

# LES NOTES DU CRGN

Centre de Recherche de la Gendarmerie Nationale

Numéro 114 – Avril 2025

Chef d'escadron Matthieu AUDIBERT (Dr)



Priorité stratégique de la prospective



L'avenir des territoires numériques

Le CRGN certifie que ce document a été rédigé par une intelligence humaine

## LA PREUVE NUMÉRIQUE AU CŒUR DES ENQUÊTES JUDICIAIRES, QUELS ENJEUX ET QUELLES PERSPECTIVES EN PROCÉDURE PÉNALE ?

L'émergence d'Internet, l'avènement des connexions à haut débit et la diffusion des outils numériques ont considérablement bouleversé les usages sociaux. L'écrasante majorité de la population française dispose d'un accès à Internet et les trois quarts possèdent au moins un téléphone portable connecté. Dans le même temps, les applications de messagerie instantanée sont en constant développement ainsi que les objets connectés. Les délinquants se sont eux aussi emparés de ces évolutions technologiques marquées par un recours massif aux techniques de chiffrement<sup>1</sup> des communications et des supports numériques. Auparavant un attribut de la criminalité organisée, le chiffrement concerne désormais tous les utilisateurs. Consubstantiel aux révélations sur les programmes d'interception américains, le chiffrement est devenu un argument commercial largement mis en exergue par les opérateurs et les fabricants de supports numériques. Essentiel au respect du droit fondamental à la vie privée ainsi qu'à la sécurité des systèmes d'information<sup>2</sup>, le chiffrement constitue également un obstacle aux investigations judiciaires<sup>3</sup> dans la mesure où il peut agir comme un véritable « mur » à la collecte des preuves numériques.

Or, « depuis la constatation d'une infraction pénale jusqu'au jugement de son auteur, toute la chaîne pénale est articulée autour de la question cardinale de la preuve »<sup>4</sup>. De plus, selon une étude menée par l'Union européenne (UE), « plus de 85 % des enquêtes pénales nécessitent désormais la recherche de données numériques »<sup>5</sup>. En effet, ces dernières renseignent sur la vie personnelle ou professionnelle d'un suspect ou d'une victime : historique des appels, échanges de courriels, de messages, agenda électronique, opérations bancaires, téléphonie mobile, géolocalisation des objets connectés. Les preuves numériques sont particulièrement diversifiées. Elles impliquent aussi une certaine technicité. Le temps où les enquêteurs recherchaient les aveux du ou des principaux suspects est loin. La preuve numérique est indiscutablement une preuve technique reposant sur le maniement d'outils informatiques, notamment logiciels, parfois complexes à utiliser. Ainsi, l'intérêt grandissant pour les techniques de recueil de la preuve numérique s'explique par l'inadéquation des méthodes d'enquête classiques face à une délinquance de plus en plus perfectionnée et astucieuse.

Pouvant présenter parfois un caractère massif à l'ère du *big data*, le recueil de la preuve numérique au cours des enquêtes judiciaires implique des investigations numériques nécessairement invasives, réalisées dans le but de conserver un maximum de traces et d'indices, la preuve numérique demeurant par essence « fragile et volatile »<sup>6</sup>. Or, dans la mesure où le numérique est partout présent dans la vie de la majorité des citoyens, collecter de telles données constitue un moment crucial dans toute enquête judiciaire. Il en découle nécessairement une atteinte plus ou moins forte au droit au respect de

1 « Opération technique reposant sur un procédé cryptographique visant à rendre la compréhension d'une donnée impossible à une personne ne disposant pas de la clé de déchiffrement ». Voir : EYMARD, Olivier. Questions de cryptologie. *Délibérée*, 2018, vol. 3, n° 1, p. 60.

2 BLISSON, Laurence. Petits vices et grandes vertus du chiffrement. *Délibérée*, 2019, vol. 2, n° 7, p.56.

3 HUREL, Benoist, LEMONIER, Vincent. L'enquête pénale à l'épreuve du chiffrement. *Délibérée*, 2018, vol. 4, n° 2, p. 53.

4 GUINCARD, Serge, BUISSON, Jacques. *Procédure pénale*. LexisNexis, 16<sup>e</sup> édition, 2023, p. 287.

5 QUÉMÉNER, Myriam. Le numérique, nouveau vecteur de l'administration de la preuve en matière pénale. *Dalloz IP/IT*, 2024, p. 61.

