Projet REV – Lot 5
« Aspects juridiques »
Livrable – L 5.4

L'administration des preuves numériques résultant de l'exploitation de vulnérabilités informatiques

Réalisé par Lila de Lattre

Encadré par Noémie Véron, responsable Lot 5

Version	Date	Auteur	Commentaires
V0.1	25 juin 2025	Lila de Lattre	Réalisation du livrable
V0.2	25 juin 2025	Noémie Véron	Mise en forme et relecture
V1.1	30 juin 2025	Lila de Lattre	Bibliographie, résumé et relecture
V1.2	01 juillet 2025	Noémie Véron	Relecture
V2.0	01 juillet 2025	Lila de Lattre	Modifications

Résumé

L'administration des preuves obtenues par l'exploitation de vulnérabilités informatiques diffère selon deux variables. La matière dans laquelle elles sont produites (en procédure civile, en procédure pénale ou en procédure administrative contentieuse) et la qualité de la personne qui les produit (un particulier ou une autorité publique). En procédure civile, ce type de preuve n'est admissible qu'au motif de leur caractère indispensable à la prétention d'une partie au procès. En effet, leur production par un particulier est intrinsèquement illicite et déloyale, puisqu'elles sont obtenues en infraction des dispositions du code pénal. Leur recevabilité conditionnée est le fruit de développements jurisprudentiels.

En procédure pénale leur production par les particuliers est autorisée sans restriction, ceux-ci s'exposant cependant à des poursuites ultérieures. Les autorités publiques doivent, quant à elles, respecter le cadre juridique applicable sans détournement ou contournement des règles de procédures sous peine de voir les éléments récoltés rejetés.

En procédure administrative contentieuse, les règles de recevabilité sont celles relatives à la production de notes blanches par services de renseignement dans le cadre de l'examen par le juge administratif, du bien-fondé d'une mesure administrative.

En outre, de l'adaptation du système probatoire national à l'ère du numérique, des critères de qualification peuvent être appliqués aux preuves numériques pour permettre aux magistrats et aux parties de les interpréter en conditions valides. Ces critères proviennent principalement de la pratique des experts judiciaires, ce sont l'authentification, l'intégrité, la traçabilité et la conservation. Une forme de consensus international émerge quant à la nécessité d'établir des règles précises et rigoureuses pour assurer la fiabilité des preuves obtenues au moyen du numérique.

Ces règles permettraient de minimiser les actes de contestation des pièces du dossier par les parties opposées, susceptibles d'engendrer des coûts supplémentaires ou de rallonger les procédures. Enfin, les modalités de contestation donnent lieu à d'importants débats, notamment, en procédure pénale, sur le droit à ne pas s'auto-incriminer et, en procédure administrative contentieuse, sur la véracité des éléments relatés par les notes blanches.

Table des matières

Liste des principales des abréviations

CA	Cour d'appel
CAA	Cour d'appel administrative
CE	Conseil d'Etat
C. cass.	Cour de cassation
Ch. com.	Chambre commerciale (Cour de cassation)
Ch. crim.	Chambre criminelle (Cour de cassation)
Ch. soc.	Chambre sociale (Cour de cassation)
CEDH	Cour européenne des droits de l'homme
CNEJITA	Commission nationale des experts de justice en informatique et techniques associées
CPP	Code de procédure pénale
CSI	Code de la sécurité intérieure
JORF	Journal officiel de la République française
STAD	Système de traitement automatisé de données
TA	Tribunal administratif

Introduction

Le deuxième livrable requis au sein du projet Recherche et Exploitation de Vulnérabilités (REV) a pour objet de clarifier l'administration des preuves numériques obtenues par l'exploitation de vulnérabilités informatiques, aux fins de déterminer comment ces éléments pourraient être versés aux procédures et utilisés dans différents procès, civil, pénal ou administratif.

Le terme de preuves numériques regroupe en réalité plusieurs types de preuves, de nature variée. L'absence de définitions strictes et consensuelles en droit interne renforce cette circonstance.

La distinction classique des éléments de cette même catégorie est celle qui s'attache à séparer les preuves analogiques digitalisées, comme les photos, les vidéos ou le courrier électroniques, des preuves obtenues par le biais de la technologie, comme les métadonnées, les coordonnées GPS, les traces d'utilisation d'un logiciel ou d'une intrusion frauduleuse dans un système de traitement automatisé de données (STAD)[1]. L'intérêt de cette classification est sa capacité à faciliter la compréhension des difficultés auxquelles les parties, les magistrats, et avocats peuvent être confrontés, dans l'appréhension des preuves analogiques numérisées et des autres. Elle souligne également la fonction de la personne qualifiée ou de l'expert judiciaire[2].

Au niveau des preuves analogiques numérisées la difficulté réside dans la certification de la véracité de la preuve apportée. Il s'agira de prouver que l'élément n'a pas été modifié, truqué, garantissant que les faits interprétés sont avérés. L'expert aura une fonction de certificateur, il en sera l'artisan. En ce qui concerne les preuves obtenues par le biais de la technologie, la difficulté sera davantage celle de trouver un sens, de donner de la cohérence à un ensemble disparate d'informations. Ici, les connaissances

[1] VERGES (E.), « La preuve numérique, entre continuité et changement de paradigme », *Revue Justice Actualité*, édition n°21/Juin 2019, p. 16.

[2] Pour rappel ces personnes qualifiées peuvent avoir la qualité d'experts judiciaires : toute personne physique ou morale habilitée et inscrite sur l'une des listes prévues à l'article 157 du code de procédure pénale, figurant sur une des listes nationales dressées par la Cour de cassation ou une des listes dressées par les cours d'appel. Elles peuvent aussi être toute personne ayant prêté serment, selon les conditions de l'article 60 du code de procédure pénale. Pour des raisons de praticité, ces deux types de personnes seront nommées « *experts judiciaires* » dans ce document.

techniques de l'expert seront mises en avant puisqu'il aura, outre sa fonction de certificateur, une fonction interprétative. Ces fonctions sont complémentaires.

À l'échelle européenne, le terme de « preuve électronique » remplace celui de preuve numérique. Tant l'Union européenne que le Conseil de l'Europe utilise ce premier dans leurs actes normatifs, leurs recommandations ou lignes directrices. Les deux termes recoupent une réalité similaire.

Par exemple, le Conseil de l'Europe définit la preuve électronique par « *toute preuve qui découle de données contenues ou produites par un dispositif dont le fonctionnement dépend d'un logiciel ou de données stockées ou transmises sur un système ou un réseau informatique* »[3]. Au niveau de l'Union européenne, la définition est un peu plus éloignée du sens généralement accordé à la preuve numérique. Selon le règlement relatif aux injonctions de production ou de conservation de preuves électroniques, elle serait « *les données relatives aux abonnées, les données relatives au trafic ou les données relatives au contenu stockées par un fournisseur de services ou pour le compte d'un fournisseur de services, sous forme numérique (…)* »[4].

Cependant, cet éloignement tient davantage à l'objet du règlement qui vise à créer des injonctions de production ou de conservation aux fournisseurs de services, la définition de la preuve électronique étant étayée à travers ce prisme bien précis.

Eu égard la promiscuité de l'Union européenne et du Conseil de l'Europe, les parallèles entre la directive 2013/40[5] et la Convention sur la cybercriminalité[6], le Règlement

[3] Lignes directrices du Comité des Ministres du Conseil de l'Europe CM(2018)169 sur les preuves électroniques dans les procédures civiles et administratives, adoptées par le Comité des Ministres le 30 janvier 2019, lors de la 1335e réunion des Délégués des Ministres.

[4] Art. 3, 8) du Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de libertés prononcées à l'issue d'une procédure pénale, *JOUE* L 191 du 28 juillet 2023.

[5] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, *JOUE* L. 218/8, 14 août 2013 (Directive 2013/40).

[6] Convention STE n°185 du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité, Budapest.

européen sur la protection des données[7] et la Convention 108+[8], la Convention européenne des droits de l'homme[9] et la Charte des droits fondamentaux[10], il n'est pas déraisonnable de supposer que la définition générale de la preuve électronique, donnée par le Conseil de l'Europe, puisse être reprise dans un autre cadre par l'Union européenne.

Dans ce livrable il sera recouru à l'expression « *preuve numérique* », la définition sera celle retenue par le Conseil de l'Europe, puisqu'elle couvre à la fois les preuves analogiques numérisées, et celle obtenue par le biais de la technologie.

Face aux preuves numériques, toutes les problématiques associées n'ont pas nécessairement été solutionnées. Elles sont en partie le fruit de l'ajustement du système probatoire français aux nouvelles technologies, dont l'impact n'a pas été suffisamment anticipé.

En effet, les preuves numériques ont dû répondre aux conditions générales de recevabilité qui existaient déjà, mais qui avaient été construites dans un monde où l'internet des objets, par exemple, n'était pas encore implanté dans notre société. L'aspect « *numérique* » de ces preuves n'a pas entraîné une modification immédiate et substantielle des règles de procédure. Ce sont les expériences de juges, qui, au fil des années, ont souligné l'impératif d'ajustement plus étroitement le système probatoire. Les évolutions sont donc principalement jurisprudentielles. Des principes directeurs, comme celui de la licéité ou la loyauté, ont ainsi difficilement survécu à l'apparition des preuves numériques, leur importance dans certaines procédures s'étant graduellement amenuie.

Il ne faut cependant pas se méprendre. L'utilisation quotidienne de la technologie génère un volume considérable de données et métadonnées, sans que celles-ci soient forcément toutes qualitatives, intéressantes, ou fiables.

---

[7] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), *JOUE* L 119 du 4 mai 2016.

[8] Convention (STE n°108) du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement des données à caractère personnel, (Convention 108 +).

[9] Convention (STCE n°005) du Conseil de l'Europe du 4 novembre 1950, de sauvegarde des droits de l'homme et des libertés fondamentales, (Convention EDH).

[10] Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000, *JOCE* C 364/01, (Charte DFUE).

Deux réflexions naissent de ce constat.

Tout d'abord, toutes les données collectées dans le cadre des missions des services de police judiciaire ou de renseignement ne sont pas des preuves. Qu'il s'agisse de la captation des données informatiques, mise en œuvre sur le fondement de l'article 706-102-1 du code de procédure pénale (ci-après « CPP ») ou L.853-2 du code de la sécurité intérieure (ci-après « CSI »), de l'accès au support physique ou numérique de données, par le biais des articles 60-3, 77-1-3 et 99-5 du CPP, ou de la mise au clair de données chiffrées des articles 230-1 et suivants du CPP également, les autorités compétentes ont l'obligation d'opérer un tri pour ne garder que les données intéressant l'enquête. Celles, donc, qui pourront être qualifiées de « *preuves* » par les avocats ou le magistrat.

Partant, les données obtenues de l'exploitation de vulnérabilités informatiques, technique employable en vertu des articles ci-dessus, subissent plusieurs opérations avant d'être exploitables en procédure. Elles sont récupérées par des personnes qualifiées à l'aide d'outils technologiques, triées, puis interprétées par les acteurs judiciaires.

Ensuite, la qualification d'une donnée de preuve numérique n'est pas suivie d'une présomption de fiabilité. Que cette preuve soit le fruit d'une mission de police judiciaire ou de renseignement, ou qu'elle soit celle apportée par une partie en civil en infraction des articles 323-1 à 323-3-1 du code pénal, par exemple. En effet, la donnée, la preuve, est vulnérable : elle est effaçable, modifiable, non statique[11]. Ainsi, en parallèle des ajustements jurisprudentiels concernant l'incorporation des preuves numériques en procédure, des règles se sont développées pour répondre spécifiquement à l'aspect « *numérique* » de ces preuves, afin de garantir leur fiabilité.

En résulte l'étude dans ce livrable, à la fois des conditions générales de recevabilité de la preuve numérique (**1**), et des conditions spécifiques qui leur sont applicables (**2**). Il conviendra de revenir aussi sur la relation entre les magistrats, les avocats et les experts judiciaires dans ce processus. Un point très important puisqu'il met en exergue la problématique de la contestation de ces preuves par les parties, susceptible de mettre en

[11] MIGAYRON (S.), « Critères d'appréciation technique, vraies et fausses preuves numériques », in *La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique*, colloque par la Compagnie nationale des experts de justice en informatique et techniques associées (CNEJITA), le 13 avril 2010, p. 19. URL : https://www.lagbd.org/images/3/3a/Colloque_CNEJITA_13_Avril_2010.pdf, consulté le 01 juillet 2025.

porte à faux le travail effectué par l'expert, dont la justesse est notamment appréciée par le magistrat.

1. Les conditions générales de recevabilité de la preuve numérique

En matière probatoire, la recevabilité de la preuve se distingue de sa valeur probante. La première notion renvoie à la possibilité pour un élément de rentrer dans le dossier d'une affaire afin d'être pris par la suite en considération[12]. La deuxième est la capacité pour un élément du dossier à établir suffisamment la véracité du fait allégué[13].

