

Preuves scientifiques et technologiques

Olivier Leclerc, Etienne Vergès, Géraldine Vial

▶ **To cite this version:**

Olivier Leclerc, Etienne Vergès, Géraldine Vial. Preuves scientifiques et technologiques. Cahiers Droit, Sciences & Technologies, 2022, 15, pp.241-261. 10.4000/cdst.6883 . hal-03860992

HAL Id: hal-03860992
https://hal.science/hal-03860992

Submitted on 19 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Cahiers Droit, Sciences et Technologies, **n° 15, 2022, pp. 241-261**

Preuves scientifiques et technologiques

Olivier Leclerc, Directeur de recherche au CNRS, CTAD (UMR 7074), Université Paris Nanterre, Ecole normale supérieure

Etienne Vergès, Professeur à l'Université Grenoble Alpes

Géraldine Vial, Maître de conférences à l'Université Grenoble Alpes

I. Les preuves numériques dans l'enquête pénale

Les preuves numériques sont celles qui résultent de la collecte d'informations par l'intermédiaire de systèmes informatiques. Ces preuves se présentent sous des formes très différentes et elles visent des catégories d'informations très diverses. Les preuves numériques jouent un rôle croissant dans les enquêtes pénales en raison de l'évolution des techniques. En effet, d'une part, la masse de données numériques conservées et disponibles augmente au fil du temps, car ces données s'accumulent progressivement sur des supports et sont, de plus en plus couramment, stockées sur des serveurs ; d'autre part, les technologies utilisées pour accéder à ces données évoluent et se diversifient. Lorsqu'elles sont accessibles à tous (on les dit parfois « en sources ouvertes »), c'est-à-dire disponibles en ligne, ces données peuvent être collectées sans obstacle juridique. La Cour de cassation les considère comme des constatations visuelles, que les enquêteurs peuvent observer et consigner dans leurs des procès-verbaux ou rapports « de constatation ». Lorsque ces données ne sont pas accessibles publiquement (par opposition, on les dira « en sources fermées »), elles sont alors protégées par le droit au respect de la vie privée. On envisagera successivement ces deux situations.

A- Les preuves numériques en sources ouvertes

Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law, janv. 2022, 102 p.

Au début de l'année 2020, Bernard E. Harcourt publiait un ouvrage intitulé *La société d'exposition*[1] dans lequel il analysait la façon dont les usages contemporains des outils numériques, en particulier des réseaux sociaux et d'Internet, « enregistrent des données susceptibles d'être archivées, exploitées et identifiées » (p. 7). Ces traces numériques nous exposent : « un nouveau pouvoir – un pouvoir d'exposition – permet de suivre à la trace et de reconstituer en permanence notre moi numérique » (pp. 22-23). Au-delà de la société de surveillance, qui est au cœur de l'ouvrage, cette disponibilité d'un volume massif de traces numériques ouvre également des voies nouvelles d'enquête pénale. Les données numériques disponibles par une simple recherche sur Internet, sur un réseau social, dans des bases de données publiques peuvent nourrir l'enquête pénale et constituer des éléments de preuve dans le cadre d'un litige. Avec la multiplication des traces numériques croît l'empire de la preuve.

[1] B. E. Harcourt, *La société d'exposition. Désir et désobéissance à l'ère numérique*, Paris, Seuil, 2020.

Avec la multiplication des traces numériques accessibles à tout un chacun croît l'empire de l'enquête.

Par une remarquable actualisation de la confiance placée dans la trace par Locard et les criminologues initiateurs de la police scientifique (« les seuls témoins qui ne se trompent ni ne mentent jamais sont les témoins muets, à condition qu'on sache les interpréter »[2]), les enquêteurs exploitent maintenant les traces numériques afin d'établir la preuve d'infractions les plus diverses. Tout comme la criminologie a mené des investigations approfondies pour établir la fiabilité des traces matérielles[3], les traces numériques sont logiquement l'objet d'attentions particulières, à mesure que leur place augmente dans les enquêtes. En France, le parquet national financier a mis en place un groupe de travail sur les recherches en sources ouvertes chargé de réfléchir aux informations librement accessibles (articles de presse, Internet, données publiques gouvernementales, données commerciales, etc.) et à leur utilisation pour décider d'ouvrir des poursuites et prouver des infractions[4]. Mais cet intérêt n'est évidemment pas cantonné à la France. La publication en janvier 2022 du *Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law* marque une étape importante dans la réflexion sur la collecte et l'utilisation des données numériques librement accessibles. Ce document, réalisé conjointement par le *Human Rights Center* de l'Université Berkeley aux États-Unis et par le Haut-commissariat aux droits de l'homme des Nations-Unies, vise à proposer les standards professionnels que devraient suivre les enquêteurs lorsqu'ils identifient, recueillent, conservent, analysent et présentent des sources numériques d'information librement accessibles dans le cadre d'enquêtes pénales internationales portant sur des violations des droits humains.

Le Protocole retient une conception large des informations librement accessibles (*open source information*). Il s'agit « des informations que toute personne peut observer, acheter ou réclamer, sans avoir besoin d'un statut juridique l'y habilitant ou d'autorisations d'accès particulières ». Plus précisément, les informations numériques ouvertes sont celles qui sont accessibles publiquement dans un format numérique, le plus souvent au moyen d'Internet (§ 14). Cela recouvre les données produites par des utilisateurs ou par des machines, notamment les contenus postés sur un réseau social ; les documents, images, vidéos et enregistrements mis en ligne sur un site Internet ou sur une plateforme d'échange ; les images saisies par les satellites ; les données rendues publiques par les gouvernements dans le cadre des politiques d'*open data* (§ 1). Ce type d'informations sur support numérique occupe une place croissante dans les enquêtes internationales[5], et devrait trouver à nouveau une terre d'élection en Ukraine

[2] E. Locard, *L'enquête criminelle et les méthodes scientifiques*, Paris, Flammarion, 1920 : « Appliquant les données biologiques et chimiques découvertes dans les laboratoires universitaires ou policiers, on a pu procéder à la recherche des criminels, uniquement d'après les empreintes ou les traces qu'ils ont laissées. Le principe est que les seuls témoins qui ne se trompent ni ne mentent jamais sont les témoins muets, à condition qu'on sache les interpréter » (p. 19).

[3] D. Faigman, D. Kaye, M. Saks, J. Sanders, *Science in the Law. Forensic Science Issues*, West Group, 2002.

[4] G. Thierry, « Comment la justice travaille avec les recherches en sources ouvertes », *Dalloz Actualité*, 8 juill. 2022.

[5] S. Jamal, *Le rôle de la science dans l'établissement des faits en droit international : contribution à l'analyse des interactions entre le droit et la science.* Thèse Université Paris 2 Panthéon Assas, 2019 ; S. Jamal, « L'apport des nouvelles technologies aux enquêtes sur place : Le consentement de l'Etat est-il toujours nécessaire ? », in O. De Frouville et J Tavernier (dir.), *La Déclaration universelle des droits de l'homme, 70 ans après : les fondements des droits de l'homme au défi des nouvelles technologies*, Paris, Éd. Pedone, 2019, pp. 177-193 ; Sam Dubberley, Alexa Koenig and Daragh Murray (eds.), *Digital Witness. Using Open Source Information for Human Rights Investigation, Documentation, and Accountability*, Oxford University Press, 2020.

où Eurojust a récemment reçu compétence pour recueillir et conserver les éléments de preuve relatifs aux génocides, aux crimes contre l'humanité, aux crimes de guerre et aux infractions pénales connexes[6].