6 QUÉMÉNER, Myriam. L'accès à la preuve numérique, enjeu majeur de toute enquête pénale : pratique et perspectives. *Dalloz IP/IT*, 2018, p. 418.

la vie privée des personnes concernées par la mesure. Or, l'article 8 de la Convention européenne de sauvegarde des droits de l'Homme énonce que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». Cet article précise ensuite dans quelles circonstances les autorités publiques (les enquêteurs) peuvent s'ingérer dans l'exercice de ce droit. Cette ingérence doit être prévue par la loi, être nécessaire et proportionnée aux objectifs poursuivis par les autorités publiques. Ainsi, il n'est pas possible d'accéder à tout type de données pour tout type d'infractions. De plus, qui doit contrôler et autoriser ces accès ?

L'articulation entre le recueil de la preuve numérique dans les enquêtes et la protection du droit au respect de la vie privée est donc un sujet fondamental mais également particulièrement complexe. Le même constat peut être dressé à propos de la loyauté de certaines techniques d'enquête numérique employées. À l'heure de l'intelligence artificielle (IA) ou encore de l'*open source intelligence* (OSINT), les perspectives sont intéressantes et les questionnements multiples.

Enfin, la preuve numérique est mouvante, en constante évolution au gré des différentes lois adoptées par le Parlement ou encore au gré de la jurisprudence de la Cour européenne des droits de l'Homme, de la Cour de justice de l'Union européenne (CJUE), du Conseil constitutionnel et de la Cour de cassation.

Dans un premier temps, il est nécessaire de présenter les principales méthodes de recueil de la preuve numérique et leur articulation avec les droits fondamentaux, *via* une lecture pratique et fonctionnelle. Dans un second temps, il conviendra d'aborder une approche modernisée et systémique de l'administration de la preuve numérique en procédure pénale.

## I) La preuve numérique et les droits fondamentaux dans les enquêtes judiciaires

La preuve numérique apparaît plus que jamais centrale dans l'ensemble des procédures judiciaires menées sous la direction du procureur de la République ou du juge d'instruction. En effet, différents moyens numériques sont susceptibles d'être utilisés par les services d'enquête dans le but de prouver la commission d'une infraction.

Saisies judiciaires de données informatiques, enquêtes sous pseudonyme, captation des données informatiques, accès aux correspondances stockées, géolocalisations ou encore interceptions de correspondances sont autant de techniques permettant, à des degrés divers, d'obtenir des données relatives à un suspect ou à son environnement. L'actualité judiciaire nous l'a récemment montré : c'est l'exploitation du téléphone portable de Dominique Pelicot par les enquêteurs qui a permis de révéler l'affaire des « *viols de Mazan* »<sup>7</sup>.

Or, le recueil de la preuve numérique implique par essence une atteinte substantielle au droit au respect de la vie privée des personnes. Initialement réservé à certaines formes les plus graves de criminalité et de délinquance, depuis plusieurs années, un mouvement de fond tend à étendre les possibilités de recourir à différents modes de recueil de la preuve numérique pour des infractions relevant du droit commun. Occupant une place de plus en plus importante dans le procès pénal par symétrie avec la preuve génétique, l'importance accordée à la preuve numérique témoigne d'une plus grande recherche d'efficacité dans l'adaptation de la procédure pénale aux nouvelles formes de criminalités<sup>8</sup>. Cette recherche d'efficacité implique parfois d'aller plus en profondeur dans la mémoire des outils numériques et, par conséquent, plus en profondeur dans la vie privée des personnes. Il est ainsi possible, au cours d'une perquisition, d'accéder aux contenus numériques de l'ensemble des supports présents sur les lieux mais également d'accéder aux contenus distants accessibles depuis ces mêmes supports<sup>9</sup>. De même, dans certaines circonstances, un suspect ne pourra pas s'opposer à la communication ou à la mise en œuvre du code de déverrouillage de son téléphone, son éventuel refus de collaborer avec les enquêteurs pouvant être constitutif d'une infraction<sup>10</sup>.