Ainsi, les conditions générales de recevabilité sont des critères auxquels les éléments doivent être conformes, sous peine de devoir être écartés. Trois variables sont susceptibles d'influencer ces critères. La matière (civile, pénale ou administrative), le système de preuve qui y est associé (système de preuve légale ou système de preuve libre), l'application des principes structurants de licéité ou de loyauté de la preuve. Enfin, selon la matière, d'autres variables peuvent influencer ces critères, sans qu'il soit possible d'en dégager une tendance générale. Pour une meilleure clarté de propos, il faut avant toute présentation revenir sur le sens de ces variables.

Le système de preuve :

Le droit interne oppose le système de preuve libre au système de preuve légale. Dans ce dernier, la loi organise l'admissibilité et la force probante des modes de preuve. La valeur des preuves est hiérarchisée, codifiée, ce qui affaiblit par ailleurs le pouvoir d'appréciation souverain du juge[14]. À l'inverse, dans un système de preuve libre, la loi n'impose aucune condition de forme pour établir la preuve d'un fait[15].

Le principe de licéité des preuves :

Le principe de licéité des preuves, renvoie directement à l'article 9 du code de procédure civile : « *il incombe à chaque partie de prouver conformément à la loi les faits*

[12] GUINCHARD (S.), DEBARD (T.), « *Lexique des termes juridiques 2024-2025* », Dalloz, coll. « Lexiques Dalloz », 32ème éd., 2024.
[13] *Ibidem*.
[14] LARDEUX (G.), *« Preuve : règles de preuve – Les principes fondamentaux* », Répertoire de droit civil, Octobre 2018, Mise à jour de Juillet 2024, p. 54.
[15] FERAL-SCHUHL (CH.), *Le droit à l'épreuve de l'internet*, Dalloz, coll. « Praxis Dalloz », 8e éd., p. 7.

nécessaires au succès de sa prétention ». La preuve illicite est celle obtenue en violation de la législation, mais aussi celle qui « *heurte un des principes jugés supérieurs, considérés comme d'ordre public impérieux, au premier rang desquels le respect des droits de l'homme, et ce, qu'ils aient été consacrés par un texte ou pas* »[16].

Parmi ces droits de l'homme, le droit au respect de sa vie privée, tel que présent à l'article 9 du code civil[17], mais également à l'article 8 de la Convention européenne des droits de l'homme[18], et 7 de la Charte des droits fondamentaux de l'Union européenne[19].

Les preuves numériques obtenues par le moyen de l'exploitation de vulnérabilités informatiques sont intrinsèquement illicites, puisqu'elles violent le principe de rang supérieur du droit au respect de la vie privée, auquel renvoient les articles 226-1 et 226-15 du code pénal[20].

Lorsqu'elles sont produites par des parties privées, elles sont aussi susceptibles de violer les dispositions des articles 323-1 à 323-3 du code pénal, relatifs aux atteintes aux systèmes d'information[21].

Le principe de loyauté de la preuve :

En vertu de celui-ci, les éléments de preuves en doivent avoir été recueillis sans stratagèmes, sans détournement des règles de procédures à l'insu de la personne, sans fraude ou moyens frauduleux. Il s'agit d'une construction jurisprudentielle[22] qui participe au droit à un procès équitable.

Or, il ne fait aucun doute que la méthode d'exploitation de vulnérabilités est à la fois un stratagème, ou, au minimum, réalisée à l'insu de la personne concernée. Ce qui fait théoriquement des preuves obtenues par ce moyen, des preuves déloyales.

Comme expliqué ci-dessus, chacune de ces variables s'applique différemment selon la matière. Partant, il a semblé opportun d'étudier méthodologiquement, l'impact du

[16] LARDEUX (G.), « *Preuve : règles de preuve – Les principes fondamentaux* », préc., p. 73.
[17] Art. 9, code civil.
[18] Art. 8, Convention (STCE n°005) du Conseil de l'Europe du 4 novembre 1950, de sauvegarde des droits de l'homme et des libertés fondamentales.
[19] Art. 7, Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000, *JOCE* C 364/01.
[20] Voir notamment Livrable 1.
[21] *Ibidem*.
[22] Lardeux (G.), « *Preuve : règles de preuve – Les principes fondamentaux* », préc. p. 53.

système de preuve et des principes structurants pour chaque matière. Une catégorie autre permettra de venir spécifier le cas des critères supplémentaires.

Il s'agira d'étudier la procédure civile (**1.1**), la procédure pénale (**1.2**) et la procédure administrative contentieuse (**1.3**).

1.1 La procédure civile

Par procédure civile, il faut entendre toute « *procédure suivie, en matière civile, commerciale, prud'homale, rurale et sociale devant les juridictions de l'ordre judiciaire* »[23]. Les règles probatoires de cette matière sont disséminées dans plusieurs sources, entre le code civil, le code de procédure civile et les jurisprudences de la Cour de cassation.

1.1.1 L'impact du système de preuve

Tout d'abord, la charge de la preuve est à celui qui allègue un fait. Autrement dit, elle ne dépend pas de la qualité de la partie.

Par ailleurs, depuis l'ordonnance n°2016-131[24], le système probatoire civil a évolué pour instaurer le principe de liberté de la preuve, tel qu'en atteste l'article 1358 du code civil : « *hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen* »[25]. Conformément à ce principe, aucun mode de preuve ne peut être exclu par le magistrat[26]. Il existe cependant une exception en matière de preuve d'un acte juridique d'une somme ou d'une valeur excédant 1 500 euros, seul l'écrit sous signature privée ou authentique est admissible[27]. Cette règle contient elle-même des exceptions, en cas

[23] GUINCHARD (S.), DEBARD (T.), « *Lexique des termes juridiques 2024-2025* », *op. cit*.
[24] Ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, JORF n°35, 11 février 2016
[25] Art. 1358, code civil.
[26] Vergès (E.), « Étude : La preuve civile », in *Procédure civile*, Vergès (E.) (dir.), Lexbase, 2022, p. 3.
[27] Art. 1359, code civil ; somme fixée par l'article 1er du décret n°80-533 du 13 juillet 1980 pris pour l'application de l'article 1341 du code civil.

d'impossibilité matérielle ou morale de se procurer un écrit, s'il est d'usage de ne pas établir ce dernier, ou en cas de perte par force majeure, par exemple[28].

Certains modes de preuve sont par ailleurs encadrés par le code civil, tels que la preuve par écrit[29], la preuve par témoins[30], la preuve par présomption judiciaire[31], la preuve par aveu[32] et la preuve par serment[33].

En effet, bien que la preuve soit libre en procédure civile, toutes les preuves n'ont pas le même degré de force probante. Par exemple, l'aveu judiciaire dispose d'une force probante absolue[34]. Cette hiérarchisation implique une rigidité dans la forme que doivent revêtir certaines catégories de preuves, d'où le cadre applicable aux cinq modes de preuve ci-dessus.

Cela veut dire que les preuves obtenues par l'exploitation de vulnérabilité sont admissibles en procédure civile, mais qu'elles n'auront pas nécessairement une force probante élevée, selon le type de preuve numérique dont il s'agit. L'appréciation de cette force probante est une compétence des juges, qui, en dehors des cas où un texte juridique détermine celle-ci, disposent d'une liberté souveraine. Cela signifie qu'ils peuvent opérer un tri entre les preuves retenues pour leur raisonnement, sans qu'ils soient tenus de s'expliquer précisément sur chacune des preuves produites[35].

Enfin, dernière précision, le système de liberté de la preuve est également présent en matière matrimoniale, où les faits « *invoqués en tant que causes de divorce ou comme défenses à une demande peuvent être établis par tout mode de preuve* »[36]. Ici, le code civil ne règlemente pas certains types de preuve ni ne hiérarchise leur force probante. Par exemple, les traces d'une intrusion dans un système de traitement automatisé de

[28] Article 1360, code civil. Voir également l'article 1361 du code civil « *Il peut être suppléé à l'écrit par l'aveu judiciaire, le serment décisoire ou un commencement de preuve par écrit corroboré par un autre moyen de preuve* ».
[29] Art. 1363 à 1380, code civil.
[30] Art. 1381, code civil.
[31] Art. 1382, code civil.
[32] Art. 1383 à 1383-2, code civil.
[33] Art. 1384 à 1386-1, code civil.
[34] Vergès Étienne, « *Étude : La preuve civile* », *art. cit.,* p. 29.
[35] *Ibid.,* p. 30.
[36] Art. 259, code civil.

données par un ancien partenaire peuvent être admises comme preuves pour démontrer les faits d'une cyberviolence[37].

1.1.2 Les principes structurants de licéité et de loyauté

Les principes de licéité et de loyauté des preuves en matière civile ont connu une évolution similaire.

Auparavant strictement irrecevables, les preuves illicites ont bénéficié d'un aménagement conditionné à partir de 2007 quant à leur production en procédure. Il en va de même pour la production de preuves déloyales, bien que la modification de leur statut ait été effectuée ultérieurement, en 2023.

Le point de départ de cette évolution est l'arrêt de la Cour européenne des droits de l'homme, *L.L contre France*[38] qui créa un « *droit à la preuve* », c'est-à-dire la faculté « *de pouvoir faire la preuve de quelque chose, c'est-à-dire l'accès à tout élément de preuve et la possibilité de produire tout élément de preuve quelle qu'en soit sa teneur* ».

Dans l'arrêt de la Cour européenne, le requérant contestait le recours par son ex-conjointe, durant une procédure de divorce, à un document médical le concernant pour justifier ses allégations d'alcoolisme. Selon le requérant, l'admissibilité de ce document portait atteinte à son droit à la vie privée, tel que garanti par l'article 8 de la Convention européenne des droits de l'homme[39].

C'est à l'occasion de son examen relatif à la légitimité du but poursuivi que la Cour a jugé l'atteinte causée au droit à la vie privée du requérant, légitime. Elle a estimé que *« l'ingérence était destinée à "la protection des droits et libertés d'autrui", en l'occurrence le droit à la preuve du conjoint aux fins de faire triompher ses prétentions* »[40]. La Cour a cependant condamné la France pour une violation de l'article 8. Elle a examiné notamment que la production de la pièce contestée n'avait pas été déterminante dans le prononcé du divorce. Que la pièce avait été invoquée à titre subsidiaire et surabondant[41]. Ainsi, selon les principes de cette jurisprudence, le droit à

[37] CEDH, 11 février 2020, *Buturaga c. Roumanie*, n°56867/15.
[38] CEDH, octobre 2006 *L.L. c. France*, 10, n°7508/02.
[39] Pour rappel, il est tout à fait possible de limiter la portée des articles 8 à 11 de la Convention tant que cette ingérence est prévue par la loi, poursuit un but légitime, et est nécessaire dans une société démocratique.
[40] *Ibid.,* c. 40.
[41] *Ibid.,* c. 46.

la preuve ne prévaut que dans la mesure où la pièce invoquée est nécessaire pour l'exercice de celui-ci.

Ce dénouement, ainsi que le raisonnement adopté par la Cour, a été partiellement repris par la Cour de cassation pour la première fois en matière de preuve illicite par un arrêt du 15 mai 2007[42].

La Cour de cassation a tout d'abord interprété le droit à la preuve comme étant une composante du principe d'égalité des armes : « *attendu qu'en statuant ainsi, alors que constitue une atteinte au principe de l'égalité des armes résultant du droit au procès équitable garanti par l'article 6 de la Convention européenne des droits de l'homme le fait d'interdire à une partie de faire la preuve d'un élément essentiel pour le succès de ses prétentions* ».

Elle a ensuite assoupli le régime de recevabilité des preuves illicites, lorsque « *cette preuve est indispensable*[43] *au succès de la prétention de celui s'en prévaut, et que l'atteinte portée aux droits antinomiques en présence est strictement proportionnée au but poursuivi* ». Les principes dégagés par cette jurisprudence ont été réappliqués dans les affaires postérieures[44].

Cependant, la preuve illicite est toujours susceptible d'être déclarée irrecevable, quand bien même les faits allégués seraient avérés. Ce fut notamment le cas d'un employeur, dont la preuve justifiant le bien-fondé du licenciement a été déclarée illicite par la Cour de cassation parce qu'elle résultait d'une exploitation des fichiers de journalisation, laquelle constitue un traitement de données à caractère personnel licite uniquement si la personne y a consenti[45]. En l'occurrence, le licencié n'y avait pas consenti.

En matière de preuves déloyales, celles recueillies « *à l'insu de la personne ou obtenue par une manœuvre ou un stratagème* », leur irrecevabilité fut un principe de

[42] C. cass., ch. com., 15 mai 2007, n° 06-10.606.
[43] Nous soulignons.
[44] C. cass., 1ère civ., 5 avril 2012, n° 11-14.177 ; C. cass., ch. soc., 9 novembre 2016, n° 15-10.203 ; C. cass., ch. soc., 30 septembre 2020, n° 19-12.058 ; C. cass., ch. soc., 25 novembre 2020, n° 17-19.523 ; C. cass., ch. soc. 8 mars 2023, n° 21-17.802.
[45] C. cass., ch. soc., 9 avril 2025, n°23-13.159.

jurisprudence constante[46] jusqu'au revirement opéré par la Cour de cassation par un arrêt du 22 décembre 2023[47].