Si le Protocole insiste sur la nécessité de distinguer information et preuve (§§ 21 et 55 et s.), il souligne que les informations recueillies ont bien vocation, dans certains cas, à être produites comme preuves dans un litige. Le Protocole en tire la conclusion attendue que les enquêteurs doivent être attentifs au cadre juridique dans lequel les éléments d'information recueillis pourront être mobilisés à titre de preuve. Ce cadre juridique détermine en effet les faits à prouver, les standards de preuve applicables, les règles relatives à la licéité des preuves réunies. Mais c'est surtout sur l'appréciation des preuves que le Protocole apporte des éclairages intéressants. Dans un tel cas, en effet, les informations collectées en source ouverte seront appréciées, comme les autres éléments de preuve éventuellement disponibles, par les juges en charge de trancher le litige. D'où l'importance que les éléments de preuve recueillis soient jugés pertinents pour le litige à trancher et suffisamment fiables pour fonder la décision des juges. Or, souligne le rapport, « alors qu'un nombre croissant de personnes enquêtant sur des crimes internationaux et des atteintes aux droits humains utilisent l'Internet pour faciliter leur travail, aucune référence universelle, ni aucun guide ou standard n'existe actuellement pour les enquêtes en sources ouvertes ». C'est cette lacune que le Protocole entend combler en proposant aux enquêteurs des « principes et des bonnes pratiques qui [les] aideront à mener leur travail selon un standard professionnel et qui pourront faciliter si nécessaire la conservation des informations librement accessibles en vue de leur utilisation éventuelle dans le cadre d'une mise en cause officielle » (§ 3). Purement facultatif dans son usage, le Protocole marque ainsi la volonté d'assurer la fiabilité des informations numériques librement accessibles en vue d'établir leur force probante dans le cadre d'un éventuel litige international portant sur les droits humains. La démarche est intéressante : on assiste là à un effort pour assurer la fiabilité des informations numériques librement accessibles, tout comme la fiabilité du témoignage ou de l'écrit ont longtemps occupé les spécialistes de la preuve. Circonscrit dans son objet (les violations internationales des droits humains), le Protocole se reconnaît cependant une vocation extensive : l'analyse du recueil et des usages des données librement accessibles faite pour les violations des droits humains doit pouvoir être étendue à d'autres types de litiges dans le cadre national aussi bien qu'international (§ 5).

Les « standards » que le Protocole propose aux enquêteurs reposent sur trois volets : « professionnel », « méthodologique » et « éthique ».

Le Protocole identifie d'abord des bonnes pratiques « professionnelles ». Celles-ci renvoient au fait de pouvoir rendre compte de ses actions (transparence des recherches effectuées et des méthodes suivies, documentation et conservation du processus de recherche), à la compétence technique et à l'objectivité (entendue comme l'absence de « biais culturels et structurels »), au respect du droit applicable, à la prise en compte de la sécurité dans la collecte et la conservation des informations (§ 25 et s.). Ces exigences, on le comprend, conditionnent à la fois la recevabilité des informations recueillies comme preuve (elles doivent avoir été recueillies de manière licite et leur intégrité doit être garantie) et leur force probante (elles doivent présenter certaines qualités pour convaincre). S'agissant de « témoins muets »[7], il n'est pas surprenant que l'attention se porte, tout comme l'ont fait les spécialistes du témoignage

[6] Règlement (UE) 2022/838 du 30 mai 2022.

[7] E. Locard, *L'enquête criminelle et les méthodes scientifiques*, op. cit., p. 19.

depuis Bentham[8], aussi bien sur la fiabilité des informations que sur la crédibilité des témoins. Le Protocole s'attache donc non seulement à la fiabilité des informations réunies qu'à la crédibilité des producteurs d'information. Sur ce dernier terrain, le Protocole se situe sur une ligne de crête. En effet, il ne soutient pas que les enquêtes en sources ouvertes devraient être réservées à des enquêteurs professionnels. Une telle orientation serait à l'évidence mal venue tant les ONG et les citoyens apportent une contribution essentielle au recueil d'informations numériques pour établir des violations des droits humains[9]. Cependant, le risque existe dans ce cas que la traçabilité du processus de recueil des informations soit insuffisant ou que les enquêteurs apparaissent plus animés par la volonté de faire triompher une cause que par l'établissement des faits, affaiblissant *in fine* la force probante des éléments ainsi recueillis. Le Protocole s'efforce ainsi de tracer une voie médiane entre professionnalisation de l'enquête et mise en œuvre de compétences « professionnelles » propres à garantir la fiabilité des informations recueillies.

Le Protocole formule ensuite à destination des enquêteurs des lignes directrices méthodologiques. Même si leur finalité probatoire n'est pas toujours explicite, les exigences méthodologiques mises en avant sont bien celles qui assurent aux informations recueillies des qualités de fiabilité et de pertinence suffisantes pour prospérer comme preuves en justice. Le Protocole insiste ainsi sur la nécessaire précision de l'enquête, assurée par le recours exclusif à des sources fiables. Les informations librement accessibles collectées par les enquêteurs devraient, ensuite, être seulement des données pertinentes pour une enquête donnée (il convient d'éviter aussi bien la sous-collecte que la sur-collecte des informations). Enfin, les enquêteurs doivent veiller à la conservation des données dont la disponibilité en ligne est toujours précaire, afin de permettre le contrôle de leur exactitude et la vérification de la qualité du travail d'enquête. Le Protocole évoque à ce sujet – par un remarquable rapprochement avec la preuve scientifique[10] – la nécessaire reproductibilité (*replicability*) de l'enquête. A ces trois exigences méthodologiques, le Protocole ajoute celle – plus particulière au contexte des violations des droits humains souvent réalisées en contexte répressif ou belliqueux – de disposer d'un matériel et de logiciels conçus dès l'amont afin d'assurer la sécurité des personnes. En particulier, il importe alors que les données recueillies soient correctement anonymisées et non-attribuables.

Enfin, le protocole encourage les personnes menant des enquêtes à partir de sources librement accessibles à veiller au respect de principes éthiques. Ce volet du Protocole est particulièrement intéressant car il rend visible l'idée, souvent laissée dans l'ombre, que la fiabilité – et, dans le cadre de la preuve, la force probante – des données ne dépend pas seulement des conditions matérielles de leur recueil mais aussi du respect de principes éthiques. Sous cet intitulé, le Protocole vise la dignité des personnes protégées par le droit international ; l'humilité des enquêteurs qui doivent rester conscients des zones d'ignorance qui subsistent et des limites de leurs données ; l'inclusivité des données, qui doivent refléter les perspectives et expériences d'une variété d'acteurs impliqués[11] ; l'indépendance des enquêteurs contre toute influence inappropriée ; et enfin, l'absence de stratagèmes et de manœuvres

[8] J. Bentham, *Rationale of Judicial Evidence, specially applied to English Practice*, 5 vol., Hunt and Clarke, 1827.

[9] M. K. Land, « Democratizing Human Rights Fact-Finding », in Philip Alston and Sarah Knuckey, *The Transformation of Human Rights Fact-Finding*, Oxford University Press, 2016, pp. 399-424 ; J. D. Aronson, « The Utility of User-Generated Content in Human Rights Investigations », *in* Molly K. Land and Jay D. Aronson, *New Technologies for Human Rights Law and Practice*, Cambridge University Press, 2018, pp. 130-148.