La preuve numérique questionne également un principe fondamental en procédure pénale : la loyauté de la preuve. Condition d'exercice des droits de la défense et plus généralement de la conduite du procès équitable, l'exigence de loyauté probatoire revêtait un caractère presque absolu<sup>11</sup>. Ce principe a, par la suite, été aménagé. En effet, « *le stratagème employé par un agent de l'autorité publique pour la constatation d'une infraction ou l'identification de ses auteurs ne constitue pas en soi une atteinte au principe de loyauté de la preuve* »<sup>12</sup>. Ainsi, par principe, le stratagème mis en œuvre par les autorités publiques visant à provoquer à la preuve est admissible. Par exception, un tel stratagème serait déloyal s'il avait pour effet d'atteindre un droit essentiel ou une garantie fondamentale de la personne visée par les investigations<sup>13</sup>. Une construction jurisprudentielle a ainsi distingué la provocation à la commission d'une infraction

7 JAUSSENT, Violaine. Procès des viols de Mazan : la "personnalité à double facette" de Dominique Pelicot, jugé pour avoir drogué et livré sa femme à des hommes. *Franceinfo*, 9 septembre 2024.

8 CASTETS-RENARD, Céline. Quelles nouveautés en matière de preuve numérique ? *Justice et Cassation*, 2017, p. 23.

9 Article 57-1 du Code de procédure pénale.

10 AUDIBERT, Matthieu. Refuser de communiquer le code de déverrouillage de son téléphone peut être une infraction. *Actualité juridique Pénal*, 2022, p. 577.

11 Cass. Ass. Plén., 7 janvier 2011, n° 09-14.316 pour un enregistrement d'une conversation téléphonique à l'insu de l'auteur des propos utilisés.

12 Ass. Ass. Plén., 9 décembre 2019, n° 18-86.767.

13 *Ibidem*.

(interdite) *versus* la provocation à la preuve (autorisée). Or, les investigations numériques peuvent reposer sur de véritables stratagèmes : création de faux sites Internet pour identifier des suspects, utilisation de pseudonymes<sup>14</sup>, possibilité de se faire passer pour des acheteurs en ligne, etc.

La preuve numérique questionne également l'applicabilité du droit de garder le silence et du droit de ne pas s'auto-incriminer. Si un suspect ne parle pas, ses données peuvent parler pour lui. À la suite d'une construction jurisprudentielle de la Chambre criminelle<sup>15</sup>, confirmée par l'Assemblée plénière de la Cour de cassation<sup>16</sup>, sous certaines conditions, il est possible d'imputer à un suspect qui refuserait de communiquer le code de déverrouillage de son téléphone l'infraction prévue par l'article 434-15-2 du Code pénal<sup>17</sup>. En effet, la Cour de cassation a notamment énoncé que « *le droit de ne pas s'incriminer soi-même ne s'étend pas aux données que l'on peut obtenir de la personne concernée en recourant à des pouvoirs coercitifs mais qui existent indépendamment de la volonté de l'intéressé* »<sup>18</sup>. Cette solution a été critiquée par la doctrine juridique<sup>19</sup>. Pour autant, cette construction jurisprudentielle a été récemment remise en cause par un arrêt rendu par la CJUE<sup>20</sup>. Effectivement, au titre de la protection des données à caractère personnel et de l'ingérence dans le droit au respect de la vie privée, elle a jugé que l'exploitation des données contenues dans un téléphone portable devait être subordonnée à un contrôle préalable effectué soit par une juridiction, soit par une autorité administrative indépendante<sup>21</sup>.

Cet exemple illustre toute la difficulté, pour le législateur et les magistrats, d'appréhender la preuve numérique. En particulier, il n'existe pas à ce jour des dispositions organisées et dédiées à la preuve numérique dans le Code de procédure pénale<sup>22</sup>.

## **II) Vers une approche modernisée et systémique de la preuve numérique en procédure pénale**

Le recueil de la preuve numérique présente de nombreux défis pour la procédure pénale : son articulation avec les principes et droits fondamentaux est complexe. L'expansion des différents modes de recueil de la preuve a pour corollaire un affaiblissement des principes et droits fondamentaux. Il devient donc de plus en plus impératif de moderniser les règles applicables au recueil de la preuve numérique dans le but, d'une part, de maintenir et renforcer les capacités des services d'enquête et, d'autre part, de préserver les droits fondamentaux. Cette conciliation complexe doit reposer sur une démarche méthodique afin de confronter et mettre en balance les techniques d'investigations numériques avec les droits fondamentaux<sup>23</sup>.