Pour justifier ce revirement, la Cour s'est fondée sur plusieurs arguments. Considérant sa position en matière de recevabilité de preuves illicites, elle a rappelé la difficulté de tracer une frontière claire entre celles-ci et les preuves déloyales. Cette position, combinée à l'admission des preuves déloyales en matière pénale, a poussé une partie de la doctrine à suggérer une évolution de la jurisprudence, puisqu'il existait un risque que « *la voie pénale permette de contourner le régime plus restrictif des preuves en matière civile* »[48].

Enfin, la Cour de cassation est revenue sur la décision de la Cour européenne des droits de l'homme sur la recevabilité des preuves déloyales, laquelle n'y était pas opposée. La Cour européenne estimait qu'en cas de conflit de droit (ici, le droit de la preuve et le droit au respect de la vie privée), il appartenait aux juges de mettre en balance les différents droits et intérêts privés en cause. Elle a également ajouté que l'égalité des armes impliquait l'obligation d'offrir à chaque partie la possibilité de présenter sa cause, sans que des conditions la placent en « *net désavantage par rapport à son adversaire* ».

Sur la base de ces constats, la Cour de cassation a opéré un revirement de jurisprudence, en rendant recevables, de manière conditionnée, les preuves déloyales. Celles-ci doivent être indispensables à l'exercice du droit à la preuve ; les atteintes aux autres droits en cause doivent être strictement proportionnées au but poursuivi, et leur prise en compte ne doit pas porter atteinte au caractère équitable de la procédure. Autrement dit, ces preuves doivent avoir été discutées conformément au principe du contradictoire.

Partant, les preuves illicites ou déloyales en matière civile peuvent être reçues, pour peu que leur prise en compte répondre à des critères de proportionnalité.

Appliqué à notre cas, celui des preuves numériques obtenues par l'exploitation de vulnérabilités informatiques, celles-ci, bien qu'illicites et déloyales, pourraient être jugées recevables si leur production est la seule manière pour une partie de faire valoir ses prétentions.

---

[46] De jurisprudence constante : C. cass., Ass.,7 janvier 2011, n°09-14-316 et 09-14.667 ; C. cass., 2ème civ., 9 janvier 2014, n°12-23.387 et 12-17.875 ; C. cass., ch. com., 10 novembre 2021, n°20-14.669 et 20-14.670 ; C. cass., ch. soc., 18 mars 2008, n°06-40.852, C. cass., ch. soc., 4 juillet 2012, n°11-30.266.

[47] C. cass., Ass., 22 décembre 2023, n°20-20.648.

[48] C. cass., Ass., 22 décembre 2023, n°20-20.648, c. 11.

Pour finir, l'article 259-1 du code civil dispose qu'en matière de divorce, l'époux « *ne peut verser aux débats un élément qu'il aurait obtenu par violence ou par fraude* ». La notion explicite de fraude permet de dire que les preuves obtenues par l'intrusion frauduleuse sur un système de traitement automatisé de données sont automatiquement irrecevables. Seules les preuves résultant de données publiquement publiées sont autorisées.

Cette spécificité s'inscrit dans un ensemble cohérent de renforcement de la protection de la vie privée des personnes dans le cadre conjugal. Par exemple le droit interne majore les peines liées aux atteintes au secret des correspondances lorsque celles-ci sont commises par le conjoint ou le concubin de la victime, ou le partenaire lié à la victime par un pacte civil de solidarité[49]. De plus, les personnes ayant porté plainte pour violence intrafamiliale peuvent faire vérifier la présence d'un logiciel intrusif sur leur STAD, comme leur portable[50].

Cette possibilité de vérification peut aussi être utilisée en dehors de cas de plaintes, en cas de suspicion d'atteinte à la vie privée et au secret des correspondances, d'intrusion frauduleuse dans un STAD, de telles infractions relevant de la matière pénale.

1.2 La procédure pénale

Par procédure pénale, il faut entendre « l'ensemble des règles qui définissent la manière de procéder pour la constatation des infractions, l'instruction préparatoire, la poursuite et le jugement des délinquants »[51].

1.2.1 L'impact du système de preuve

La matière pénale obéit au système de liberté de la preuve. Cette circonstance est consacrée par l'article 427, alinéa 1er du CPP, dont la formulation est similaire à l'article

[49] Article 226-15, alinéa 3, code pénal, les peines passent d'un an à deux ans d'emprisonnement et de 45 000 euros à 60 000 euros d'amende.

[50] Site du Ministère de l'intérieur, « Lutte contre les violences intrafamiliales : signature d'une convention de partenariat avec le groupe La Poste », publié le 28 septembre 2023, mis à jour le 26 novembre 2024.

[51] GUINCHARD (S.), DEBARD (T.), « *Lexique des termes juridiques 2024-2025* », *op. cit*.

1358 du code civil : « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve (…)* »[52].

Le système de liberté de la preuve est bien plus prégnant dans la matière pénale, le juge peut, par exemple, se fonder sur des pièces obtenues dans le cadre d'une autre procédure pénale[53], ou ayant été obtenues après la clôture de l'information[54]. Par ailleurs, le juge dispose d'une marge de manœuvre plus étendue dans l'appréciation des faits allégués, sur la base de ces preuves. En effet, l'article 427, alinéa 1[er,] poursuit « *les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction* ». À titre complémentaire, l'alinéa 2 du même article dispose que « *le juge ne peut fonder sa décision que sur des preuves qui lui apportées au cours des débats et contradictoirement discutées devant lui* ».

Selon ces deux alinéas, en l'absence de hiérarchisation législative des modes de preuve à l'instar du code civil, le juge est libre d'attribuer la valeur probante qu'il estime raisonnable pour chacune des preuves qui lui sont apportées.

Ainsi, les preuves obtenues par le biais de l'exploitation de vulnérabilité sont admissibles, pour peu qu'elles aient pu être débattues contradictoirement, c'est-à-dire qu'elles aient été librement discutées par les parties. Il en va de même pour les traces de commission d'une ou de plusieurs infractions relatives aux atteintes aux STAD.

Le principe du contradictoire s'étend à l'expertise, souvent requise pour pallier les mécanismes de protection des données récoltées, en imposant que ses résultats aient été discutés contradictoirement[55]. En pratique, l'expert joindre à ses résultats un dossier comprenant l'ensemble des éléments nécessaires à leurs compréhensions, ou effectuer, si nécessaire, à un exercice de simulation en présence de tous les acteurs. Ce serait la simulation d'une intrusion frauduleuse avec l'outil incriminé, par exemple, dans le but sa responsabilité[56].

---

[52] LARDEUX (G.), « *Preuve : règles de preuve – Les principes fondamentaux* », Octobre 2018, *op. cit.,* p. 54.

[53] C. cass., ch. crim., 19 décembre 1973, n°73-90.224.

[54] C. cass., ch. crim., 11 juillet 2001, n°00-84.832.

[55] C. cass., ch. crim., 9 novembre 1972, n°71-93.529.

[56] *La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique*, colloque par la Compagnie nationale des experts de justice en informatique et techniques associées (CNEJITA), *op. cit.,* spéc. p. 78.

1.2.2 Les principes structurants de licéité et de loyauté

En matière de licéité et de loyauté, les preuves obtenues par le biais de l'exploitation de vulnérabilités rentrent dans deux cas de figure.

Lorsqu'elles sont produites par des particuliers, tant leur caractère illicite que déloyal ne font pas échec à leur recevabilité par le juge. Il est de jurisprudence constante que les parties privées ne sont pas soumises aux principes de licéité et de loyauté des preuves[57], les juges répressifs ne pouvant pas écarter ce type de preuve pour peu qu'elles aient été discutées contradictoirement[58].

Dans ces conditions précises, toutes les preuves résultant d'une exploitation de vulnérabilité sont recevables. Et ce, malgré que leur obtention puisse avoir enfreint les dispositions des articles 323-1 à 323-3-1 du code pénal[59] ou des articles 226-1[60] et 226-15, alinéa 2[61] du même code, ce qui rendrait les preuves illicites, ou que l'exploitation de vulnérabilités informatiques s'apparente à un stratagème conduit à l'insu de la personne visée, rendant les preuves déloyales.

Cela ne veut cependant pas dire que le particulier ne s'expose pas à des poursuites pénales ultérieures, sur fond de violation des articles susmentionnés.

---

[57] Voir par exemple : C. cass., ch. crim., 15 juin 1993, n°92-82.509 ; C. cass., ch. crim., 6 avril 1994, n°93-82.717.

[58] Voir par exemple : C. cass., ch. crim., 30 mars 1999, n°97-83.464.

[59] L'article 323-1 du code pénal incrimine le fait « *d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* ».
L'article 323-2 du code pénal incrimine le fait « *d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données* ».
L'article 323-3 du code pénal incrimine le fait « *d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient* ».
L'article 323-3-1 du code pénal incrimine le fait « *sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute données conçus ou spécialement adaptés pour commettre un ou plusieurs des infractions prévues par les articles 323-1 à 323-3 du code pénal* ».

[60] L'article 226-1 du code pénal incrimine le fait « *au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui* ».

[61] L'alinéa 2 de l'article 226-15 du code pénal incrimine le fait « *commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions* ».

Lorsque les preuves sont produites par les services de police judiciaire, les principes de licéité et de loyauté doivent en revanche être respectés[62].

Le respect du principe de licéité implique que l'obtention ait été effectuée conformément à la procédure adéquate. Il sera généralement question des procédures de captation de données informatiques[63], d'accès au support de données informatiques[64] ou de mise au clair de données chiffrées[65]. Ainsi, l'agent qui agit selon les strictes conditions légales qui lui sont applicables ne saurait se voir contester la licéité des preuves obtenues, pour infraction d'atteintes aux STAD, d'atteintes au secret des correspondances ou d'atteintes à l'intimité de la vie privée d'autrui.

Sur ce dernier point, la Cour de cassation a notamment rappelé dans une décision en 2014[66], que l'article 226-1 du code pénal « *loin de présenter une portée générale et absolue, laissant déjà hors de son domaine les interceptions de conversations opérées à de strictes conditions légales par les autorités publiques en charge de la lutte contre le crime, régit seulement la captation et la diffusion, par des particuliers et à l'insu de leur auteur, de propos relatifs à sa vie privée* »[67].

Au niveau du principe de loyauté, « *seul est proscrit le stratagème qui, par un contournement ou détournement d'une règle de procédure*[68]*, a pour objet ou pour effet de vicier la recherche de la preuve en portant atteinte à l'un des droits essentiels ou à l'une des garanties fondamentales de la personne suspectée ou poursuivie* »[69]. Autrement dit, pour qu'une preuve soit jugée déloyale et puisse être écartée, porter atteinte à un droit essentiel ou à une garantie fondamentale ne suffit pas, il faut en outre

[62] C. cass., ch. crim., 27 février 1996, n°95-81.366 ; C. cass., ch. crim., 11 mai 2006, n°05-84.837.
[63] Article 706-102-1, code pénal.
[64] Article 60-3, code pénal.
[65] Article 230-1 et suivants, code pénal.
[66] C. cass., ch. civ., 5 février 2014, n°13-21.929.
[67] Dans cet arrêt la Cour de cassation se prononçait sur le renvoi ou non au Conseil constitutionnel d'une question prioritaire de constitutionnalité qui était ainsi formulée : « *Les articles 226-1 et 226-2 du code pénal, subsidiairement leur interprétation par la jurisprudence constante de la Cour de cassation, méconnaissent le droit à la liberté d'expression garanti par l'article 11 de la Déclaration universelle des droits de l'homme et du citoyen du 26 août 1789, en ce qu'ils interdisent, de façon générale et absolue, toute diffusion de paroles prononcées à titre privé ou confidentiel, enregistrées sans le consentement de leur auteur ?* ». La décision fut un non-lieu à renvoi pour absence de nouveauté de la question et défaut de caractère sérieux.
[68] Nous soulignons.
[69] C. cass., ch. crim., 9 décembre 2019, n°18-86.767.

que l'obtention soit le résultat d'un contournement ou d'un détournement d'une règle de procédure.

Cela signifie que dans le cadre des activités de polices judiciaires, la preuve recueillie par exploitation de vulnérabilités jugée illicite est automatiquement déloyale. Comme expliqué ci-dessus, tant qu'elle respecte le cadre légal l'obtention de la preuve par ces acteurs ne peut se voir opposer ni le droit au respect de la vie privée, ni le droit au secret de ses correspondances. Bien que les opérations autorisées par le cadre légal soient intrinsèquement constitutrices d'une atteinte à ces droits. Ces atteintes n'ont de conséquences que si les opérations ne respectent pas strictement la procédure définie : lorsque la preuve est illicite, les atteintes légalement autorisées ne le sont plus. Le caractère illicite de la preuve a pour effet de porter atteinte aux droits de la personne, ce qui rend la preuve déloyale.

Pour illustrer ce propos, il convient de revenir sur l'arrêt de la chambre criminelle de la Cour de cassation, du 25 octobre 2022[70].

