d'en identifier l'auteur, doit être un délit puni d'un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques. Par ailleurs, si les réquisitions concernent uniquement les équipements terminaux de la victime et qu'elles interviennent à sa demande, l'infraction doit seulement être punie d'emprisonnement[76].

La condition tenant à la durée de la mesure, ensuite, diffère également selon la technique d'enquête étudiée. En effet, l'usage des drones[77], l'interception des correspondances[78], la captation de données informatiques[79] et les sonorisations et fixations d'images[80] sont limités à un mois, renouvelable une fois. Les opérations de géolocalisation, quant à elles, ne peuvent excéder huit jours ou, dans le cas où l'infraction concernée relèverait de la criminalité organisée, quinze jours. À l'issue de ces délais, elles peuvent néanmoins être reconduites pour un mois renouvelable, sans pouvoir excéder un an ou, si l'infraction relève de la criminalité organisée, deux ans[81]. Le recours aux IMSI-Catcher ne connaît de limite temporelle, fixée à quarante-huit heures, que dans le cas où le dispositif a pour objet d'intercepter les correspondances émises ou reçues par un équipement terminal[82]. Enfin, aucun délai maximum n'encadre les perquisitions informatiques[83], la mise au clair de données chiffrées[84], les cyberpatrouilles[85], l'accès aux

[75] Art. 60-1, 60-2, 77-1-1 et 77-1-2, Code de procédure pénale.
[76] Art. 60-1-2, Code de procédure pénale.
[77] Durant l'instruction, le recours à ce dispositif est autorisé pour quatre mois, renouvelables dans la limite de deux ans : Art. 230-48, Code de procédure pénale.
[78] Art. 706-95, Code de procédure pénale. Durant l'instruction, cette mesure est limitée à quatre mois, renouvelables dans la limite d'un an ou, si l'infraction relève de la criminalité organisée, de deux ans : Art. 100-2, Code de procédure pénale.
[79] Durant l'instruction, le recours à ce dispositif est autorisé pour quatre mois, renouvelables dans la limite de deux ans : Art. 706-95-16, Code de procédure pénale.
[80] *Ibidem.*
[81] Durant l'instruction, elle est autorisée pour quatre mois renouvelables, sous réserve des mêmes durées maximales que dans le cadre de l'enquête : Art. 230-33, Code de procédure pénale.
[82] En effet, aucune condition de durée n'est imposée lorsque le dispositif a seulement pour objet 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 : Art. 706-95-20, Code de procédure pénale.
[83] Art. 57-1, Code de procédure pénale.
[84] Art. 230-1, Code de procédure pénale.
[85] Art. 230-46, Code de procédure pénale.

correspondances stockées[86] et les réquisitions[87] sauf, pour ces dernières, s'il s'agit de requérir des opérateurs de télécommunications qu'ils conservent le contenu des informations consultées[88].

Enfin, quant à l'organe compétent pour autoriser la mesure, le procureur de la République intervient s'agissant de la mise au clair de données chiffrées[89], de l'usage des drones[90] et des cyberpatrouilles[91]. Il laisse sa place au juge des libertés et de la détention lorsqu'il s'agit d'accéder à des correspondances[92], de procéder à une sonorisation, à une captation d'images[93] ou de données informatiques[94] ou, enfin, d'intercepter des communications[95], y compris lorsque cette interception résulte de l'utilisation d'un IMSI-Catcher[96]. Concernant les géolocalisations, les deux autorités se partagent la compétence, selon le lieu où le dispositif est installé et/ou la durée de la mesure[97]. Il en va de même pour les réquisitions où, malgré les critiques[98], le juge des libertés et de la détention n'intervient que si celles-ci portent sur les données de connexion émises par un avocat ou si elles tendent à conserver des données de contenu[99]. Enfin, les perquisitions informatiques font, quant à elles, l'objet d'un régime particulier au sein duquel aucune autorisation n'est requise si les enquêteurs agissent en flagrance et, en enquête préliminaire, s'ils disposent de l'assentiment de l'intéressé. À défaut d'un tel consentement, le juge des libertés et de la détention peut tout de même autoriser la mesure si l'enquête est relative à une infraction punie d'une peine d'emprisonnement d'une durée égale ou supérieure à trois ans[100].