[10] O. Leclerc, « Jalons prospectifs sur l'exigence de reproductibilité dans la recherche juridique », *Mélanges en l'honneur de Pascal Ancel*, Luxembourg, Larcier, 2021, pp. 175-186.

[11] Rappr. S. Atrey, « 'The danger of a single story': Introducing Intersectionality in Fact-Finding », *in* Philip Alston and Sarah Knuckey, *The Transformation of Human Rights Fact-Finding*, op. cit., pp. 155-173.

(*misrepresentations*) de la part des enquêteurs pour obtenir des informations (le Protocole emploie ici à nouveau le terme de « transparence », déjà employé plus haut pour désigner l'explicitation des méthodes employées par les enquêteurs).

L'usage probatoire des données numériques librement accessibles a quelque chose de vertigineux. Ces données sont tellement nombreuses, circulent avec une telle célérité, sont si aisément accessibles que les éléments de preuve rendus disponibles, sans que l'on en ait toujours bien conscience, pourraient sembler se multiplier à l'infini. A l'opposé de la preuve préconstituée, on aurait affaire à une preuve par inadvertance. Le Protocole tempère quelque peu ces inquiétudes en venant rappeler que si l'information numérique est maintenant omniprésente, ses usages probatoires restent (classiquement ?) conditionnés à sa licéité, sa pertinence et sa fiabilité.

Olivier Leclerc

B- ***Les preuves numériques en sources fermées***

Cons. const, décision n° 2021-980 QPC du 11 mars 2022 (accès à distance à des données numériques)

Cons. const, décision n° 2021-930 QPC du 23 septembre 2021 (géolocalisation)

Cons. const, décision 3 déc. 2021, n° 2021-952 QPC (communication des données de connexion)

Cons. const, décision 17 juin 2022, n° 2022-1000 QPC (communication des données de connexion)

Cass crim. 12 juill. 2022, 4 arrêts, n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652 (conservation et communication des données de connexion)

Les preuves numériques en sources fermées se trouvent dans un système clos. Soit elles sont conservées sur des supports qui sont physiquement inaccessibles au public (dans un domicile, un bureau), soit elles sont contenues dans un système informatique connecté à un réseau, mais protégé par un code d'accès. Pour accéder à ces données, les enquêteurs peuvent avoir recours à des procédures classiques (perquisitions, saisies des supports numériques), à des techniques plus évoluées (interception de correspondance, accès à distance des systèmes informatiques, balises GPS) ou encore demander aux opérateurs qui collectent ces informations dans des bases de données de les leur communiquer. Ces données concernent généralement la vie privée des personnes visées par les enquêtes : leur localisation, leurs déplacements, les personnes avec qui elles communiquent, les sites internet sur lesquelles elles naviguent, etc.

La question qui se pose depuis l'apparition des techniques d'enquêtes contemporaines (à commencer par les écoutes téléphoniques dans les années 80) est toujours la même : dans quelle mesure, la recherche des auteurs d'infractions peut-elle justifier une atteinte à la vie privée ? La jurisprudence est devenue si abondante dans cette matière, que l'on pouvait croire la question réglée. Toutefois, l'apparition régulière de nouvelles techniques fait ressurgir des difficultés. En effet, la quantité de données numériques conservées, leur durée de conservation et la possibilité d'accéder à ces données en tout lieu accroissent l'ampleur de l'atteinte à la vie privée. Par ailleurs, un acteur généralement peu actif en matière pénale, la Cour de justice de

l'Union européenne, modifie l'équilibre sur lequel se sont accordées au fil des années les trois juridictions habituellement saisies de cette matière (la CEDH, le Conseil constitutionnel et la Cour de cassation). C'est donc un jeu de rôle complexe qui se joue entre ces juridictions, et qui rend l'état du droit positif peu lisible. D'un côté, les juridictions s'attachent à appliquer les principes qui régissent la matière : la nécessité et la proportionnalité, qui doivent se conjuguer avec un contrôle de l'autorité judiciaire (voire juridictionnelle) ; d'un autre côté, les mêmes juridictions brouillent les cartes, en rendant l'application de ces principes obscure, voire en les contournant. Ce paradoxe s'est illustré au cours des derniers mois, à propos de plusieurs techniques probatoires que nous présentons ici rapidement.

1) Identification des preuves numériques

La saisie de données informatiques stockées à distance constitue une évolution majeure des enquêtes pénales, mais également fiscales. Les enquêteurs qui réalisent une perquisition ou une visite domiciliaire peuvent accéder aux documents sur support électronique qui se trouvent dans le lieu visité, mais ils peuvent aussi accéder à des données informatiques stockées à l'extérieur des lieux où la visite a été autorisée, dès lors que cet accès est réalisé à partir de ce lieu[12]. L'intrusion occasionnée par cette mesure est ainsi de plus grande ampleur que celle constituée par la visite physique des lieux. Elle concerne des masses de données plus importantes, conservées le cas échéant sur des serveurs distants, détenues par des tiers et parfois localisées à l'étranger[13].

La géolocalisation est une technique désormais classique dans l'enquête pénale, notamment depuis qu'elle a fait l'objet d'une loi, autorisant expressément le recours à la géolocalisation en temps réel[14]. Cette légalisation n'a pas empêché des plaideurs de contester la constitutionnalité du dispositif, notamment en ce qu'il soustrait la géolocalisation au contrôle d'une autorité juridictionnelle indépendante.

Les données de connexion forment une masse importante et diversifiée d'informations collectées par les opérateurs de communication électronique. Il peut s'agir de l'identité des abonnés, de la localisation de l'équipement terminal (le téléphone par exemple), des dates, heures et durées des communications, des données permettant d'identifier les destinataires, des sites Internet et autres services de communication en ligne consultés par l'abonné. Les détails de la vie privée (d'un individu) révélés par ces données sont très riches. Depuis 2020, ces données numériques sont au cœur d'un contentieux intense concernant, d'une part, leur conservation par les opérateurs de communication, et d'autre part, leur collecte dans le cadre d'enquêtes pénales. En effet, les enquêteurs ont abondamment recours à des réquisitions, pour enjoindre aux opérateurs de communication de conserver et de leur transmettre ces précieuses données, qui permettront, par exemple, de savoir si un suspect se trouvait à proximité du lieu de l'infraction ou s'il a communiqué avec telle ou telle autre personne. Pour cela, ils ont recours à une procédure légère, qui consiste à envoyer aux opérateurs des réquisitions de communication d'informations. Les textes qui régissent la conservation et la communication des données figurent tant dans le Code des postes et des communications électroniques que dans le Code de procédure pénale. Leurs termes particulièrement généraux et la facilité offerte

[12] Cass. com., 15 déc. 2021, n° 21-10.022.

[13] Nous retrouvons ici un thème que nous avions évoqué dans notre chronique des Cahiers droit sciences et technologie n° 11, 2020, spéc. « Preuves spéciales : à la recherche de la preuve électronique », https://doi.org/10.4000/cdst.2963.

[14] Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation.

aux enquêteurs pour recueillir ces données de connexion ont conduit à la saisine de la CJUE, laquelle a rendu en 2020 un arrêt qui a eu un impact retentissant sur le droit français[15].