Dans cette affaire, un dispositif de captation de données informatiques avait été mis en place sur un serveur alimentant un réseau de téléphones cryptés aux fins d'une enquête préliminaire diligentée par la juridiction interrégionale spécialisée pour des faits d'association de malfaiteurs et d'infraction aux règles de cryptologie. Treize utilisateurs de téléphones cryptés furent interpellés et mis en examen.

Ceux-ci ont formé un pourvoi contre l'arrêt de la chambre de l'instruction de la Cour d'appel de Nancy du 9 septembre 2021, qui, « *dans l'information suivie contre eux des chefs, notamment, d'infractions à la législation sur les stupéfiants, association de malfaiteurs, importations de stupéfiants en bande organisée et blanchiment, a prononcé sur leurs demandes d'annulation d'actes de la procédure* [71]», en rejetant celles-ci.

Selon les requérants, les preuves produites avaient été collectées de manière **illégale** du fait d'un contournement des règles de procédures, par le recours à des procédés qui ne répondaient pas strictement à la définition légale de la captation de données informatiques.

Ils arguaient notamment le fait « *qu'il ne peut y avoir d'ingérence d'une autorité publique dans l'exercice du droit au respect de sa vie privée que pour autant que cette ingérence est prévue par la loi, celle-ci devant ainsi faire l'objet d'un encadrement légal*

[70] C. cass., ch. crim., 25 octobre 2022, n°21-85.763.
[71] Nous soulignons.

spécifique et précis, qu'est ainsi exclue l'interprétation extensive d'un dispositif légal en place[72]*, pour justifier, au besoin, le recours à des procédés qu'il ne prévoit pas* »[73].

Les procédés incriminés étaient la mise en place d'un « *dispositif de "blocage des opérations" auprès de différents prestataires, de nature à affecter le nom de domaine, la résolution DNS*[74] *et l'infrastructure réseau en place* » et « *des opérations de "redirection des flux", lesquelles consistent en une "modification des règles de routage du réseau"* »[75].

Sur la question de savoir si ces procédés constituent effectivement un contournement des règles de procédure par l'interprétation extensive de celles-ci, la Cour répond par la négative. Elle conclut que ces procédés sont des **opérations préalables** à la captation de données informatiques, une distinction (opération préalable ou principale) que l'article 706-102-1 ne fait pas[76], notamment parce que l'opération de captation « *suppose que les administrateurs de la solution de chiffrement en cause en soient pas mis en mesure de neutraliser l'opération des enquêteurs, en redirigeant les accès vers un autre serveur* »[77].

Leur caractère nécessaire les rend indissociables des opérations de captation stricto sensu, elles rentrent ainsi dans le champ de l'article 706-102-1 du CPP et sont légales. Partant, les preuves obtenues sont bien licites et recevables.

La réutilisation de ce raisonnement par la Cour de cassation pour justifier de la loyauté des preuves met en exergue l'interdépendance de ces deux principes dans ce contexte précis. Lorsqu'il lui est demandé d'étudier la demande de nullité tirée du recours par une autorité publique, non pas à un procédé illégal, mais déloyal, elle renvoie directement aux considérants traitant de la légalité de ceux-ci en jugeant « *qu'il résulte des paragraphes 14 à 16 du présent arrêt qu'aucune déloyauté n'a été commise par les enquêteurs dans la captation des données numériques* »[78].

Sans plus de développements sur la question de la loyauté, cette réutilisation appuie la thèse développée plus haut dans le document, qui veut que dans le cadre des opérations

[72] Nous soulignons.
[73] *Ibid.,* c. 12.
[74] Processus de traduction d'une adresse humainement intelligible en une adresse IP.
[75] *Ibidem.*
[76] *Ibid.,* c.15.
[77] *Ibid.,* c.16.
[78] *Ibid.,* c. 47

utilisant l'exploitation de vulnérabilités par des autorités publiques, la loyauté d'une preuve dépende de sa licéité.

1.3 La procédure administrative contentieuse

Il existe en réalité deux types de procédure administrative, l'une contentieuse et l'autre non contentieuse. Au sens non contentieux, il s'agit « *de l'ensemble des règles qui s'imposent à l'administration, lors de l'édiction d'actes administratifs unilatéraux dans l'objectif de mieux garantir les droits des administrés face à l'administration* ». Au sens contentieux, il s'agit « *de la procédure suivie devant les juridictions administratives, régie par des règles spécifiques caractérisées par l'importance des éléments écrits par rapport aux éléments oraux ainsi que par ses traits inquisitoires* »[79]. Seule la procédure contentieuse sera développée au sein de la présente section, puisqu'elle intéresse la thématique de l'administration de la preuve.

1.3.1 L'impact du système de preuve

Le contentieux administratif répond au système de preuve libre. Il n'existe pas de texte de portée générale régissant les modes de preuves admissibles, ou consacrant une forme de hiérarchie en ceux-ci. Les parties sont libres d'apporter toutes informations jugées pertinentes pour appuyer leur thèse, le juge étant tout autant libre d'en apprécier la valeur probante[80]. Par exemple, le Conseil d'État a considéré en 2014 qu'en l'absence de dispositions législatives contraires, « *l'autorité investie du pouvoir disciplinaire (...) peut apporter la preuve de ces faits devant le juge administratif par tout moyen* »[81]. Le système de preuves par tout moyen irrigue cependant tout le contentieux administratif, ce qui concède une grande liberté au juge dans son appréciation[82].

Le juge administratif aura généralement à traiter des éléments obtenus par le biais d'une opération de captation de données informatiques, autorisée selon les règles de procédure inscrites à l'article L.853-2 du CSI, sous la forme de notes blanches.

[79] GUINCHARD (S.), DEBARD (T.), « *Lexique des termes juridiques 2024-2025* », *op. cit*.
[80] Leger (D.), « *Rapport sur la preuve devant le juge administratif français* », Rapport du Conseil d'État, 1972, p. 2.
[81] CE, sect., 16 juillet 2014, n°355201, cons. 3.
[82] PACTEAU (B.), « Preuve », *Répertoire du contentieux administratif*, Janvier 2016, § 24.

Dans le cadre des activités des services de renseignement, les résultats des opérations de captation peuvent servir, sous forme de notes, de motivation à l'adoption de mesures administratives, telles que celles de prévention du terrorisme et des phénomènes de radicalisation[83]. En cas de contestation de la légalité d'une de ces mesures, les notes peuvent alors être produites en tant que preuves devant le juge administratif qui aura accès à leur contenu. Une recevabilité en contentieux validée par le Conseil d'État, sous réserve que celles-ci aient été versées au débat contradictoire et qu'elles n'aient pas été sérieusement contestées par le requérant[84].

Pour permettre au juge de contrôler la légalité de la mesure sans porter atteinte à la sécurité des sources de l'administration, les notes sont cependant blanchies. Sont effacées toutes les indications de nature à révéler le rédacteur de la note, ainsi que toute mention des techniques utilisées pour obtenir le renseignement.

Puisque de manière plus large, les notes des services de renseignement, peuvent servir à motiver des mesures autres que celles de prévention du terrorisme, par exemple, les mesures de suspension d'un fonctionnaire[85], de refus de renouvellement d'autorisations d'accéder aux centrales nucléaires[86], de sanctions disciplinaires[87], de retrait d'agrément[88], leur version blanchie est cruciale pour que les juges, ne bénéficiant pas d'habilitation au secret de la défense nationale, aient en leur possession tout élément pertinent relatif au contenu.

Par ailleurs, le Conseil d'État dispose, depuis la loi relative au renseignement du 24 juillet 2015, d'une formation spécialisée habilitée au secret de la défense nationale, compétente pour accéder à tous les éléments nécessaires à son office juridictionnel. Elle n'a pas de restriction en matière de notes des services de renseignement, pour connaitre par exemple la technique employée ou l'agent responsable. Elle peut être saisie dans le cadre d'une question préjudicielle pour apprécier la régularité des techniques de renseignement ayant permis de rédiger la note blanche.

La présence de cette formation a été jugée par la Cour européenne comme faisant partie « *des garanties compensatoires essentielles face aux restrictions apportées aux*

[83] COMBRADE (B.-L.), « Les notes blanches des services de renseignement », *RFDA*, p. 1103.
[84] CE, sect., 11 décembre 2015, n°39989, cons.19.
[85] TA Melun, 16 mai 2017, n°1703246.
[86] CAA Nancy, 15 janvier 2015, n°14NC01754.
[87] DIARD (E.), POUILLAT (E.), *Rapport d'information (nº 2082) de la commission des lois, sur les services publics face à la radicalisation, présenté à l'Assemblée nationale*, 27 juin 2019, p. 58.
[88] TA Bastia, 7 septembre 2017, n°1700254.

principes du contradictoire et de l'égalité des armes, inhérentes à un système de surveillance secrète »[89].

Malgré cela, l'utilisation de notes blanches dans le cadre contexte de la captation de données informatiques soulève quelques problèmes.

D'une part, il n'est pas impossible que certaines de ces notes soient constituées d'informations sur l'entourage de la personne initialement visée l'opération de captation, récoltées de manière incidente. En effet, les opérations de captation permettent d'obtenir un nombre conséquent de données, incluant le contenu de communications électroniques en clair entre la personne visée et son entourage. Or, la technique de captation ne dispose pas de règles procédurales pour étendre sa mise en œuvre à l'entourage, contrairement aux interceptions de sécurité, par exemple[90]. L'utilisation d'informations récoltées de manière incidente donnerait à la technique de captation un périmètre plus élargi que celui pour lequel la demande a été effectuée de prime abord.

Il n'est pas assuré que la formation spécialisée du Conseil d'État puisse invalider une mesure fondée sur une note contenant des informations de cette nature.

D'autre part, ni le juge administratif ni la formation spécialisée ne disposent explicitement d'une compétence pour examiner l'intégrité et la fiabilité des données qui, captées, servent de base à la note.

Par ailleurs, le juge pénal peut être amené à prendre en considération ces notes blanches, dans trois cas précis.

Le premier cas est celui où il aurait fait usage, par l'article 111-5 du code pénal, de sa compétence « *pour interpréter les actes administratifs, réglementaires ou individuels et pour en apprécier la légalité, lorsque, de cet examen, dépend la solution du procès pénal qui lui est soumis* ». Il s'agit d'un mécanisme de « *sollicitation préjudicielle* », par lequel le juge demande la note blanche susceptible d'être à l'origine de la mesure

[89] CEDH, 10 décembre 2024, *Association confraternelle de la presse judiciaire et autres c. France*, n[os] 49526/15 et 13 autres, §117.

[90] Les interceptions de sécurité sont une autre technique spéciale de renseignement. L'article L852-1 autorise, « *lorsqu'il existe des raisons sérieuses de croire qu'une ou plusieurs personnes appartenant à l'entourage d'une personne concernée par l'autorisation d'interception sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée pour ces personnes* ».

administrative contestée par son destinataire, soupçonné d'avoir commis une infraction pour non-respect de celle-ci[91].

Le deuxième cas relève des notes blanches adressées aux juges judiciaires en application de l'article 40 du CPP qui impose aux agents publics l'obligation de notifier le procureur de la République, de tous soupçons d'infraction issus de leur activité[92]. Ce peut être le cas d'une opération de captation de données informatiques qui aurait permis de constater que la personne visée ou qu'un de ses proches, commettrait, aurait commis ou projetterait de commettre une infraction.

Ici, la force probatoire de ces notes est minimisée, elles ne constituent que de simples renseignements[93].

Enfin, le dernier cas concerne les autorisations de visite d'un lieu et de saisie des documents et des données qui s'y trouvent, aux fins de prévenir la commission d'actes de terrorisme. Cette procédure, inscrite à l'article L. 229-1 du CSI, est autorisée par le juge des libertés et de la détention du tribunal judiciaire de Paris, après avis du procureur de la République antiterrorisme, sur saisine motivée du représentant de l'État dans le département ou à Paris, du préfet de police.

Dans ce cadre, le juge des libertés et de la détention peut être amené à avoir connaissance des notes blanches ayant motivé la saisine, afin d'expliquer pourquoi la personne visée par la demande constitue « *une menace d'une particulière gravité pour la sécurité et l'ordre public* ». Cette compétence vise à minimiser les risques d'abus et d'arbitraire de la part des autorités administratives. En cas de recours, la note est soumise au débat contradictoire et le juge peut inviter l'administration, en cas de contestation sérieuse, à produire tout élément utile[94].

En pratique cependant, tant la sollicitation de l'administration à produire des éléments supplémentaires que le versement au débat contradictoire de la note blanche se heurtent au secret de la défense nationale. Le juge judiciaire n'ayant pas les habilitations nécessaires pour accéder aux informations classées, sa capacité à statuer en pleine connaissance de cause peut être légitimement remise en question[95].

---

[91] COMBRADE (B.-L.), « Les notes blanches des services de renseignement », *RFDA*, p. 1103.

[92] Art. 40, code de procédure pénale.

[93] COMBRADE (B.-L.), « Les notes blanches des services de renseignement », *RFDA*, p. 1103.