---

[86] Art. 706-95-1 et 706-95-2, Code de procédure pénale.
[87] Art. 60-1, 60-2, 77-1-1 et 77-1-2, Code de procédure pénale.
[88] En ce cas, les données ne peuvent être conservées qu'un an : 60-2, al. 2 et 77-1-2, al. 2, Code de procédure pénale.
[89] Art. 230-1, Code de procédure pénale.
[90] Art. 230-48, Code de procédure pénale.
[91] Mais cette autorisation n'est requise que lorsque les enquêteurs recueillent, à cette occasion, des données : Art. 230-46, Code de procédure pénale.
[92] Art. 706-95, Code de procédure pénale.
[93] 706-95-12, Code de procédure pénale.
[94] *Ibidem*.
[95] Art. 706-95-1, Code de procédure pénale.
[96] Art. 706-95-20, Code de procédure pénale.
[97] En effet, le procureur de la République est compétent pour autoriser la mesure pour une durée maximale de quinze jours consécutifs lorsque l'enquête porte sur un crime ou une infraction mentionnée aux articles 706-73 ou 706-73-1 ou pour une durée de huit jours dans les autres cas : Art. 230-33, 1°, Code de procédure pénale. De même, si le moyen technique permettant la géolocalisation doit être introduit dans un lieu privé qui n'est pas destiné ou utilisé à l'entrepôt de véhicules, fonds, valeurs, marchandises ou matériel ou qui n'est pas un véhicule situé sur la voie publique ou dans de tels lieux, seul le juge des libertés et de la détention peut autoriser la mesure : Art. 230-34, al. 2, 1°, Code de procédure pénale.
[98] V. *infra*.
[99] Art. 60-1-2, 60-2 et 77-1-1, Code de procédure pénale.
[100] Art. 57-1 et 76, Code de procédure pénale.

À l'évidence, de profondes différences se font jour sans qu'il soit possible de comprendre, immédiatement, leur raison d'être. Effectivement, toutes les mesures d'enquête numériques portent atteinte aux droits à la vie privée et à la protection des données ce qui, théoriquement, devrait justifier l'édiction de garanties analogues, sinon identiques. Toutefois, ce désordre pourrait, en réalité, n'être qu'apparent, car, en y regardant de plus près, certains éléments, dont la nature de la donnée fait partie, pourraient justifier une variation des garanties encadrant les techniques d'enquête numériques.

B : L'élaboration progressive du régime de la preuve numérique

À l'image des réquisitions[101], les garanties entourant les techniques d'enquête numériques pourraient fluctuer selon la sensibilité de la preuve qu'elle vise à recueillir, donc selon la nature de la donnée en cause. Pour s'en convaincre, il convient d'étudier, précisément, l'objet des mesures d'enquête numériques. À l'analyse, elles portent, à la fois, sur des données d'identité, des données de trafic et de localisation ainsi que sur des données de contenu, à l'exception des réquisitions et de la géolocalisation qui ne concernent pas ces dernières. Partant, ces mesures d'enquêtes devraient connaître un encadrement moins exigeant que celui dévolu, par exemple, aux mises au clair de données chiffrées qui, elles, peuvent également porter sur des données de contenu, ce qui n'est pourtant pas le cas[102]. En revanche, la nature de la preuve a eu une incidence dans le cadre des réquisitions où les données de connexion réclament une exigence de gravité accrue[103]. De surcroît, ce critère vient, ici et là, justifier des aménagements au sein du régime d'une même technique d'enquête. Ainsi, le recours aux IMSI-Catcher se trouve, lorsque des données de contenu sont en cause, subordonné à l'autorisation de juge des libertés et de la détention. La nature de la donnée semble donc déjà jouer un rôle dans la détermination du régime des techniques numériques d'enquête, bien que celui-ci ne soit pas systématique. Si ce critère ne suffit pas, à lui seul, à justifier l'oscillation des garanties légales, en existe-t-il un autre susceptible, en s'y additionnant, de l'expliquer ? Celui-ci pourrait trouver son origine dans la jurisprudence de la Cour européenne des droits de l'homme opérant une distinction selon que l'intrusion dans le droit à la vie privée s'opère en temps réel ou en temps