Cette démarche méthodique transparaît de plus en plus dans les différents arrêts<sup>24</sup> rendus par la CJUE sur le sujet épineux de la conservation et de l'accès aux données de connexion. Au fil du temps et face à la carence du droit primaire et du droit dérivé de l'UE, la CJUE a construit un ensemble prétorien visant à renforcer la protection des droits fondamentaux. Celui-ci a ensuite été transposé par la Cour de cassation dans plusieurs arrêts qui constatent l'inadéquation de plusieurs règles de procédure pénale française avec le droit de l'UE<sup>25</sup>. Or, depuis 2022, aucune modification législative n'est intervenue sur ces questions et, de fait, la validité des enquêtes perdure grâce au régime restrictif des nullités dégagé par la Cour de cassation<sup>26</sup>. Cette situation n'est néanmoins pas satisfaisante : il est indispensable de reconstruire le recueil de la preuve numérique. Considérant son caractère particulièrement intrusif dans les droits fondamentaux, leur protection ne peut s'accommoder d'un dispositif prétorien. Les efforts de refondation de ce régime doivent donc se concentrer d'une part, sur les garanties entourant les différents modes de recueil de la preuve et, d'autre part, sur les autorités autorisant et contrôlant la mise en œuvre de ces mesures.

14 Article 230-46 du Code de procédure pénale.

15 Cass. Crim., 13 octobre 2020, n° 20-80.150.

16 Cass. Ass. Plén., 7 novembre 2022, n° 21-83.146.

17 AUDIBERT, Matthieu, *op. cit.* note 10.

18 Cass. Crim., 10 décembre 2019, n° 18-86.878.

19 CONTE, Philippe. Refus de remettre une convention secrète de déchiffrement d'un moyen de cryptologie – Élément matériel – Droit de ne pas s'incriminer soi-même. *Droit pénal*, n° 2, février 2020, comm. 27 ; ROUSSEL, Bruno. Droit de se taire et investigations numériques : l'accès aux ressources numériques d'une personne visée par une enquête. *Revue Lamy droit de l'immatériel*, n° 176, décembre 2020, p. 24-27.

20 CJUE, gr. ch., 4 octobre 2024, aff. C-548/21 – *CG c/ Bezirkshauptmannschaft Landeck*.

21 AUDIBERT, Matthieu. *L'exploitation d'un téléphone portable revue par la Cour de justice de l'Union européenne*. Actualité juridique Pénal, 2024, p. 567.

22 AUDIBERT, Matthieu. *Le recueil de la preuve numérique : enjeux et perspectives en procédure pénale*, Thèse de droit privé et sciences criminelles, Université Paris Nanterre, 2024.

23 AUROY, Benoît. La preuve numérique en procédure pénale : un système à (re)construire. *Recueil Dalloz*, 2023, p. 697.

24 CJUE, gr. ch., 8 avr. 2014, aff. C-293/12 et C-594/12, *Digital Rights Ireland et Seitlinger e.a* ; CJUE 21 déc. 2016, aff. C-203/15 et C-698/15, *Tele2 Sverige* ; CJUE 6 oct. 2020, aff. C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a. c/ Premier ministre e.a.* ; CJUE 2 mars 2021, aff. C-746/18, *Prokuratuur* ; CJUE 5 avr. 2022, aff. C-140/20, *G.D c/ Commissioner of An Garda Siochana* ; CJUE 20 sept. 2022, aff. C-793/19 et C-794/19, *SpaceNet* ; CJUE 30 avr. 2024, aff. C-178/22, *Bolzano*.

25 Cass. Crim., 12 juill. 2022, n°s 21-83.710, 21-83.820, 21-84.096 et 20-86.652.

26 *Ibid.*

Les différentes normes relatives au recueil de la preuve numérique souffrent d'un éparpillement dans le Code de procédure pénale et leur régime apparaît illisible et déconstruit au gré des évolutions législatives et jurisprudentielles. Une piste de réforme pourrait être de créer un droit commun de la preuve numérique en procédure pénale, articulé autour de la méthodologie de recueil des données et des garanties associées au degré d'ingérence dans la vie privée et à la durée des mesures d'investigation comme seuil d'intervention du juge.