[94] C. cass., ch. crim., 5 décembre 2023, n°22-80.611.

[95] SIZAIRE (V.), « Blanc-seing pour les notes blanches », *La Revue des droits de l'homme*, *Actualités Droits-Libertés*, 26 février 2024, URL :

1.3.2 Les principes structurants de licéité et de loyauté

Lorsque la procédure est respectée, les preuves résultant d'une opération de captation de données informatiques par les services de renseignement s'inscrivent dans un cadre légal, ce qui leur confère le qualificatif de « *preuves licites* ». Le caractère déloyal de leur captation étant intrinsèque au succès des opérations de surveillance secrète, seule l'irrégularité demeure un motif capable d'écarter certaines preuves du dossier.

Outre les preuves résultant de cette captation, il faut distinguer deux cas d'usage en matière de contentieux administratif pour lesquels l'application du principe de licéité et de loyauté est différente.

Le premier est celui où la procédure impose à l'administré la production d'éléments de preuve. Dans ce cas, l'utilisation d'éléments confidentiels comme moyen de preuve n'est pas de nature à entacher d'irrégularité la procédure[96]. Il en va de même pour des éléments produits qui auraient été soustraits à leur auteur. Les principes de loyauté et de licéité des preuves ne s'appliquent pas, à l'instar de la matière pénale, aux particuliers. Cette circonstance se justifie par le déséquilibre naturel entre l'administration et l'administré, une telle liberté dans les moyens de preuve ayant ainsi un lien direct avec les droits et garanties de l'individu face à la puissance publique[97].

De fait, les preuves obtenues par l'exploitation de vulnérabilités pourraient être recevables.

Ensuite, le cas où la charge de la preuve revient à l'administration. En théorie, il n'existe pas de principe de loyauté strictement applicable à l'administration. La seule restriction qui a été apportée à la production de preuves pour des motifs de loyauté est en matière de sanction disciplinaire.

En vertu de l'obligation de loyauté de l'employeur public vis-à-vis de ses agents, il ne saurait fonder une sanction disciplinaire sur une pièce obtenue en méconnaissance de cette obligation « *sauf si un intérêt public majeur le justifie* » [98]. Il ne s'agit toutefois pas du principe de loyauté dans sa forme existante en droit civil ou pénal. Pour rappel, en

https://www.google.com/search?client=safari&rls=en&q=Sizaire+(V.)%2C+«+Blanc-seing+pour+les+notes+blanches+»%2C+La+Revue+des+droits+de+l'homme%2C+Actualités+Droits-Libertés%2C+26+février+2024&ie=UTF-8&oe=UTF-8, consulté le 01 juillet 2025.

[96] TA Cergy-Pontoise, 4 octobre 2018, n°160771.

[97] PACTEAU (B.), « Preuve », *Répertoire du contentieux administratif*, Janvier 2016, § 5 et 0

[98] CE, sect., 16 juillet 2014, *Ganem*, n°355201.

l'absence de dispositions législatives contraires, l'autorité investie du pouvoir disciplinaire peut apporter la preuve par tout moyen devant le juge administratif des faits qui permettraient d'attester la légalité d'une sanction infligée.

Par exemple, le Conseil d'État a validé l'interprétation d'une cour administrative d'appel, qui, dans un arrêt de 2014, a jugé que ne traduisait pas un manquement à l'obligation de loyauté, le recours par une commune aux services d'une agence de détectives privés pour réaliser « *des investigations dans le but de mettre en évidence les activités professionnelles d'un couple et d'en administrer les preuves par des surveillances* » [99]. Puisque ni le recours à une agence privée ni la surveillance de son employé ne peuvent être assimilés à un manquement, la surveillance d'un agent par l'exploitation de vulnérabilités afin d'établir des preuves pour fonder une sanction disciplinaire semble être autorisée. Toutefois, il faudra attendre une jurisprudence précise sur ce cas pour s'en assurer.

Eu égard à ce qui précède, les principes de licéité et de loyauté de la preuve en contentieux administratif n'ont qu'une incidence légère, dont les contours de leurs répercussions en ce qui concerne les preuves numériques résultant d'une telle exploitation, sont encore relativement ambigus.

[99] *Ibid.*

Conclusion

Les conditions générales de recevabilité autorisent, pour la plupart, l'utilisation de preuves obtenues par l'exploitation. Même les plus strictes, situées au niveau de la licéité et de la loyauté de la preuve en matière civile, tendent à s'assouplir pour pallier les disruptions créées par les nouvelles technologies de communications. Il existe bien des règles de recevabilité supplémentaires, cependant, elles visent un type précis de preuve (telles que les signatures électroniques) et n'ont pas de portée générale.

La réalité est telle que les procédures ne peuvent désormais plus se passer de ce type de preuves. L'utilisation toujours plus croissante des technologies de l'information et de la communication a rendu inéluctable leur impact en contentieux, indépendamment de la matière.

Pour autant que cela soit indéniable, la preuve numérique est aussi fragile, quelque peu douteuse, que ce soit par sa nature qui la rend volatile, ou parce que les parties, magistrats et avocats, n'ont parfois pas l'expertise requise pour la comprendre dans son entièreté. Ainsi, la donnée à partir de laquelle se base la preuve, doit revêtir un certain nombre de conditions matérielles pour être jugée qualitative, intègre, et donc, fiable.

Figure 1. Tableau récapitulatif des conditions de recevabilités des preuves obtenues par le biais de l'exploitation de vulnérabilités informatiques

2. Les conditions spécifiques à la preuve numérique

Les données, bien qu'incontestablement riches quantitativement en raison du volume, et qualitativement en raison de la précision des informations qu'elles contiennent, sont vulnérables. Elles dépendent de leurs environnement, matériel ou logiciel, sont effaçables et non statiques[100]. Cette vulnérabilité a pour conséquence d'amenuir la confiance qu'ont les parties au procès en la fiabilité des preuves numériques produites, ce qui donne lieu à des contestations.

Pour pallier cette vulnérabilité, mais également pour niveler la qualité des preuves produites, de bonnes conditions de validité s'imposent à la donnée pour qu'elle puisse être qualifiée de preuve numérique, fiable.

Dégagées par la pratique des experts judiciaires, ces conditions se matérialisent en quatre critères de qualification : l'authenticité, l'intégrité, la traçabilité, et la conservation. Une réponse nécessaire aux problématiques liées à la fiabilité de la preuve numérique, déjà soulevées par le Conseil de l'Europe en 1995[101] qui jugeait que « *l'intérêt commun de recueillir, de sauvegarder et de présenter des preuves électroniques de manière à garantir au mieux leur caractère irréfutable et leur intégrité* devrait être reconnu *(...). À cette fin, des procédures et méthodes techniques du traitement des preuves électroniques devraient être développées*[102] *(...)* »[103].

Au-delà de la stricte définition de ces critères de qualification, l'étude des méthodes techniques sous-jacentes utilisées en pratique est ainsi également importante (**2.1**), de même que la place des experts judiciaires (**2.2**). Il conviendra aussi de définir les modalités de contestation des preuves produites (**2.3**).

---

[100] MIGAYRON (S.), « Critères d'appréciation technique, vraies et fausses preuves numériques », préc.

[101] Recommandation n°R(95)13 du Comité des ministres aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information, adoptée par le Comité des Ministres le 11 septembre 1995, lors de la 543e réunion des Délégués des Ministres.

[102] Nous soulignons.

[103] *Ibid.,* point IV, rec. 13.

2.1 Les critères de qualification nécessaires à de bonnes conditions d'interprétation

Chaque critère a une fonction bien précise. Palliatif à la nature volatile des preuves numériques[104], ils participent à assurer les droits de la défense en donnant une base concrète pour contester une preuve produite.

Le critère de l'authenticité vise à garantir l'origine de l'information[105]. Il s'agit donc du critère le plus important, puisqu'il permet de déterminer l'opposabilité d'une preuve à un individu, l'imputabilité de faits incriminants ou disculpants. L'origine de l'information, et donc nécessairement l'identification des parties impliquées, peut être déterminée par deux moyens. Par le biais d'un mécanisme de gestion des identités s'il existe, lorsque les données sont extraites depuis un support ou par le biais d'un faisceau d'indices. Ce peut être l'adresse postale, l'adresse mail ou IP, la messagerie électronique, les données de recherches sur internet, l'historique d'appel et leur durée, les fichiers bureautiques, les avatars de monde virtuel, pour citer quelques exemples[106].

Les méthodes pour garantir l'authenticité de la preuve peuvent se heurter aux techniques d'anonymisation, qui rendent difficile la tâche d'identification de la personne auteur ou destinataire[107].

De plus, il faut rappeler que selon le type de données récoltées, les propriétés du fichier peuvent aisément être modifiées, de manière accidentelle ou intentionnelle. La simple consultation d'un fichier Windows modifiant directement ses métadonnées.

Le critère de l'intégrité vise à garantir la véracité du contenu de l'information, afin que les faits rapportés par la preuve produite puissent être incontestablement établis. Cela suppose que la donnée fondant la preuve n'ait pas été altérée.

---

[104] Association Internationale de Droit pénal, « *Société de l'information et Droit Pénal* », organisé au XIXe Congrès international de Droit Pénal, Brésil, 31 août – 6 septembre 2014, Section III « Procédure pénale », résolution 18.

[105] MIGAYRON (S.), « Critères d'appréciation technique, vraies et fausses preuves numériques », préc., spéc., p. 22.

[106] KAI (M. F.), *La preuve numérique à l'épreuve de la cybercriminalité*, Mémoire de stage de Master 2 Droit pénal international et européen de l'Université de Limoges, 2020/2021, spéc. p. 22.

[107] ITEANU (O.), « L'avocat ensemblier de preuves numériques », in *La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique, op. cit.*, p. 43.

En pratique, il est fait recours à des outils pour certifier qu'aucune modification n'a été conduite sur les données stockées. À titre d'information, la disponibilité de ces outils et leur usage régulier font partie des recommandations formulées en 2014 par l'association internationale de Droit pénal[108].

En termes de procédés, la technique de hachage (dite de « *calcul d'empreinte numérique* ») est la méthode privilégiée pour la certification. Elle permet d'attribuer à un fichier, grâce à un algorithme, une série de caractères uniques. Chaque changement opéré sur le fichier génèrera une nouvelle série de caractères uniques.

Il existe différents algorithmes plus ou moins sensibles aux modifications, certains nécessiteront un degré plus élevé de changements effectués sur un fichier donné avant générer une nouvelle série de caractères uniques. Par exemple, l'algorithme *Message Digest 5* ou *MD5*, particulièrement hypersensible aux modifications, génèrera une empreinte totalement différente lorsque le point final du fichier de 7 millions de caractères représentant un volume de l'Encyclopaedia Universalis est remplacé par un espace [109].

A contrario, l'algorithme utilisé par la méthode du contrôle de redondance cyclique, ou *cyclic redundancy check,* plus communément connu sous le nom de CRC32, n'a pas été jugé comme apte à garantir l'intégrité des données. Par exemple, dans l'affaire *Zacarias v. États-Unis* à propos des attentats du 11 septembre 2001, les éléments obtenus par les autorités publiques étatsuniennes ont fait l'objet de contestation de la part de la défense, parce que la copie des ordinateurs portables des prévenus avait été effectuée avec l'algorithme CRC32. La totalité des opérations de copies ont été refaites avec l'algorithme MD5, davantage fiable[110].

Cela ne signifie pour autant pas que l'algorithme MD5 soit sans failles. Il a pu être décelé que les objets dynamiques qui utilisent la mémoire flash pouvaient avoir une incidence sur l'empreinte numérique initiale. Puisque la mémoire technologique flash fonctionne sur la base de microprogrammes chargés de déplacer automatiquement les informations stockées lorsqu'un certain niveau d'usure est atteint, l'empreinte numérique de l'algorithme MD5 pourrait être différente selon le moment où l'analyse est effectuée.

---

[108] Association Internationale de Droit pénal, « *Société de l'information et Droit Pénal* », 31 août – 6 septembre 2014, *op. cit.,* Section III « Procédure pénale », résolution 18.

[109] Avant la modification : *A64C0C668E613B5D10B936F6BD2ED75D* ; Après la modification : *A616D59F9FC2E2671BB84F3621E41595*.

[110] ITEANU (O.), « L'avocat ensemblier de preuves numériques », préc., spéc., p. 47.

Ce type de mémoire est aujourd'hui présente dans les terminaux numériques mobiles, tels que les *smarthphones,* les tablettes, mais aussi certaines clés USB[111].

De plus, l'algorithme peut être victime d'attaques malveillantes ou contenir des failles.

Le critère de la traçabilité est essentiel pour répertorier les différentes opérations ou procédés techniques qui auraient été effectués depuis la collecte jusqu'à la conservation des données obtenues[112], ou du moins, jusqu'à leur gel ou leur préservation dans un état stable[113].

Il peut s'agir à la fois des traces préexistantes au moment de la saisie, et celles résultant du travail de l'expert lors de la captation, du déchiffrement, de l'accès ou de la copie des données.