[101] V. *supra*.
[102] V. *supra*.
[103] V. *supra*.

différé, considérant la mesure plus attentatoire dans le premier cas[104]. Il s'agit, pour le dire autrement, de distinguer les recueils de données déjà disponibles des interceptions de flux actifs de données qui seraient plus intrusives, l'individu, véritablement surveillé, n'ayant aucune possibilité de les supprimer[105]. Préconisé par la juridiction de Strasbourg, et repris par la Cour de justice de l'Union européenne[106], ce critère a-t-il une incidence dans l'encadrement interne des techniques d'enquête numériques ? La condition tenant à la gravité, d'abord, est imposée pour toutes les mesures consistant à intercepter un flux actif de données. À l'inverse, elle est absente s'agissant des perquisitions informatiques, de la mise au clair des données chiffrées et des réquisitions, lesquelles sont bien des techniques de recueil. Toutefois, lorsque les réquisitions concernent des données de connexion, l'exigence de gravité réapparaît. Il en va de même pour l'accès aux correspondances stockées qui, s'il ne permet qu'un recueil, est, en portant sur des données de contenu, soumis à une exigence de gravité. Partant, le critère lié à la nature de la donnée vient se cumuler au premier et justifier l'accroissement des garanties. La condition tenant à la durée, ensuite, s'impose dans la majorité des cas impliquant une interception de données, à l'exception notable des cyberpatrouilles. À l'inverse, elle s'applique s'agissant de l'accès aux correspondances stockées qui ne permet pourtant qu'un simple recueil. Si le cas des cyberpatrouilles ne trouve, *a priori*, aucune explication, il semble que, dans le second cas, la condition de durée soit, une nouvelle fois, justifiée par la nature des données concernées. Le régime des IMSI-Catcher illustre cette affirmation, la mesure n'étant limitée que lorsqu'elle porte sur des données de contenu. Enfin, concernant la condition tenant à la qualité de l'organe compétent, il est très difficile de déceler une quelconque logique. En effet, si les techniques d'enquête impliquant une interception supposent parfois l'intervention du juge des libertés et de la détention[107], celle-ci est souvent subordonnée à la durée de la mesure ou à la nature des données concernées[108]. En outre, dans d'autres cas, le procureur de la République demeure compétent, en dépit de la sensibilité de ces dernières[109]. Parallèlement, les simples

[104] CEDH, 5ème sec., 8 févr. 2018, *Ben Faiza c/ France*, req. n°31446/12, spé. §74 – D. actu., 2018, obs. N. Nalepa.
[105] Le Professeur Décima affirme, à ce sujet, qu'« il existe (ou devrait exister) désormais deux grands types d'investigations numériques, que le code de procédure pénale traite malheureusement ensemble ». Précisément, selon l'auteur, « D'une part, les autorités répressives peuvent détourner un flux de données » ; « D'autre part, les investigations peuvent consister à s'introduire dans un ordinateur pour en fouiller le contenu et extraire toute information utile ». Contrairement à la Cour européenne des droits de l'homme, le Professeur Décima estime les premières plus intrusives : O. DÉCIMA, « Du piratage informatique aux perquisitions et saisies numériques ? », *op. cit*. V. également en ce sens, P. COLLET, « La censure des réquisitions de données informatiques en enquête préliminaire ! », JCP-G, 2022, n° 4.
[106] CJUE, gde ch., 6 oct. 2020, *La Quadrature du Net e. a.*, Aff. Jtes. C-511/18, C-512/18 et C-520/18, §187.
[107] Il en va ainsi pour les sonorisations et captations d'images et les interceptions de communications : V. *supra*.
[108] Il en va ainsi pour la géolocalisation et pour le recours aux IMSI-Catcher : V. *supra*.
[109] Il en va ainsi de l'usage des drones ainsi que des opérations de cyberpatrouilles : V. *supra*.

recueils de données réclament, lorsque celles-ci sont intrusives, l'intervention du juge des libertés et de la détention[110].