Les questions posées par toutes ces techniques probatoires sont similaires, car elles permettent aux différentes juridictions saisies d'appliquer les principes classiques en la matière. Toutefois, la tension entre le respect de la vie privée, imposé parfois par des juridictions éloignées du terrain, et la nécessité de permettre aux enquêteurs de disposer des techniques probatoires les plus modernes provoque de multiples remous.

2) Le régime des preuves numériques face au droit au respect de la vie privée

Pour concilier la recherche des preuves et le droit au respect de la vie privée, le recours aux principes de nécessité et de proportionnalité est bien connu. Parfois, vient s'ajouter à ces principes, la nécessité pour l'enquêteur d'obtenir une autorisation juridictionnelle. Ces standards s'imposent sans difficulté aux preuves numériques.

Par exemple, saisie d'une QPC qui contestait la constitutionnalité de l'accès à des données distantes lors de visites domiciliaires en matière fiscale, le Conseil constitutionnel a considéré que le droit de saisie accordé aux enquêteurs poursuivait l'objectif de lutte contre la fraude fiscale, caractérisant ainsi la nécessité d'avoir recours à des techniques probatoires permettant de caractériser ces infractions[16].

Autre exemple, à propos des géolocalisations en temps réel, le Conseil constitutionnel considère que l'usage de cette technique n'est pas disproportionné dans la mesure où il n'implique pas d'acte de contrainte sur la personne visée, ni d'atteinte à son intégrité corporelle, de saisie, d'interception de correspondance ou d'enregistrement d'image ou de son[17]. En d'autres termes, le suivi de la position et des déplacements d'un individu ne constitue pas une atteinte disproportionnée à sa vie privée.

La question la plus délicate concerne l'autorité habilitée à entreprendre ou autoriser la mesure. Sur cette question, le droit français est pris dans un paradoxe. La raison en est assez simple. Depuis plusieurs décennies, la procédure pénale subit une évolution qui conduit à déplacer le pouvoir de contrôle sur les preuves de la phase d'instruction, vers la phase d'enquête. Par conséquent, la plupart des nouvelles techniques peuvent aujourd'hui être employées durant l'enquête. Toute la difficulté réside dans le contrôle exercé par l'autorité judiciaire sur ces mesures intrusives, qui sont alors initiées, non pas par un juge, mais par des officiers de police judiciaire. Le strict respect de la vie privée nécessiterait que les mesures intrusives soient autorisées par un juge indépendant, en l'occurrence le juge des libertés et de la détention. C'est la procédure classique du « mandat » (*warrant*) plus connue des amateurs de séries policières américaines que des juristes français. La recherche d'efficacité implique, au contraire, que ces mesures soient prises rapidement par les OPJ, sous le contrôle du procureur de la République, lequel peut suivre les affaires en temps réel. Cette tension entre une protection efficace de la vie privée et une enquête efficace, conduit à de multiples louvoiements.

Par exemple, à propos de la géolocalisation autorisée durant l'enquête par le procureur de la République (CPP art. 230-33), le Conseil constitutionnel s'en tient à une conception minimaliste du contrôle judiciaire, en considérant que le procureur de la République est un magistrat de l'ordre judiciaire dont la mission est de contrôler la légalité des moyens mis en

[15] CJUE, 6 octobre 2020, Aff. Conjointes, C-511/18 et C-512/18, la Quadrature du Net, C-511/18 et C-512/18 French Data Network, C-511/18 et C-512/18 Fédération des fournisseurs d'accès à Internet associatifs et C-511/18 Igwan.net

[16] Cons. const, décision n° 2021-980 QPC du 11 mars 2022.

[17] Cons. const, décision n° 2021-930 QPC du 23 septembre 2021.

œuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits. Le Conseil se conforme ici à sa vision de l'autorité judiciaire qui, selon l'article 66 de la Constitution, n'exclurait pas le ministère public.

Toutefois, cette conception est perturbée par l'irruption de la CJUE dans le débat sur la conservation et la communication des données de connexion aux enquêteurs. Dans son arrêt précité du 6 octobre 2020, la juridiction européenne a imposé que l'injonction faite par les enquêteurs aux services de communication électronique pour obtenir des données de connexion fasse l'objet d'un contrôle effectif, soit par une autorité administrative indépendante, soit par une juridiction. Cette décision a contraint le Conseil constitutionnel à modifier sa ligne de conduite en considérant désormais que le procureur de la République ne pouvait représenter ni cette juridiction, ni cette autorité indépendante. Ainsi, dans sa décision du 3 décembre 2021[18] le Conseil constitutionnel a considéré que l'autorisation donnée par le procureur de la République pour accéder à des données de connexion n'était pas assortie de garanties suffisantes. Sans évoquer le contrôle d'une juridiction indépendante et sans se référer au droit de l'Union européenne - dont il ne contrôle pas l'application - le juge constitutionnel a tout de même été contraint de s'aligner sur la position de la CJUE. La décision rendue le 17 juin 2022 confirme cette interprétation[19]. Le Conseil était saisi d'une QPC identique en ce qu'elle contestait le pouvoir accordé au juge d'instruction d'adresser des réquisitions aux opérateurs de communication électronique (ou d'autoriser un OPJ à le faire). Dans sa décision, le Conseil estime que cette disposition n'est pas contraire à la Constitution en s'appuyant sur le fait que le juge d'instruction est un « magistrat du siège dont l'indépendance est garantie par la Constitution ».

L'intervention d'un contrôle *a priori* par l'autorité judictionnelle des preuves portant atteinte à la vie privée s'impose peu à peu comme un nouveau standard permettant de garantir que les critères de nécessité et de proportionnalité sont examinés par une autorité indépendante des enquêteurs. Cette conception issue de la *common law* peine tout de même à se généraliser en droit interne, tant elle est antagonique à la tradition d'une enquête menée tambour battant par des policiers zélés qui prennent l'initiative des actes, même s'ils constituent des atteintes aux libertés fondamentales. C'est probablement pour cette raison que les juridictions internes continuent à résister à la tendance qui s'impose peu à peu au niveau européen. Dans les derniers arrêts rendus par la Cour de cassation à propos des données de connexion, cette résistance prend la forme d'un étonnant contournement des principes.

3) Le contournement des principes au profit de la recevabilité des preuves technologiques

Saisie de quatre pourvois à la suite de l'arrêt rendu par la CJUE, la Cour de cassation a dû s'emparer de la question des données de connexion, pour interpréter le droit français en conformité avec le droit européen. Cet exercice était particulièrement délicat, puisque le droit français autorise de façon générale les enquêteurs à adresser des réquisitions aux opérateurs pour obtenir des données de connexion[20]. La Cour de cassation se livre donc à une interprétation du droit français, faite de contorsions et de contournements.

[18] Cons. const, décision 3 déc. 2021, n° 2021-952 QPC

[19] Cons. const, décision 17 juin 2022, n° 2022-1000 QPC

[20] Jusqu'à la fin de l'année 2022 au moins, puisque le Conseil constitutionnel a déclaré plusieurs articles du Code de procédure pénale non conformes, mais qu'il a décalé l'application dans le temps de sa décision (Cons. const, décision 3 déc. 2021, n° 2021-952 QPC).