Ainsi, au moins pour celles résultant du travail de l'expert, ces mêmes traces devraient répondre à un cadre strict pour assurer leur fiabilité non équivoque. Par exemple, elles devraient être identifiables individuellement à l'aide d'un numéro, afin de garantir qu'aucune trace n'a été ajoutée ou supprimée dans un ensemble. Des mécanismes de certification devraient être mis en place pour prouver que celles-ci n'ont pas fait l'objet de modifications, et, de fait, qu'elles sont intègres[114]. En pratique cela nécessite la mise en place d'une politique de gestion des privilèges et des accès à ces traces. Il n'existe cependant pas de recommandations officielles quant aux éléments de formes et de contenus impératifs pour la conformité de cette politique aux exigences ci-dessus.

La mise en place de telles règles renforce la crédibilité du travail de l'expert, d'éviter les remises en question fréquentes de la fiabilité des preuves et des traces associées. En outre, ces règles solidifient le principe du contradictoire, puisqu'elles rendent accessible à chaque partie l'étendu du travail de l'expert.

Enfin, **le critère de la conservation** des preuves obtenues est intrinsèquement lié à la question des supports utilisés. Par exemple, il a été mis en évidence le caractère faillible des CD-R ou des DVD-R[115] en tant que support de données, eu égard à leur sensibilité

---

[111] *Ibid.,* p. 24.

[112] Kai (M. F.), « La preuve numérique à l'épreuve de la cybercriminalité », *op. cit., spéc.,* p. 21.

[113] LUCQUIN (J.-P.), « Exemples de difficultés rencontrées par le Juge chargé du Contrôle des Expertises », in *La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique, op. cit.,* p. 60.

[114] *Ibid.*

[115] Le CD-ROM, de l'anglais *Compact disc – read-only memory,* est un disque optique utilisé pour stocker des données numériques destinées à être lues par un lecteur compatible, comme celui d'un

aux facteurs environnementaux susceptibles d'entrainer leur dégradation[116]. La pérennité des informations stockées est alors dépendante à la fois de la stabilité physique du support, mais aussi chimique dans le cas des CD-R et DVD-R. L'exposition à la chaleur, à l'humidité, aux agents polluants, mais aussi aux rayures, ou contraintes mécaniques influencent la disponibilité des preuves obtenues.

Le critère de la conservation est alors particulièrement important à l'égard des autres critères étudiés, puisque son respect assure la pérennité de la preuve numérique dans le temps. Une importance soulignée dans les lignes directrices du Conseil de l'Europe en matière de preuves électroniques dans les procédures civiles et administratives[117], « *les preuves électroniques devraient être stockées de manière à en préserver la lisibilité, l'accessibilité, l'intégrité, l'authenticité, la fiabilité (…). Elles devraient être stockées accompagnées de métadonnées normalisées, de manière à préciser clairement le contexte de leur production. La lisibilité et l'accessibilité des preuves électroniques devraient être garanties dans le temps, en tenant compte de l'évolution des technologies de l'information*[118] ». Cette dernière mention fait directement écho au choix des supports de conservation, certains moins stables que d'autres.

Lorsque ces quatre critères de qualification sont présents, la preuve numérique peut être interprétée en procédure, civile ou pénale, en conditions valides. Et, si l'absence d'un ou plusieurs critères ne rend pas irrecevable la preuve produite, elle portera atteinte à sa valeur probante. Susceptible d'être alors plus aisément contestable par les parties, la preuve numérique bénéficie grandement d'un cadre méthodique garantissant sa fiabilité.

2.2 Le rôle des experts de justice en informatique et techniques associées

Les experts requis dans le cadre de procédures peuvent exercer, une fois la donnée obtenue, plusieurs types de missions.

---

ordinateur. Par rapport au DVD-ROM, *Digital Versatile Disc – read-only memory,* qui fonctionne de manière similaire, le CD-ROM dispose d'un espace de stockage plus limité.

[116] LAMBERT (J.-M.), SAUNDERS (Y.), « La conservation des données sur CD-R », Laboratoire National d'Essais – Synthèse étude LNE 021/2000, p. 2.

[117] Lignes directrices CM(2018)169 du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives, adoptées par le Comité des Ministres le 30 janvier 2019 lors de la 1335 réunion des Délégués des Ministres.

[118] *Ibid.,* point 25 à 27.

D'une part, ils sont chargés du respect des critères ci-dessus étayés, par la mise en œuvre de procédés techniques. L'expert doit se constituer un dossier solide, étayer sa théorie par de la bibliographie, de la méthode ainsi que de la logimétrie. Chaque action doit être le résultat d'un procédé, ce dernier devant être explicable et expliqué à tout instant. L'objectif poursuivi est la reproductibilité des résultats, ainsi que la transparence. Par exemple la technique utilisée pour le déchiffrage de données, apportées par les services de police judiciaire dans le cadre de la mise au clair de données chiffrées, doit être compréhensible par les parties et devrait conduire systématiquement aux mêmes résultats.

D'autre part, ils jouent un rôle interprétatif, lorsque l'interprétation des données pertinentes mène à plusieurs hypothèses plausibles. Ils sont compétents pour analyser les questions complexes soulevées en matière de preuve ou en cas d'allégation de manipulation des preuves électroniques[119]. Le haut degré de technicité nécessaire pour effectuer ces deux missions accorde à l'expert un rôle crucial, indissociable de la procédure judiciaire. Il se positionne comme un intermédiaire entre les magistrats et les parties.

Toutefois, l'expert ne peut se substituer au rôle de l'avocat ou du juge, l'un chargé de transformer la donnée en preuve, et l'autre d'en apprécier la valeur probante. En effet, les experts « *apportent des éléments qui doivent être solides, mais pas des preuves* »[120].

Par exemple, dans le cas d'allégations d'intrusion frauduleuse dans un STAD, l'expert analyse les traces présentes sur celui-ci, en tirer des conclusions sur les évènements probables qui ont conduit à la présence de telles traces. Il aura pour compétence d'isoler les éléments pertinents dans le cadre d'un futur contentieux. Par la suite, les avocats, les magistrats ainsi que les parties devront prendre en considération ces éléments, ainsi que les conclusions de l'expert, avec l'ensemble des autres preuves et éléments produits, qui ne relèvent pas nécessairement de l'informatique.

Dans le cadre de ses missions, l'expert doit également respecter les principes du contradictoire. Chaque élément doit avoir été communiqué à toutes les parties. Pour aller plus loin, et dans une mise en œuvre extensive du principe du contradictoire, il a même

[119] Lignes directrices CM(2018)169 du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives, adoptées par le Comité des Ministres le 30 janvier 2019 lors de la 1335 réunion des Délégués des Ministres, point 18.

[120] BILLARD (D.), « L'expert et les bonnes pratiques techniques », in *La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique* », *op. cit.,* p. 47.

été signé une Convention[121] entre la Cour d'appel de Paris, l'ordre des avocats de cette dernière, d'autres ordres d'avocat et l'union des compagnies d'experts de la Cour d'appel de Paris, pour qui soit remis aux parties une synthèse explicative des résultats obtenus, avant que celles-ci n'émettent leurs observations.

Actuellement, la **C**ompagnie **N**ationale des **E**xperts de **J**ustice en **I**nformatique et **T**echniques **A**ssociées (**CNEJITA**), association loi 1901 créée en juin 1992, regroupe les experts en informatiques qui sont inscrits sur les listes d'experts judiciaires, des Cours d'Appel, de la Cour de cassation ou d'une juridiction administrative.

L'objectif de cette association est de diffuser la connaissance entre les experts informaticiens, à la fois techniques (comme les failles de sécurité ou des virus), mais aussi sur la procédure et les évolutions juridiques. Elle promeut également une mise en commun des moyens utilisés dans le cadre d'expertise en raison de la flambée des coûts des outils d'investigation[122].

L'association facilite les échanges entre les experts et les magistrats ou les avocats spécialisés, en organisant des sessions d'échanges et de vulgarisation bilatérales. Une étroite collaboration rendue cruciale du fait de l'externalisation des processus de récupération et de certification de la donnée numérique pour la transformer en preuve exploitable. Ceci implique une relation de confiance entre les deux professions, puisque le magistrat ne dispose en théorie pas du bagage académique et de l'expérience requise pour avoir le même point de vue que l'expert sur les moyens mis en œuvre, les procédés utilisés et inversement.

À cet égard, la contestabilité de l'expertise et des preuves numériques obtenues, est un pan crucial des procédures civiles, judiciaires et administratives.

2.3 Les modalités de contestation de la preuve numérique

Faculté impérative en contentieux indépendamment de la matière, la possibilité de contester ce type de preuve numérique peut être rendue complexe pour des raisons qu'il faut explorer. Les contestations se situent principalement sur deux aspects, soit au niveau

[121] Convention entre la Cour d'appel de Paris, l'ordre des avocats de la Cour d'appel de Paris, les ordres des avocats des barreaux de Bobigny, Créteil, Évry, Meaux, Melun, Auxerre, Fontainebleau, Sens, et l'Union des compagnies d'experts de la Cour d'appel de Paris, concernant l'étape conclusive du rapport d'expertise en matière de procédure civil, 8 juin 2009.
[122] Site de la CNEJITA, consulté le 11 juin 2025.

de la procédure à l'origine de leur collecte, soit au niveau de l'authenticité des données collectées, et donc, leur fiabilité. Celles-ci devront être analysées conjointement aux aspects strictement procéduraux, en civil (**2.3.1**), pénal (**2.3.2**) et administratif (**2.3.3**).

2.3.1 La contestation en procédure civile

La contestation en procédure civile se fait généralement sur le plan de l'authenticité de la preuve produite. En effet, les pièces issues de communication électronique font partie des preuves couramment produites pour attester d'une notification, d'une rupture de contrat ou des modalités convenues par celui-ci, par exemple. La Cour de cassation a eu l'occasion de rappeler à ce sujet que « *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* »[123].

Une posture reprise par les lignes directrices du Conseil de l'Europe sur les preuves électroniques en procédure civile et administrative, même si celles-ci vont plus loin. Elles disposent notamment que « *les données électroniques devraient bénéficier d'une présomption de fiabilité, sous réserve que l'identité du signataire puisse être validée et que l'intégrité des données puisse être assurée, à moins qu'il n'existe des motifs raisonnables de penser le contraire* »[124].

Il n'existe pas à ce jour de texte de loi, de jurisprudences spécifiques à la contestation des preuves obtenues par l'exploitation de vulnérabilité. Leur caractère intrinsèquement illicite et déloyal les a rendues absentes des procédures civiles, les revirements de jurisprudence de 2007[125] et de 2023[126] ayant seulement autorisé leur production en théorie et de manière strictement conditionnée.

Il est possible de supposer que la contestation de ce type de preuve réponde au même cadre que celui concernant les preuves numériques au sens large, bien que certaines présomptions pourraient ne pas s'appliquer. Par exemple, le cas des preuves qui auraient été produites de manière non sécurisée, puisque la Cour de cassation considère qu'« *un*

[123] C. cass., ch. com., 4 octobre 2005, n°04-15.195.
[124] Lignes directrices CM(2018)169 du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives, adoptées par le Comité des Ministres le 30 janvier 2019 lors de la 1335 réunion des Délégués des Ministres, point 22.
[125] C. cass., ch. com., 15 mai 2007, pourvoi n° 06-10.606.
[126] C. cass., Ass., 22 décembre 2023, n°20-20.648.

écrit électronique non sécurisé constitue une preuve dès lors que la preuve est libre et que la sincérité du détenteur de l'écrit ne peut être suspectée »[127].

Le détenteur de ce type de preuve ayant agi en infraction des articles du code pénal, la présomption de sa sincérité pourrait être remise en question, ou plus aisément contestable.

Par ailleurs, lorsqu'il n'est pas question de signature électronique, la contestation d'une preuve numérique ne semble pas imposer aux juges de vérifier son bien-fondé. En effet, les critères relatifs à l'identité de l'auteur de l'écrit et de sa conservation dans de conditions de nature à en garantir l'intégrité ne valent pas, par exemple, au courrier électronique. Dans un arrêt du 27 novembre 2014[128], la Cour de cassation a notamment estimé que ce courrier avait été produit pour « *faire la preuve d'un fait, dont l'existence peut être établie par tous moyens de preuve, lesquels sont appréciés souverainement par les juges du fond* ». Or, il n'est pas improbable que des preuves soient falsifiées dans le but de servir un intérêt privé, ou que l'individu ait été la cible d'une cyberattaque malveillante.

Dans ce contexte, la prise en compte des preuves originaires d'une intrusion frauduleuse sur un système de traitement de données renforce davantage l'instabilité de la fiabilité d'une bonne administration de la justice en matière civile. Il est possible de supposer à nouveau que les conditions permettant l'utilisation de preuves illicites et déloyales répondent à cette circonstance-ci.