Le constat est identique s'agissant des nouveaux modes de recueil de la preuve numérique. En effet, elle est en évolution perpétuelle, étant intimement liée aux évolutions technologiques. Au-delà des prouesses techniques, elle repose sur l'immensité des perspectives pratiques offertes par de nouvelles techniques et technologies probatoires. Les enquêteurs sont confrontés à des volumes de données toujours plus importants à analyser. Stockées sur des serveurs ou des supports physiques, ces données à analyser dans un laps de temps toujours contraint représentent un immense défi pour les enquêteurs<sup>27</sup>. De ce fait, l'IA peut représenter de nombreux espoirs pour faciliter les investigations. De plus en plus utilisée par les enquêteurs, elle suscite des interrogations sur son positionnement dans l'administration de la preuve numérique. De même, les utilisateurs de solutions technologiques diffusent toujours plus d'informations en libre accès sur Internet. Réseaux sociaux, communications en ligne, ce sont autant d'informations qui représentent une véritable mine d'or pour les enquêteurs. Pour autant, le recueil plus ou moins massif et potentiellement automatisé d'informations disponibles en sources ouvertes sur Internet (OSINT, cf. *supra* p. 2) dans le cadre des enquêtes judiciaires pose de nombreuses difficultés<sup>28</sup>.

En conclusion, le recueil de la preuve numérique est une matière vivante, inhérente aux évolutions technologiques et techniques ainsi qu'aux pratiques des utilisateurs, tant victimes que mis en cause. Mais c'est une matière vivante qui doit être profondément et indiscutablement renouvelée, même si ses fondations en procédure pénale sont solides et permettent la recherche d'un juste équilibre entre la protection des droits fondamentaux et la recherche, l'identification et la poursuite des auteurs d'infractions. Les articulations entre le droit positif et les évolutions technologiques sont complexes et transcendent l'ensemble des matières juridiques. S'agissant de la procédure pénale, il est indispensable qu'elle conserve une certaine plasticité et une certaine malléabilité face aux évolutions technologiques, en particulier numériques.

Dans le silence de la loi, la jurisprudence crée parfois de manière prétorienne le régime applicable, comme nous l'avons constaté à propos de l'accès aux données de trafic et de localisation. Il faut donc renforcer le contrôle légal de ces modes de recueil de la preuve numérique sans toutefois faire preuve d'un légalisme irraisonné. Le numérique est un vrai défi pour la société contemporaine, car le cyberspace a été construit et existe en s'affranchissant des contrôles étatiques. La définition des modalités de contrôle de ces mesures ne peut donc pas être que nationale. Il faut néanmoins se prémunir contre une révolution procédurale qui n'apparaît pas souhaitable. Les techniques d'enquête numérique ont changé la manière de mener les enquêtes mais « *il s'agit de procédés qui ont changé sous l'effet de la technologie, mais dont la fonction ne diffère pas* »<sup>29</sup>. Dans ces conditions, il faut questionner le principe fondamental du droit de la preuve : la preuve est-elle licite, est-elle probante<sup>30</sup> ?

L'impératif de réformer et de mieux encadrer le recueil de la preuve numérique en procédure pénale doit donc être mené dans le cadre d'une réforme d'envergure de l'enquête pénale. Cette réforme globale devra être menée en associant tous les acteurs : enquêteurs, magistrats, experts mais aussi techniciens et spécialistes des investigations numériques, et ce, dans le but de rendre la procédure pénale plus intelligible pour les non-spécialistes des investigations numériques et pour les citoyens. « *L'écriture de la loi n'a jamais été aisée tout simplement parce qu'il s'agit d'un art de la conception, d'une habileté à saisir le principal. C'est pourquoi il ne faut pas négliger les conditions dans lesquelles se conduit cet exercice* »<sup>31</sup>.

Le chef d'escadron Matthieu AUDIBERT est chef du département doctrine et prospective juridique du Commandement du ministère de l'Intérieur dans le cyberspace, docteur en droit privé et sciences criminelles, chercheur associé au Centre de Droit Pénal et de Criminologie (EA 3982) de l'Université Paris Nanterre. La présente Note est une synthèse de sa thèse, soutenue en 2024 : Le recueil de la preuve numérique : enjeux et perspectives en procédure pénale.

Le contenu de cette publication doit être considéré comme propre à son auteur et ne saurait engager la responsabilité du CRGN.

27 AUDIBERT, Matthieu. L'extraction et l'exploitation des données contenues dans des supports numériques. *Actualité juridique Pénal*, 2023 p. 116.

28 Voir, par exemple : Cass. Crim., 30 avril 2024, n° 23-80.962 à propos du délit de collecte de données à caractère personnel par un moyen déloyal.

29 VERGÈS, Étienne. La preuve numérique, entre continuité et changement de paradigme. *Revue Justice Actualités*, ENM, n° 1, 2019.

30 *Ibid.*

31 URVOAS, Jean-Jacques. Libres réflexions sur l'écriture de la loi. *Actualité juridique Pénal*, 2023, p. 85.