Elle examine dans un premier arrêt[21] les dispositions qui permettent la conservation des données, et en particulier, en matière pénale, la « conservation rapide », laquelle est tolérée par la CJUE. Par chance, la Cour de cassation trouve dans les dispositions du Code de procédure pénale relatives aux réquisitions, un régime juridique qui lui semble assimilable à des injonctions de conservation rapide. Plus précisément, elle affirme qu'une injonction de conservation rapide (droit de l'UE) peut résulter d'une injonction de produire (réquisitions du CPP). Un premier tour de passe-passe permet ainsi de transformer un hamster en lapin.

Elle précise ensuite que l'injonction de produire des données de connexion (qui implique donc l'injonction de conservation rapide) ne peut concerner que des infractions de criminalité grave, restriction qui n'est pas prévue par les textes français. Toutefois, elle ajoute que c'est à la juridiction saisie qu'il appartient d'apprécier la gravité de la criminalité au regard du droit national. À cet égard, elle ne définit pas un critère strict de gravité, comme pourrait le faire par exemple le législateur en définissant le seuil d'emprisonnement encouru par l'auteur de l'infraction. Bien au contraire, la gravité est ici entendue au sens le plus large, en tenant compte de la nature des agissements, de l'importance des dommages, des circonstances de commission des faits et de la peine encourue.

S'agissant enfin de l'accès aux données, la Cour de cassation bute sur l'exigence d'un contrôle préalable par une juridiction ou une autorité indépendante. Elle est ainsi obligée de reconnaître que la CJUE refuse de confier au ministère public le contrôle des mesures probatoires telles que les données de trafic ou de localisation. Ce constat la conduit à affirmer que l'ensemble des dispositions autorisant les réquisitions durant l'enquête pénale[22] sont contraires au droit de l'Union européenne. En revanche, durant l'instruction, l'intervention du juge d'instruction satisfait à l'exigence de contrôle juridictionnel.

Partant de ce constat, la Cour de cassation aurait dû reconnaître que la procédure française relative aux données de connexion était contraire au droit de l'UE et constituait une atteinte disproportionnée à la vie privée. Une telle irrégularité aurait dû entraîner l'annulation des actes de procédure contenant les données de connexion. Toutefois, la haute juridiction s'est à nouveau livrée à un jeu d'illusionniste. Elle invoque ainsi le principe d'équivalence, qui commande que les règles de procédure nationale s'appliquent indifféremment aux recours fondés sur la violation du droit de l'UE ou du droit interne. Ce raisonnement la conduit à appliquer le régime procédural des nullités à l'irrégularité qu'elle a constatée (l'absence d'autorisation donnée par un juge). Ce régime comporte une importante limite, selon laquelle une irrégularité procédurale n'entraîne la nullité de l'acte que si elle a causé un préjudice au requérant. Or, à l'égard des mesures probatoires intrusives, le préjudice réside précisément dans l'atteinte à la vie privée, que la CJUE a jugé d'une particulière intensité. La violation est telle que la Cour de cassation aurait dû juger que l'irrégularité portait nécessairement atteinte aux intérêts du requérant, comme elle le fait dans de très nombreuses situations où les droits fondamentaux des individus ont été violés (dépassement des délais de garde à vue, atteinte aux droits de la défense, etc.).

Au contraire, la Chambre criminelle affirme que c'est au requérant d'établir qu'il a été victime d'une « ingérence injustifiée » dans sa vie privée. L'affirmation ne peut que surprendre, puisque les conditions posées par la CJUE n'ayant pas été respectées, l'atteinte à la vie privée est nécessairement injustifiée. Plutôt que de tirer les conséquences de cette violation, la Cour de cassation se lance dans une longue litanie d'éléments que les juridictions du fond doivent examiner : l'accès a-t-il porté sur des données régulièrement conservées ? Quelle est la nature des données visées ? Sur quelle durée portent les données communiquées ?

[21] Cass. crim. 12 juill. 2022, n° 21-83.710.
[22] CPP, art. 60-1, 60-2, 77-1-1 et 77-1-2.

Plus étonnant encore, lorsque la Cour de cassation se lance dans un contrôle des circonstances de l'espèce, pour vérifier que l'atteinte été justifiée, elle ne s'intéresse pas à l'ampleur de l'atteinte à la vie privée, mais à l'intérêt des données collectées pour l'enquête. Elle constate ainsi que les données ont été utilisées pour corroborer la thèse de la culpabilité, qu'elles poursuivaient donc un but légitime à propos de faits relevant de criminalité grave. Elle en déduit que la juridiction du fond n'a méconnu aucun des textes visés au moyen.

Dans une argumentation qui mélange les conditions relatives à la protection de la vie privée et celles relatives au régime des nullités, la Cour de cassation jette un voile opaque sur son raisonnement. En arrière-plan, la sauvegarde de procédures irrégulières apparaît comme le seul motif susceptible d'expliquer de tels méandres.

En définitive, la série d'arrêts rendue par la Cour de cassation le 12 juillet 2022 à propos des données de connexion témoigne du malaise croissant que provoque la montée en puissance, à la fois du droit au respect de la vie privée et des preuves intrusives dans l'enquête pénale. Ces deux phénomènes semblent inconciliables. D'un côté, face à l'apparition de preuves nouvelles, certaines juridictions tentent de poser un cadre strict, incluant une limitation de l'utilisation de ces preuves et un contrôle préalable d'une juridiction. D'un autre côté, dans un souci de protéger l'intégrité de procédures en cours, la Cour de cassation tente une opération de sauvetage, au risque de rendre sa parole inaudible et sa jurisprudence incompréhensible. Par l'intrusion toujours plus grande qu'elles suscitent dans la vie privée des individus, les preuves numériques sont à l'origine de cette tension et il est difficile d'anticiper l'évolution du droit en la matière.

Etienne Vergès

II. Licéité du constat d'huissier portant sur des données numériques : une nouvelle pierre à l'édifice

CA Paris, 23 novembre 2021, n° 21/02336

Bien qu'il ne soit pas réglementé par le législateur, le constat d'huissier de justice réalisé sur Internet[23] constitue aujourd'hui une pratique très répandue[24] et encadrée par la jurisprudence[25]. Comme nous l'avions indiqué lors d'une chronique précédente[26], ce constat en ligne pose de nouvelles difficultés qui questionnent l'idée même de constatation réalisée par l'huissier. Lorsqu'il procède au constat de données numériques au moyen d'un dispositif informatique (un ordinateur, un téléphone portable, etc.), l'huissier exerce en effet un rôle plus actif que lorsqu'il est confronté à des contenus matériels. C'est sur ce rôle que revient l'arrêt présenté.

Dans la pratique, un constat d'huissier portant sur des données numériques et réalisé sur Internet recoupe deux hypothèses bien distinctes. La première concerne celle où les constatations de l'huissier reposent sur le *contenu d'une page web* (texte, image, son, vidéo) en vue notamment d'établir la preuve d'un plagiat, d'une diffamation, d'une publicité mensongère ou encore d'un

---

[23] V. sur ce nouveau mode de preuve : E. Vergès, G. Vial et O. Leclerc, *Droit de la preuve*, PUF, coll. Thémis, 2è éd., 2022, n° 640.

[24] V. not. : A. Bobant et E. A. Caprioli, « Le constat en ligne par l'huissier de justice », *D. et procédures* 2007, p. 192. – J. Legrain, « Le constat d'huissier sur Internet », *JCP G*, 2010, p. 959.