2.3.2 La contestation en procédure pénale

En ce qui concerne la matière pénale, deux cas de figure se distinguent. La contestation horizontale des preuves obtenues par l'exploitation de vulnérabilités informatiques, c'est-à-dire entre particuliers, concernera la fiabilité des preuves, leur véracité. La contestation verticale ascendante, elle, s'insère dans le rapport entre autorités publiques, comme les services de police judiciaire, et les personnes visées par leurs missions. Une contestation qui peut se fonder sur un vice de procédure, une irrégularité dans la conduite des opérations, rendant les preuves obtenues déloyales, ou sur la fiabilité des preuves produites.

[127] C. cass., ch. com., 4 octobre 2005, n°04-15.195.
[128] C. cass., 2ème civ., 27 novembre 2014, n°13-27.797.

Sur la régularité des opérations et les rapports verticaux, l'arrêt de la chambre criminelle de la Cour de cassation du 25 octobre 2022[129] peut apporter un éclairage sur les contours d'une procédure adéquate de contestation de preuves numériques, notamment celles recueillies par le biais d'une opération de captation de données informatiques.

La portion de l'arrêt intéressante concerne le rejet d'une demande d'annulation des opérations de captation, pour défaut de qualité à agir. La demande se basait que le recours à un procédé déloyal. Pour rappel, dans cette affaire, étaient en cause 13 personnes pour des chefs d'infractions à la législation sur les armes, d'importation de stupéfiants en bande organisée, de trafic de stupéfiants et d'associations de malfaiteurs. Lors de l'enquête préliminaire, un dispositif de captation de données informatiques sur le serveur alimentant un réseau de téléphones cryptés avait été mis en œuvre, en application de l'article 706-102-1 du CPP. Un usage contesté pour manque de loyauté, en raison d'un détournement des règles de procédure. La raison de cette allégation a fait l'objet d'un développement à la section 1.2.2.

En effet, selon les termes de l'article 802 du CPP, pour contester une telle opération l'individu devait avoir qualité à agir, puisque « *toute juridiction saisie d'une demande d'annulation ou qui relève d'office une irrégularité, ne peut prononcer la nullité que lorsque (la violation) a eu pour effet de porter atteinte aux intérêts de la partie qu'elle concerne* »[130]. Cette procédure impose implicitement à la partie de justifier que l'acte critiqué porte atteinte à un droit ou à un intérêt qui lui est propre, ce qui a pour conséquence de la « *contraindre, sous peine d'être privé de son droit d'agir en nullité, à renoncer à exercer son droit au silence ou à revenir sur ses déclarations antérieures. Cela peut aussi l'obliger, notamment lorsqu'est en cause un acte attentatoire à la vie privée, à admettre l'existence d'éléments à charge, voire à reconnaître les faits qui lui sont reprochés* »[131].

Les juges du fond avaient jugé dépourvu de qualité à agir les individus visés par les opérations de captation, au motif qu'à l'exception d'un seul, aucun de ceux-ci n'avait admis être utilisateurs ou interlocuteurs des téléphonés cryptés litigieux.

Ainsi, subordonner la recevabilité de l'action en nullité par un individu à la preuve que celui-ci est concerné revenait à « *méconnaître son droit à ne pas s'auto-incriminer* »[132], droit protégé par l'article 6, §1 de la Convention européenne des droits de l'homme.

[129] C. cass., ch. crim., 25 octobre 2022, n°21-85.763.
[130] *Ibid.,* §53.
[131] *Ibid.,* §57 et 58.
[132] *Ibid.,* §60.

Cela faisait des modalités procédurales, un levier pour obtenir des aveux, puisque la contestation des éléments obtenus impliquait nécessairement que le demandeur ait reconnu que cesdits éléments le concernaient précisément.

Pour pallier ce problème, la Cour de cassation a estimé, lorsque le requérant n'allègue pas que la formalité méconnue a pour objet de préserver un droit ou un intérêt qui lui propre, qu'il appartenait à la chambre de l'instruction de rechercher s'il résulte des éléments de la procédure que tel pourrait être le cas. La charge de prouver l'intérêt propre repose ainsi sur les juridictions, conformément au principe de présomption d'innocence[133].

Cet arrêt est également intéressant vis-à-vis de la fiabilité des preuves obtenues. Leur contestation, qu'elles résultent de la captation de données informatiques, de l'accès au support de données, de la mise au clair de données chiffrées ou de l'intrusion frauduleuse sur un STAD, implique en théorie que le contestataire soit directement visé par cesdites preuves. À ce titre, il convient de rappeler que le droit de l'Union européenne impose aux services judiciaires, dans le cadre du traitement des données à caractère personnel en matière de police, d'aménager pour la personne concernée, la possibilité de rectifier les données collectées lorsqu'elles sont inexactes[134]. Le traitement de celles-ci est limité si l'exactitude contestée des données ne peut être déterminée[135].

Or, dans le cas où le contestataire aurait fait usage de son droit à garder le silence, ou aurait nié les allégations de propriété du support saisi ou du STAD visé par l'intrusion, par exemple, la contestation reviendrait également à s'auto-incriminer. Cette situation n'a cependant jamais fait l'objet d'un contentieux.

L'exercice de ces deux droits crée une friction, dont l'atténuation implique que le juge soit dans l'obligation de vérifier, soit la fiabilité de la preuve produite, soit la régularité de la procédure ayant permis son obtention, de manière systématique, sans requérir de justifications supplémentaires.

---

[133] *Ibid.,* §62

[134] Directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JOUE* L 119/89 du 4 mai 2016, article 16, paragraphe 2.

[135] *Ibid.,* paragraphe 3.

Bien que cela participerait à renforcer les droits de la défense, la conséquence pourrait être un allongement de la durée des procédures et des coûts additionnels s'il est requis une contre-expertise.

Ce coût peut être particulièrement élevé dans certains cas. Par exemple, si la preuve résulte de l'intrusion par un particulier dans un STAD, l'expert pourrait devoir recréer les conditions d'intrusion pour démontrer que celle-ci n'a pas pu être altérée par l'extraction post-intrusion[136].

La question des coûts est intrinsèquement liée à l'opération, en amont, de récolte de données informatiques. Plus cette opération est encadrée par une procédure qui permet une collecte sûre de données, aux fins de minimiser les risques d'altération, de destruction ou de perte, moins ces données auront des chances d'être contestables[137]. Le montant des coûts d'une potentielle contre-expertise sera minimisé par la présence de garanties appropriée, en amont.

Puisqu'il n'existe pas de telle procédure pour les particuliers, les contestations pourraient être accrues. C'est la raison pour laquelle, à l'instar des huissiers dans le cadre des constats sur internet[138], la collaboration avec une personne qualifiée serait bénéfique. Elle n'existe pas à ce jour entre particuliers.

2.3.3 La contestation en procédure administrative contentieuse

La matière administrative pose plusieurs difficultés à l'individu souhaitant contester la preuve numérique résultant des activités des services de renseignement, lesquels, pour rappel, utilisent généralement les notes blanches.

Elles peuvent être contestées par le requérant qui fournit des explications suffisamment claires et détaillées concernant une erreur de fait induite par la note blanche, ce qui

[136] *La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique*, colloque par la Compagnie nationale des experts de justice en informatique et techniques associées (CNEJITA), *op. cit.,* spéc. p. 77.

[137] Lignes directrices CM(2018)169 du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives, adoptées par le Comité des Ministres le 30 janvier 2019 lors de la 1335 réunion des Délégués des Ministres, point 11.

[138] Acte extrajudiciaire par lequel l'officier ministériel va « photographier » ce qui est visible sur son ordinateur, sur internet, et en faire une preuve incontestable. Acte soumis à des conditions procédurales (voir Cour d'appel de Paris, 27 février 2013, n°11-11785).

implique, en pratique, la production d'attestations concordantes et circonstanciées[139]. Le juge administratif a par la suite la charge d'examiner la valeur probante des faits relatés par la note blanche et ainsi, s'ils sont sérieusement contestés. Seules la présence de faits suffisamment précis et circonstanciés, et l'absence de contestations sérieuses entraînent la prise en considération de la note blanche[140].

Tout d'abord, il peut être plus difficile pour un individu de contester une note blanche, qu'un autre moyen de preuve. Une difficulté soulignée par la Commission nationale consultative des droits de l'homme (CNCDH), qui, à l'issue de plusieurs auditions, a observé que « *les magistrats de l'ordre administratif éprouvent les plus grandes difficultés à apprécier la valeur probante de tels documents, parfois imprécis, laconiques ou empreints de subjectivité et contenant parfois des erreurs factuelles. Quant aux avocats, ils disent avoir souvent le plus grand mal à apporter la preuve contraire (notamment du fait de la difficulté de réunir des éléments de preuve dans des délais très contraints ou de la difficulté de contester des informations non datées ou peu circonstanciées)* »[141].

En effet les données récoltées, sur la base desquelles la preuve et la note blanche sont produites, peuvent ne former qu'un amas d'informations difficilement interprétables pour les personnes non expertes. Or l'avocat, pour fournir les attestations circonstanciées et concordantes nécessaires, doit à la fois posséder un œil expert afin de déceler les points de protestes qualifiables de « *sérieuses contestations* », et agir rapidement afin de réunion des professionnels à même d'offrir une interprétation divergente dans un délai réduit.

La contestation de la fiabilité des données elles-mêmes, et non pas simplement de l'interprétation est encore plus ardue puisqu'elle vient interroger directement les quatre critères spécifiques aux preuves numériques (authenticité, intégrité, traçabilité et conservation). Pour cela, il est crucial d'avoir accès aux détails des différents procédés utilisés sur les données, de leur récolte jusqu'à leur conservation dans un état stable.

Ces détails sont susceptibles de donner des indications sur les personnes ayant été impliquées dans le processus, ce qui ferait perdre la qualité de « *blanche* » à la note, compromettant le secret des sources. La seule voie pour les contestataires est donc la question préjudicielle à la formation spécialisée du Conseil d'État, habilitée au secret de

[139] COMBRADE (B.-L.), « Les notes blanches des services de renseignement », *RFDA*, p. 1103.
[140] CE, 3 mars 2003, *ministre de l'Intérieur c. Rakhimov*, n°238662.
[141] CNCDH, « Avis sur le suivi de l'état d'urgence », Assemblée plénière, 18 février 2016, p. 9. Nous soulignons.

la défense nationale, qui pourra statuer sur la régularité de la technique de renseignement mise en œuvre. Il faut s'interroger sur la capacité de cette formation à examiner la fiabilité des données collectées, au-delà de la régularité (et donc du respect des règles de procédure) de la technique.

Cependant, la Cour européenne des droits de l'homme n'a pas jugé que les modalités de contestation des notes blanches étaient à même d'entraîner une violation des droits de la défense. Elle souligne notamment les pouvoirs du juge administratif pour rechercher l'exactitude des faits relatés, qu'ils aient été ou non sérieusement contestés, et les pouvoirs d'instruction dont il dispose pour ce faire[142]. L'utilisation par le requérant de sa capacité de contestation n'est pas un critère prépondérant dans l'appréciation de la Cour. La seule présence de cette possibilité est suffisante pour qu'elle conclue que « *la note blanche a été accompagnée de garanties procédurales suffisantes* »[143].

Pour autant que cela ne veuille pas dire que la charge de réfutation n'est pas lourde, la Cour européenne considère les pouvoirs du juge suffisants pour équilibrer ceci.

[142] CEDH, 19 février 2023, *Pagerie c. France*, n°24203/16, §207.
[143] *Ibid.,* §208 ; CEDH, 15 juin 2023, *Fanouni c. France*, n°31185/18, §61.

Conclusion

Il ressort de l'analyse des conditions spécifiques à la preuve numérique, et des modalités de sa contestation que la question de la présomption de validité de la preuve reste au centre des difficultés.

Tant en civil qu'en administratif, cette présomption n'est pas liée par la présence de données assurément fiables, conformément aux quatre critères énoncés ci-dessus. Elle impose aux parties un effort considérable pour démontrer le bien-fondé de leur contestation, sans qu'il ne soit garanti qu'une expertise ou qu'une contre-expertise sera mandatée.

En pénal, l'utilisation des notes blanches opacifie davantage la qualité des informations, des données ou des preuves transmises, puisque le juge pénal ne dispose pas de pouvoirs pour demander au rédacteur de la note, de plus amples explications. Or, les recommandations sont claires, « *l'accès de la défense aux données numériques devrait être assuré pour être capable de vérifier l'authenticité des preuves de manière à pouvoir présenter la preuve électronique devant le tribunal d'une façon effective et non indûment restreinte* »[144].

L'accès de la défense aux données garantirait l'effectivité de la preuve, puisque la présomption dont elle bénéficierait deviendrait plus aisément réfragable. Ainsi, le respect du principe du contradictoire semble être la condition déterminante pour assurer que le poids de cette présomption ne puisse engendrer la compromission de l'égalité des armes et de l'équité du procès.

Outre ce constat, force est de constater que le rôle de l'expert est désormais impératif, qu'il se doit *a priori* d'avoir une conduite exemplaire dans l'exercice de ces missions. Les évolutions rapides de la technologie, autant celles utilisées par les particuliers que celles utilisées par les cybercriminels, imposent à l'expert d'avoir une bonne gestion de la connaissance, en suivant des formations et en échangeant avec ses pairs notamment[145].