À bien observer le régime des techniques d'enquête numériques, la nature de la donnée et la temporalité de la mesure semblent avoir une incidence, laquelle n'apparaît toutefois pas aboutie. Ainsi, pour trouver une cohérence, ce régime doit être strictement pensé autour de ces deux critères, seuls à même de mesurer la gravité de l'ingérence portée dans les droits à la vie privée et à la protection des données à caractère personnel. Avant d'entrer dans le détail, il convient de préciser que l'ensemble des techniques d'enquête numériques est subordonné à une exigence de nécessité qui, si elle est parfois visée par les textes, s'impose dans tous les cas à la lecture de l'article préliminaire du code de procédure pénale[111]. Une fois cela indiqué, il s'agit de s'intéresser précisément aux critères précédemment dégagés. Alors que le critère temporel doit, selon nous, déterminer la durée de la mesure ainsi que l'information de la personne concernée, le critère matériel, quant à lui, doit guider les conditions tenant à la gravité de l'infraction et à la qualité de l'organe d'autorisation.

Quant à la condition tenant à la durée de la mesure, elle n'a de sens que dans le cadre des techniques captant un flux actif de données. En effet, imposer une telle exigence pour les recueils d'informations serait hypocrite, car si ceux-ci pouvaient se tenir dans le temps, ils s'apparenteraient, finalement, à une captation. Partant, cette condition doit être prévue pour chacune des mesures impliquant une interception. En outre, la nature de la donnée doit jouer un rôle dans la détermination du délai, lequel doit être plus court lorsque des informations sensibles sont en cause. En l'état actuel de la législation, les techniques d'enquête impliquant une interception active de données de contenu sont limitées à deux mois et, s'il s'agit de données de trafic et de localisation, à deux ans. Cependant, aujourd'hui, aucun délai n'encadre les captations de données de connexion réalisées par les IMSI-Catcher ou celles opérées dans le cadre des cyberpatrouilles. Partant, les secondes devraient se limiter à deux mois et les premières, à deux ans. Ce critère temporel doit également guider la garantie tenant à l'information de l'individu faisant l'objet de la mesure. Effectivement, si celle-ci consiste à

[110] Il en va ainsi pour les réquisitions concernant les données de connexion émises par un avocat ainsi que pour l'accès aux correspondances stockées : V. *supra*.

[111] En effet, « Au cours de la procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous le contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espère, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction » : Article préliminaire, III, al. 6, Code de procédure pénale.

intercepter un flux actif de données, prévenir la personne concernée pourrait nuire à l'efficacité de l'enquête. En outre, la limitation de la durée de la mesure permet de corriger cette absence, à condition qu'une information soit délivrée une fois la technique d'enquête échue. Pour les techniques impliquant un simple recueil, la personne pourrait être informée, les données étant, dans tous les cas, à disposition des enquêteurs.

Conformément aux exigences de la Cour de justice de l'Union européenne, seules les infractions « graves » devraient permettre la mise en œuvre d'une technique numérique d'enquête portant sur des données de trafic et de localisation et, *a fortiori*, de contenu[112]. Cette condition devrait donc s'étendre lorsqu'il s'agit de mettre au clair des données chiffrées ou de procéder à une perquisition informatique. Une difficulté demeure : comment définir un seuil ? En France, celui de trois ans d'emprisonnement est majoritairement imposé[113], mais est-il suffisamment élevé pour la Cour de Luxembourg ? Rien ne permet de l'affirmer[114] et il y a fort à penser que ce critère soit progressivement affiné par les juridictions, internes comme européennes. En outre, afin d'éviter les détournements de procédure, il apparaît essentiel de préciser que ces techniques d'enquête ne doivent pas avoir pour objet de rechercher d'autres infractions que celles visées dans la décision les autorisant, et ce à peine de nullité[115].