25 CA Paris, 12 janvier 2016, n°2014/14431 reprenant les exigences de la norme AFNOR Z67-147 instaurant un protocole permettant d'authentifier les constatations effectuées par les huissiers sur Internet.

[26] G. Vial, « Constats d'huissier en ligne : le cas particulier du constat portant sur une application mobile : CA Paris, 22 septembre 2020, n° 19/10492 », *Cahiers Droit, Sciences et Technologies*, n° 13, 2021, Chronique Preuves scientifiques et technologiques.

acte de contrefaçon. Les pages web étant en libre accès[27], l'huissier peut alors procéder au constat de leur contenu, sans avoir à solliciter d'autorisation mais à la condition de respecter un formalisme très précis[28] – concernant essentiellement le mode opératoire utilisé par l'huissier – visant à donner aux constatations matérielles de l'officier ministériel une neutralité incontestable, garante de la fiabilité du constat imposée par la jurisprudence. L'huissier doit par ailleurs, comme pour tout constat – virtuel ou non – se contenter de procéder à des constatations matérielles[29].

La seconde hypothèse se rencontre lorsque l'huissier doit réaliser le constat du *contenu d'une application mobile*. Ce constat lui impose d'entrer dans une démarche plus active que lorsqu'il se contente de consulter une page web. Il va en effet devoir télécharger l'application, se créer un compte, utiliser un code secret, puis ouvrir ladite application. S'est alors posée la question de savoir si, dans cette hypothèse, l'huissier se contente toujours de procéder à une « constatation », au sens de l'ordonnance du 2 novembre 1945 relative au statut des huissiers et aujourd'hui de celle du 2 juin 2016 relative au statut des commissaires de justice[30]. En d'autres termes, l'huissier conserve-t-il lors du téléchargement, puis de l'ouverture de l'application, le « rôle passif » qui doit être le sien pour que le constat réalisé puisse être admis à titre de preuve ? Ayant déjà apporté des éléments de réponse quant à la délimitation du rôle de l'huissier au moment du téléchargement de l'application[31], la Cour d'appel de Paris se prononce cette fois sur le rôle de l'huissier lors de l'ouverture de l'application mobile.

En l'espèce, le demandeur avait créé un test de personnalité informatisé se présentant sous la forme d'une base de données et avait fondé avec la partie adverse, une société pour l'exploitation de cette base de données accessible *via* une adresse URL. Suite à diverses dissensions, le demandeur a ensuite vendu ses parts à son associé et lui a concédé la jouissance provisoire de sa base de données. Au terme de la durée conventionnelle de jouissance, le demandeur soutient que la partie adverse a continué d'utiliser la base de données et produit à titre de preuve un constat d'huissier dont la recevabilité est contestée jusque devant la Cour d'appel de Paris.

Dans cet arrêt du 23 novembre 2021, les juges décident que l'huissier de justice ne peut ouvrir un compte utilisateur personnel d'une application sans adopter un rôle actif. Les juges précisent par ailleurs que la création dudit compte, sans mentionner la qualité d'huissier de justice, constitue un comportement déloyal, de sorte que le procès-verbal de constat ainsi dressé doit être partiellement écarté des débats.

Le rôle actif de l'huissier. La Cour d'appel de Paris rappelle d'abord que selon l'article 1er de l'ordonnance de 1945 en vigueur au moment des faits[32] – repris par l'article 249 du Code de

[27] Un site Internet ne constitue pas un domicile virtuel (TGI Paris, ord. réf., 14 août 1996, *JCP G* 1996, 11, n° 22727. – CA Paris, 28 fév. 2018, n° 16/0226).

[28] Ce formalisme a été décrit par le TGI de Paris en 2003, puis a été repris et augmenté par la norme AFNOR NF Z67-147 du 11 septembre 2010. Il est aujourd'hui appliqué par la jurisprudence : CA Paris, 12 janv. 2016, n°2014/14431 et 24 janv. 2014, *JurisData* nº 016966. – CA Aix-en-Pce, 15 sept. 2016, n° 13/22133. – T. Com., Paris, 22 juin 2012, *Juris-Data* nº 034113.

[29] Cass. civ. 1, 20 mars 2014, n° 12-18.518.

[30] En vertu de l'ordonnance n° 2016-728 du 2 juin 2016, les huissiers de justice ayant suivi une formation spécifique sont, depuis le 1er juillet 2022, désignés sous l'appellation de commissaires de justice. Cette nouvelle appellation ne change cependant pas le régime du constat que ces professionnels sont amenés à réaliser.

[31] CA Paris, 22 sept. 2020, n° 19/10492.

[32] L'ordonnance du 2 novembre 1945 a été abrogée par celle du 2 juin 2016 préc. relative au statut des commissaires de justice.

procédure civile et par l'article 1er de l'ordonnance de 2016 relative au statut des commissaires de justice en vigueur aujourd'hui –, l'huissier ne peut qu'« *effectuer des constatations purement matérielles, exclusives de tout avis sur les conséquences de fait ou de droit qui peuvent en résulter* ». Non définie par le législateur, cette notion de « constatations purement matérielles » a été délimitée par la jurisprudence précisant que ces constatations excluent nécessairement toute opération intellectuelle de la part de l'huissier[33]. Sur ce point, l'huissier se distingue de l'expert. Il doit conserver un rôle de spectateur, un rôle passif[34]. Pour la jurisprudence, l'huissier demeure dans ce rôle passif, lorsqu'il se contente de « cliquer » sur certaines mentions d'un site Internet[35], de réaliser des captures d'écran de certaines pages[36] ou de télécharger une application gratuite et proposée au grand public, sans sélection ou autorisation préalable, *via* le compte personnel de son mandant[37].

En l'espèce, suite au téléchargement de l'application, l'huissier s'est créé un compte personnel pour ouvrir l'application, a accepté les conditions générales d'utilisation du site Internet et a effectué le test de personnalité proposé par ladite application. Se faisant, il a exprimé un consentement et s'est, pour les juges parisiens, engagé « *dans une démarche active, de sorte qu'il n'a pas conservé un rôle passif* ». Cette solution est à rapprocher de l'arrêt rendu par la Cour de cassation le 20 mars 2014 qui avait qualifié de « démarche active », l'ouverture par l'huissier d'un compte client pour procéder à un achat en ligne[38].

A la condition d'être accessible à tous[39], le téléchargement d'une application peut donc être réalisé par l'huissier, sur le compte privé de son étude, au moyen de ses propres identifiants. En revanche, pour l'ouverture et l'utilisation de l'application, l'huissier ne peut, afin de demeurer neutre et passif, se créer de compte client personnel. Il lui est nécessaire de prendre la précaution d'ouvrir l'application *via* le compte personnel et les identifiants de son mandant. Dans le cas contraire, il sort du rôle passif qui doit être le sien lors d'un constat et prend le risque de voir le mode de preuve ainsi obtenu, écarté des débats pour cause d'illicéité.

Le comportement déloyal de l'huissier. La licéité du constat en ligne se trouve également subordonnée à sa loyauté. La Cour d'appel de Paris rappelle dans cet arrêt qu'« *il résulte de l'article 9 du Code de procédure civile qu'il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention. Le principe de loyauté dans le recueil des preuves, qui constitue un élément du procès équitable, doit se concilier avec le droit à la preuve* ». La Cour poursuit en décidant qu'« *en ne déclinant pas sa qualité d'officier ministériel, à tout le moins en utilisant une adresse internet faisant apparaître sa qualité, l'huissier de justice n'a pas recueilli loyalement les informations en cause* ». L'huissier se voit donc reprocher le fait de ne pas avoir décliné sa qualité d'officier ministériel. Pour créer le compte nécessaire à l'ouverture de l'application, l'huissier avait, en l'espèce eu recours à son identité civile et à son adresse électronique personnelle. Se faisant, les juges ont considéré que l'huissier avait tu sa qualité professionnelle et n'avait donc pas instrumenté en tant qu'huissier.