---

[144] Association Internationale de Droit pénal, « *Société de l'information et Droit Pénal* », 31 août – 6 septembre 2014, *op. cit.,* Section III « Procédure pénale », résolution 19.

[145] BILLARD (D.), « L'expert et les bonnes pratiques techniques », in *La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique* », *op. cit.,* spéc. p. 49.

Par ailleurs, plus l'investigation numérique se complexifiera, plus sa démarche se devra d'être rigoureuse.

Conclusion générale

À la vue de ce qui précède, deux conclusions peuvent être tirées.

Tout d'abord, la preuve numérique, même celle résultant de l'exploitation de vulnérabilités, est graduellement rendue difficile à écarter des procédures. La présomption de validité, le recours aux notes blanches, les exigences de contestation, les aménagements procéduraux en civil concernant les preuves illicites ou déloyales, tout cela démontre la haute confiance accordée à ce type de preuves.

Pourtant, à l'heure où l'IA générative s'est installée dans notre quotidien, la problématique des hypertrucages n'est pas sans interroger les suites d'une telle confiance. D'un côté, l'on pourrait craindre les falsifications de preuves, toujours plus crédibles et difficilement décelables. De l'autre, la méfiance grandissante des magistrats, qui rejetteraient les affaires aux moindres doutes sur la véracité de l'élément apporté.

Ensuite, s'il existe un certain consensus sur les critères permettant d'attester la validité des preuves numériques, avec des travaux tant nationaux[146] qu'internationaux à ce sujet[147], pour l'heure, l'Union européenne reste absente de ces débats. Elle se concentre plutôt sur le caractère transfrontalier de ces preuves, particulièrement celles résultant des communications électroniques, qu'il s'agisse de leur collecte ou de leur transfert[148].

Le travail de l'Union européenne permet en réalité de passer outre les problématiques liées à la fiabilité des données produites par les autorités nationales, puisque celles-ci proviendraient directement du fournisseur de service de communication, les risques

[146] V. entre autres, CNEJITA, « *La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique* », 13 avril 2010, *op. cit.*

[147] Voir notamment : Association Internationale de Droit pénal, « *Société de l'information et Droit Pénal* », 31 août – 6 septembre 2014, *op. cit.,* Section III « Procédure pénale » et les lignes directrices CM(2018)169 du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives, adoptées par le Comité des Ministres le 30 janvier 2019 lors de la 1335 réunion des Délégués des Ministres, *op. cit*.

[148] Voir notamment la directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissement et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre de procédures pénales, *JOUE* L 191/118 du 28 juillet 2023.

d'altération étant ainsi limités. Il en va de même pour le second protocole à la Convention de Budapest du Conseil de l'Europe[149], ces instruments prennent, dans une certaine mesure, le problème en amont. Ils ne règlent pour autant pas celui de la production de preuves numériques par les particuliers.

Pour terminer, malgré les adaptations effectives du système probatoire national aux preuves numériques, il serait opportun de codifier plus explicitement le régime de leur administration selon les différentes matières. Cette codification pourrait porter sur le processus de certification de la preuve numérique au sens large, sur la portée des présomptions de validités et sur les modalités de contestation spécifiques.

[149] Deuxième protocole additionnel à la Convention sur la cybercriminalité STCE n°224 du Conseil de l'Europe du 12 mai 2022 relatif au renforcement de la coopération et de la divulgation de preuves électroniques.

BIBLIOGRAPHIE

I. Manuels, ouvrages généraux et spécialisés

DEBBASCH (CH.), RICCI (J.-CL.), *Contentieux administratif,* Dalloz, coll. « Précis Dalloz », 5ème éd., 1984.

FRICERO (N.), *Procédure civile,* Gualino, coll. « Mémentos », 21ème éd., 2024.

FRISON-ROCHE (A.-M.), *Généralités sur le principe du contradictoire,* LGDJ, coll. « Anthologie du droit », 2014.

GARE (TH.), GINESTET (C.), *Droit pénal : Procédure pénale 2025,* Dalloz, coll. « HyperCours », 16ème éd., 2024.

GUYOMAR (M.), SEILLER (B.), *Contentieux administratif,* Dalloz, coll. « HyperCours », 5ème éd., 2019.

GUINCHARD (S.), DEBARD (TH.), « *Lexique des termes juridiques 2024-2025* », Dalloz, coll. « Lexique Dalloz », 32ème éd., 2024.

II. Thèses et mémoires

AUDIBERT (M), *Le recueil de la preuve numérique : Enjeux et perspectives en procédure pénale*, th., Paris 10, 2024.

KAI (M. F.), *La preuve numérique à l'épreuve de la cybercriminalité*, Mémoire de stage, Limoges, 2020/2021.

VERON (N.), *Protection des données personnelles et renseignement : Contribution à l'identification d'un régime juridique autonome*, th., Pau et Pays de l'Adour, 2021.

III. Contributions dans des ouvrages collectifs et des mémoires

La preuve numérique à l'épreuve du litige. Les acteurs face à la preuve numérique, colloque par la Compagnie nationale des experts de justice en informatique et techniques associées (CNEJITA), le 13 avril 2010, disponible en ligne

URL : https://www.lagbd.org/images/3/3a/Colloque_CNEJITA_13_Avril_2010.pdf, consulté le 01 juillet 2025.

Association Internationale de Droit pénal, *Société de l'information et Droit Pénal*, organisé au XIXe Congrès international de Droit Pénal, Brésil, 31 août – 6 septembre 2014.

IV. Articles

ABDENBI (A.), « La recevabilité de la preuve numérique obtenue au mépris du droit des données personnelles », *Gaz. Pal.*, 9 mars 2021, p. 70.

BERRENDORF (A.), CORHAY (M.), FRANSSEN (V.), « La collecte transfrontière de preuve numérique en matière pénale. Enjeux et perspectives européennes », *Revue justice actualités 2019/1*, n° 1, pp. 32 à 47.

BLANC DE LA NAULTE (A.), CURTIUS (M.), « Un partout, preuve au centre », *Droit du travail et de la protection sociale*, 31 janvier 2024.

COMBRADE (B.-L.), « Les notes blanches des services de renseignement », *RFDA*, p. 1103

DEQUESNES (A.), "Fundamental support study on encryption and fundamental rights", 4 février 2022, Projet Exfiles.

BURRONI (G.), « La preuve pénale par les données issues des objets connectés », *Lefebvre Dalloz*, 3 mai 2021.

FERAL-SCHUHL (CH.), « Le droit à l'épreuve de l'internet », Praxis Dalloz, coll. « Cyberdroit », 8ème édition, février 2020.

LAMBERT (J.-M.), SAUNDERS (Y.), « La conservation des données sur CD-R », Laboratoire National d'Essais – Synthèse étude LNE 021/2000.

MORNET (A.), « Vers un droit commun de la preuve numérique ? », *Lexbase Pénal*, février 2023.

VERGES (E.) :

- « La preuve numérique, entre continuité et changement de paradigme », *Revue Justice Actualité,* édition n°21/Juin 2019, p. 16.

- « Étude : La preuve civile », in *Procédure civile*, Vergès (E.) (dir.), Lexbase, 2022

V. Conclusions, notes et commentaires

SIZAIRE (V.), « Blanc-seing pour les notes blanches » *La Revue des droits de l'homme, La Revue des Droits de l'Homme*, Actualités Droits-Libertés, 26 février 2024.

VI. Textes officiels

A. Textes internationaux et européens

Textes du Conseil de l'Europe

Convention (STCE n°005) du Conseil de l'Europe du 4 novembre 1950, de sauvegarde des droits de l'homme et des libertés fondamentales, (Convention EDH).

Convention (STE n° 108) du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement des données à caractère personnel, (Convention 108 +)

Recommandation n°R(95)13 du Comité des Ministre aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information (Adoptée par le Comité des Ministres le 11 septembre 1995, lors de la 543e réunion des Délégués des Ministres).

Convention STE n° 185 du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité, Budapest.

Lignes directrices CM(2018)169 du Comité des Ministres du Conseil de l'Europe sur les preuves électroniques dans les procédures civiles et administratives (Adoptées par le Comité des ministres le 30 janvier 2019, lors de la 1335e réunion des Délégués des Ministres).

Deuxième protocole additionnel à la Convention sur la cybercriminalité STCE n° 224 du Conseil de l'Europe du 12 mai 2022 relatif au renforcement de la coopération et de la divulgation de preuves électroniques.

Textes de l'Union européenne

Charte des droits fondamentaux de l'Union européenne du 18 décembre 2000, *JOCE* C 364/01, (Charte DFUE).

Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, *JOUE* L 218/8, 14 août 2013 (Directive 2013/40).

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), *JOUE* L 119 du 4 mai 2016.

Directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *JOUE* L 119/89 du 4 mai 2016.

Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de productions et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de libertés prononcées à l'issue d'une procédure pénale, *JOUE* L 191 du 28 juillet 2023.

Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissement désigné et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre de procédures pénales, *JOUE* L 191/118 du 28 juillet 2023.

B. Textes nationaux

- Lois

Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, *JORF* du 6 janvier 1988.

Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, *JORF* n° 0171 du 26 juillet 2015.

- Ordonnances

Ordonnance 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations, *JORF* n° 0035 du 11 février 2016.

- Circulaires

Circulaire du 2 décembre 2016 de présentation des dispositions de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, relative au renforcement du dispositif en matière de lutte contre la délinquance et la criminalité organisée, *BOMJ* n° 2016- 12 du 30 décembre 2016.

- Rapports, études, analyses

LEGER D., « Rapport sur la preuve devant le juge administratif français », Rapport du Conseil d'État de France, 1972.

CNCDH, ass., Avis sur le suivi de l'état d'urgence, 18 février 2016

DIARD (E.), POUILLAT (E.), *Rapport d'information (n° 2082) de la commission des lois, sur les services publics face à la radicalisation, présenté à l'Assemblée nationale*, 27 juin 2019.

VII. Jurisprudences

A. Jurisprudences nationales

C. cass., ch. crim., 9 novembre 1972, n° 71-93.529.

C. cass., ch. crim., 19 décembre 1973, n° 73-90.224.

C. cass., ch. crim., 15 juin 1993, n° 92-82.509

C. cass., ch. crim., 6 avril 1994, n093-82.717

C. cass., ch. crim., 27 février 1996, n° 95-81.366

C. cass., ch. crim., 30 mars 1999, n° 97-83.464.

C. cass., ch. crim., 11 juillet 2001, n° 00- 84.832.

C. cass., ch. com., 4 octobre 2005, n° 04-15.195.

C. cass., ch. crim., 11 mai 2006, n° 05-84.837.

C. cass., ch. com., 15 mai 2007, n° 06-10.606

C. cass., ch. soc., 18 mars 2008, n° 06-40.852

C. cass., Ass., 7 janvier 2011, n° 09-14-316 et 09-14.667

C. cass., ch. civ., 5 avril 2012, n° 11-14.177

C. cass., ch. soc., 4 juillet 2012, n° 11-30.266.

C. cass., ch. civ., 9 janvier 2014, n° 12-23.387 et 12-17.875

C. cass., ch. civ., 5 février 2014, n° 13-21.929.

C. cass., ch. soc., 9 novembre 2016, n° 15-10.203

C. cass., ch. crim., 9 décembre 2019, n° 18-86.767.

C. cass., ch. soc., 30 septembre 2020, n° 19-12.058

C. cass., ch. soc., 25 novembre 2020, n° 17-19.523

C. cass., ch. com., 10 novembre 2021, n° 20-14.669 et 20-14.670

C. cass., ch. crim., 25 octobre 2022, n° 21-85.763

C. cass., ch. soc. 8 mars 2023, n° 21-17.802.

C. cass., Ass., 22 décembre 2023, n° 20-20.648

C. cass., ch. soc., 9 avril 2025, n° 23-13.159

CA de Paris, 27 février 2013, n° 11-11785.

TA Melun, 16 mai 2017, n° 1703246.

TA Bastia, 7 septembre 2017, n° 1700254.

TA Cergy-Pontoise, 4 octobre 2018, n° 160771

CAA Nancy, 15 janvier 2015, n°14NC01754

CE, 3 mars 2003, n° 238662

CE, sec. Contentieux, 16 juillet 2014, n° 355201

CE, Sect., 11 décembre 2015, n° 394989

CE, Juge des référés, 22 janvier 2016, n° 396116.

B. Cour européenne des droits de l'homme

CEDH, 10 octobre 2006, *L.L. c. France,* n° 7508/02

CEDH, 19 février 2009, *A et autres c. Royaume-Uni,* n° 3455/05

CEDH, 11 février 2020, *Buturaga c. Roumanie,* n° 56867/15.

CEDH, 19 février 2023, *Pagerie c. France*, n° 24203/16.

CEDH, 15 juin 2023, *Fanouni c. France,* n° 31185/18

CEHD, 10 décembre 2024, *Association confraternelle de la presse judiciaire et autres c. France*, n° 49526/15 et 13 autres