Enfin, la nature des données en cause devrait guider le choix de l'organe autorisant la mesure d'enquête, la jurisprudence de la Cour de justice de l'Union européenne l'impose. En effet, elle estime que la sensibilité des données de connexion exige « un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante » intervenant « à la suite d'une demande motivée »[116] des autorités répressives[117]. Elle ajoute « qu'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique ne peut se voir reconnaître la qualité de tiers par rapport aux intérêts légitimes en cause » et, qu'ainsi il « n'est pas en mesure d'effectuer le contrôle préalable des demandes d'accès aux

[112] V. *supra*.
[113] V. *supra*.
[114] V. également en ce sens, O. CAHN, « Données de connexion et enquête pénale : la chèvre et le chou malmenés », JCP-G, 2022, n°40.
[115] V. également en ce sens, J.-C. SAINT-PAU, « Les investigations numériques et le droit au respect de la vie privée », *op. cit*.
[116] L'exigence de motivation est essentielle en la matière, la Chambre criminelle y veille : V. not. à ce sujet, P. COLLET, « Le renforcement progressif des garanties applicables à deux mesures intrusives : la géolocalisation et la sonorisation », Rev. sc. crim., 2021, p. 29.
[117] CJUE, gde ch., 5 avr. 2022, *G.D. c/ Commissioner of An Garda Síochána e. a.,* Aff. C-140/20, §106.

données conservées »[118]. La solution de la Cour de Luxembourg[119] ayant été reprise par la Chambre criminelle[120], elle devrait s'imposer en France, en dépit des résistances du Conseil constitutionnel[121] et des contestations du monde judiciaire. Plus loin, en étant dictée par la nature des données concernées, elle devrait s'étendre à la totalité des techniques d'enquête numériques, lesquelles portent toutes, à tout le moins, sur des données de connexion[122]. Ainsi, le recours à d'autres critères, tels que la durée de la mesure, le lieu de l'implantation du dispositif ou l'assentiment de l'intéressé ne semble plus pertinent et seule la nature de la donnée doit être prise en compte. Qu'il s'agisse de confier ce contrôle au juge des libertés et de la détention ou à une autorité administrative indépendante dédiée[123], le ministère public devra céder sa compétence.

À l'occasion des réflexions sur une réforme d'ensemble du code de procédure pénale[124], le législateur pourrait construire un droit commun de la preuve numérique. Les critères pour réaliser cet édifice sont déjà présents, encore faut-il qu'il ait, réellement, la volonté de le bâtir...

---

[118] *Ibid*., §109.
[119] La proposition de règlement *e-evidence* va également en ce sens en imposant, lorsqu'il s'agit d'émettre une injonction de conservation de données de trafic et de localisation ou de contenu, l'intervention d'un juge, d'une juridiction ou d'un juge d'instruction, à l'exclusion de toute autre autorité en matière pénale : Art. 4§2, Proposition de règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, *op. cit*.
[120] Cass. crim., 12 juill. 2022, n°21-83.710, bull. crim. n°769, n°21-83.820, bull. crim. n°771, n° 21-84.096, bull. crim. n°772, n°21-83.729, Inédit.
[121] Le Conseil constitutionnel estime en effet que l'autorisation donnée par le procureur de la République en enquête préliminaire constitue une garantie suffisante, y compris lorsque sont en cause des données de connexion : Cons. const., 3 déc. 2021, *M. Omar Y*, n°2021-952 DC, §13.
[122] V. pour une extension de cette exigence à la géolocalisation : A. GOGORZA, « L'accès aux données de connexion : les affres du pluralisme normatif », Dr. Pénal, 2022, n°10, étude 20.
[123] V. à ce sujet, A. ARCHAMBAULT, « Accès aux données de connexion : quelles pistes pour une mise en conformité ? », AJ Pénal, 2022, p. 400.
[124] V. à ce sujet, M. LÉNA, « Le nouveau code de procédure pénale (brouillon) », AJ Pénal, 2023, p. 1 ; L. GARNERIE, « Éric Dupond-Moretti présente un plan d'action pour restaurer la place de la justice », Gaz. Pal., 2023, n°1, p. 3.