---

[33] Cass. soc., 18 mars 2008, n° 06-40.852.

[34] CA Paris, 25 oct. 2006, n° 05/20120. – Cass. civ. 1, 20 mars 2014, précit. – CA Paris, 5 juill. 2019, n° 17/03974 et 22 sept. 2020, préc.

[35] CA Paris, 5 juillet 2019, n° 17/03974.

[36] CA Paris, 25 octobre 2006, n° 05/20120. – Cass. civ. 1, 20 mars 2014, précit.

[37] CA Paris, 22 sept. 2020, préc.

[38] Cass. civ. 1, 20 mars 2014, précit.

[39] C'est-à-dire lorsque le téléchargement n'est conditionné à aucune autorisation, ni à aucun contrôle par un webmaster. V. sur ce point : G. Vial, « Constats d'huissier en ligne : le cas particulier du constat portant sur une application mobile : CA Paris, 22 septembre 2020, n° 19/10492 », chron. précit.

Sorti du contexte virtuel, cela correspondrait à l'hypothèse d'un constat réalisé par un huissier dans un domicile après avoir décliné son identité, mais en ayant caché sa qualité d'officier ministériel. Un tel constat serait inévitablement écarté des débats en tant que réalisé de manière déloyale[40]. Néanmoins, si annoncer et justifier sa qualité d'huissier au cours d'un constat « traditionnel », dans un domicile qui n'a rien de virtuel, ne pose guère de difficultés, il n'en va pas nécessairement de même lors d'un constat de données numériques stockées dans un lieu virtuel. L'article 3 du décret n° 2021-1625 du 10 décembre 2021 relatif aux compétences des commissaires de justice indique en effet que la justification de la qualité d'huissier de justice s'effectue par la présentation d'une carte professionnelle. Or, en l'espèce, aucun procédé n'était instauré pour permettre à l'huissier d'indiquer sa profession lors de la création de son compte. Le monde virtuel n'offrait pas la possibilité à l'huissier de se présenter en tant que tel. La Cour d'appel de Paris suggère néanmoins dans cet arrêt que l'huissier de justice puisse décliner sa qualité en usant simplement de son adresse électronique professionnelle.

Si l'usage probatoire des données numériques librement accessibles a effectivement « quelque chose de vertigineux »[41], il n'est toutefois possible devant les tribunaux que lorsque ces données ont été recueillies de manière licite. La Cour d'appel de Paris le rappelle clairement dans cet arrêt.

Géraldine Vial

III. Preuve d'infractions par caméras et drones : les nouvelles technologies de captation d'images au service des forces de l'ordre

Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure

A la suite de la censure par le Conseil constitutionnel[42] de certaines dispositions de la loi du 25 mai 2021 pour une sécurité globale préservant les libertés[43], plusieurs articles de la loi du 24 janvier 2022 sont venus remanier le cadre juridique de l'utilisation de certains modes de preuve par les forces de l'ordre, afin de concilier au mieux les objectifs de prévention des atteintes à l'ordre public, de recherche des auteurs d'infractions et le droit au respect de la vie privée.

Parmi les très nombreuses dispositions de cette loi[44], il est possible de citer, par exemple, le cas de la vidéosurveillance des locaux de garde à vue, l'usage des caméras piétons et des caméras embarquées dans les véhicules des policiers, gendarmes et douaniers, ainsi que celui

[40] En matière de constat « traditionnel » réalisé dans un lieu privé matériel, la jurisprudence considère que l'huissier doit annoncer sa qualité dès la réalisation du constat (Cass. civ. 2, 10 fév. 2011, nº 10-13.894. - Cass. soc., 5 juill. 1985, nº 92-40.050) et qu'il ne peut prendre une fausse qualité (Cass. soc., 5 juill. 1995, *Bull. civ*. V, nº 237). V. sur ce point : E. Vergès, G. Vial et O. Leclerc, *Droit de la preuve*, PUF, coll. Thémis, 2è éd., 2022, n° 627.

[41] Voir *supra* le commentaire qu'Olivier Leclerc consacre aux preuves numériques en sources ouvertes dans cette Chronique.

[42] Cons. Const., 20 mai 2021, DC n° 2021-817.

[43] Loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, *JORF* n°0120 du 26 mai 2021.

[44] Pour une étude détaillée de ce texte, v. not. J. Buisson, *Procédures*, n° 6, juin 2022, étude n° 8 et M. Daury-Fauveau, *JCP G*, 2022, doctr. 256.

des drones ou ballons captifs par les forces de l'ordre. L'utilisation de ces aéronefs et celle des images enregistrées par les caméras aéroportées qu'ils contiennent est désormais prévu, lorsqu'il poursuit des « finalités de police administrative » comme la prévention des atteintes à la sécurité des personnes ou des actes de terrorisme ou la sécurité des rassemblements sur la voie publique en cas de risque de « troubles graves à l'ordre public ». Il est alors entouré de garanties par l'article L. 242-5 du Code de la Sécurité intérieure dans sa nouvelle rédaction : il nécessite une autorisation préalable du préfet ; il ne peut excéder une durée de trois mois et doit porter sur un périmètre géographique réduit. Les caméras doivent par ailleurs être orientées de façon à ne pas viser l'intérieur d'un domicile ou ses entrées. L'usage des drones a également été élargi à « des finalités judiciaires » pour les nécessités d'une enquête ou d'une instruction portant sur les crimes et certains délits. Il est, par ailleurs, autorisé pour les douaniers dans leurs missions de prévention des trafics transfrontaliers. En revanche, l'utilisation des drones et des caméras embarquées a été refusé pour les policiers municipaux ; le Conseil constitutionnel ayant censuré les dispositions de la loi du 24 janvier 2022 les concernant[45].

Géraldine Vial

IV. Preuve de la minorité par le recours aux examens radiologiques osseux : l'affaiblissement jurisprudentiel d'un mode de preuve scientifique douteux

Cass. Civ. 1, 12 janv. 2022, n° 20-17.343

La preuve de la minorité constitue un enjeu important dans le contentieux de la prise en charge des mineurs non accompagnés, notamment étrangers, dans la mesure où la minorité garantit à l'individu un statut plus avantageux que celui d'une personne majeure. Toutefois, les circonstances de l'arrivée de ces personnes sur le territoire d'asile rendent parfois la preuve de leur minorité délicate à apporter, soit parce que la production des documents de leur état civil s'avère impossible, soit parce que cette production révèle des incohérences entre la minorité ressortant des documents d'identité et d'autres éléments, tels que l'apparence physique de la personne laissant penser qu'elle est majeure. Pour pallier cette carence de la preuve, les autorités peuvent alors avoir recours à des examens radiologiques osseux. Ces tests reposent sur une radiographie, le plus souvent du poignet et de la main gauches de l'individu, puis sur sa confrontation au cliché le plus proche issu d'un atlas de référence dit de Greulich et Pyle[46], du nom de deux anatomistes américains.

L'utilisation de ces tests est néanmoins controversée[47]. D'une part, cet atlas a été constitué, dans les années 50, à des fins purement médicales pour détecter, chez des enfants d'âge connu, un trouble de croissance ou de maturation osseuse et n'était aucunement destiné à apporter la preuve de l'âge de la personne dont l'état civil est incertain. D'autre part, la fiabilité de ces tests est elle-même contestée. Les radiographies utilisées dans l'atlas datent des années 1930 et proviennent d'enfants et adolescents américains blancs issus des classes moyennes. Or, les personnes soumises à ces tests arrivent quant à elles le plus souvent d'Afrique, d'Asie ou

[45] Cons. Const., 20 janvier 2022, DC n° 2021-834.

[46] Greulich WW, Pyle SI. *Radiographic atlas of skeletal development of the hand and wrist*, Stanford University, 1959.

[47] Parmi une abondante littérature, v. not. : P. Chariot, « Quand les médecins se font juges : la détermination de l'âge des adolescents migrants », *Chimères*, vol. 74, n° 3, 2010, pp. 103-111.

d'Europe de l'Est ; ce qui interroge sur la pertinence des données de l'atlas de Greulich et Pyle[48].

C'est pourquoi, cette preuve scientifique bien qu'autorisée, fait l'objet de grandes précautions et a été assortie de multiples garanties procédurales. L'article 388 du Code civil[49] énonce ainsi que ces tests ne peuvent être réalisés qu'en l'absence de documents d'identité valables[50], lorsque l'âge allégué n'est pas vraisemblable et seulement sur décision de l'autorité judiciaire, après recueil de l'accord de l'intéressé. L'article 388 du Code civil dispose en outre que les conclusions de l'examen osseux doivent préciser la marge d'erreur de celui-ci[51] et il limite les conséquences que les juges peuvent en tirer en indiquant que les conclusions de l'examen ne peuvent à elles seules forger la conviction des juges et doivent être corroborées par d'autres éléments de preuve.

Cette règle du caractère subsidiaire des tests osseux a été appliquée par la Cour de cassation à plusieurs reprises[52]. L'arrêt du 12 janvier 2022 en est une nouvelle illustration. En l'espèce, une personne née en Guinée se prétendait mineur isolé afin de bénéficier d'une procédure d'assistance éducative. Elle produisait pour cela un extrait d'acte de naissance et un passeport. Devant le peu de vraisemblance de ces documents quant à sa date de naissance, un examen osseux fut pratiqué, concluant à une fourchette d'âge comprise entre 18 et 20 ans. Considérant que la preuve de la minorité n'était pas rapportée, les juges du fond ordonnèrent la main levée de la mesure de protection. L'intéressé forma un pourvoi en cassation en invoquant que le doute ressortant des différents éléments de preuve aurait dû lui profiter et conduire au maintien des droits attachés à la minorité. Au visa de l'article 388 du Code civil, la Cour de cassation rappelle que ces tests sont insuffisants à établir à eux seuls la preuve de la majorité de la personne. Lorsqu'ils concluent à la majorité de l'intéressé, les résultats de ces tests doivent nécessairement être corroborés par d'autres éléments de preuve pour que le juge puisse considérer la preuve de la majorité établie. Or, en l'espèce, les différents documents d'identité venaient contredire les résultats des examens osseux, il existait donc bien un doute dont l'intéressé aurait dû profiter.

Cet arrêt confirme ainsi que le pouvoir d'appréciation des juges est limité lorsque la preuve issue de ces examens osseux est isolée, c'est-à-dire lorsqu'elle n'est pas corroborée par d'autres éléments de preuve. La force probante de cette preuve scientifique en ressort affaiblie ; le résultat de ces tests ne s'apparente désormais plus qu'à une demi-preuve[53].

Géraldine Vial

---

[48] Ce doute a notamment été relayé par le CCNE (avis n°88 sur les méthodes de détermination de l'âge à des fins juridiques, 11 juillet 2005, www.ccne-ethique.fr.) et par le Comité européen des droits sociaux du Conseil de l'Europe (CEDS, déc., 15 juin 2018, n° 114/2015, EUROCEF c/ France).

[49] Jugé conforme à la Constitution (CC, déc. n° 2018-768 QPC du 21 mars 2019), ainsi qu'à la CIDE et à la CESDH (Cass. Civ. 1, 12 févr. 2020, n° 18-24264 et 21 nov. 2019, n° 19-15890).

[50] Rappelé par Cass. Civ. 1, 21 nov. 2019, n° 19-17.726.

[51] Nous renvoyons sur ce point à O. Leclerc, « La preuve de la minorité au moyen d'un examen radiologique osseux », *Cahiers Droit, Sciences et Technologies*, n° 11, 2020, p. 217.

[52] Cass. Civ. 1, 22 mai 2019, n° 18-22.738 et 21 nov. 2019, précit.

[53] Sur cette notion, v. not. E. Vergès, G. Vial et O. Leclerc, *Droit de la preuve*, préc., n° 414.

V. Nomenclature des spécialités expertales

Arrêté du 22 août 2022 relatif à la nomenclature prévue à l'article 1er du décret no 2004-1463 du 23 décembre 2004 (NOR : JUSC2214169A)

Ainsi que l'écrivait, pour le déplorer, Cornelia Vismann, « les dossiers restent sous le seuil de perception du droit »[54]. Aussi n'est-il pas sans intérêt de s'arrêter un moment sur un document obscure destiné à organiser la constitution des listes d'experts judiciaires : la nomenclature des spécialités dans lesquelles doivent être inscrits les experts qui en font la demande. Celle-ci, établie par arrêté du garde des sceaux, ministre de la justice, a été récemment modifiée par un arrêté du 22 août 2022. En vigueur « pour l'établissement des listes d'experts judiciaires dressées à compter du mois de novembre 2023 », il remplacera alors l'arrêté du 10 juin 2005[55], lui-même abrogé à compter du 1er janvier 2024. Un bref rappel du contexte s'impose[56] : le décret n° 2004-1463 du 23 décembre 2004 relatif aux experts judiciaires demande que soit « dressées chaque année une liste nationale et une liste par cour d'appel sur lesquelles sont inscrits les experts désignés tant en matière civile qu'en matière pénale » (art. 1). Ces listes sont établies par l'assemblée générale des magistrats du siège des cours d'appel et par le bureau de la Cour de cassation. C'est pour ordonner ces listes que l'arrêté commenté est pris par le ministre de la justice. Formellement, cet arrêté se présente comme une liste de spécialités, suivant une division en « branches », « rubriques » et « spécialités ». Par exemple, dans la branche « A. Agriculture – Agro-alimentaire – Animaux – Forêts », on trouve la rubrique « A.14. Santé vétérinaire », qui comporte parmi ses spécialités « A. 14.3. Médecine, chirurgie, élevage, bien-être et transport des ruminants (bovins, ovins, caprins, camélidés), des équidés (chevaux, poneys, ânes et croisements) et des porcins ». Les branches sont au nombre de 8, les rubriques de 89, les spécialités de 557. L'ensemble s'étale sur près de 14 pages au Journal officiel.

A première vue, cette nomenclature constitue un document d'ordre administratif, destiné à organiser la bonne marche des juridictions de l'ordre judiciaire. Et c'est bien ce qu'elle est. Mais il est permis d'y voir plus que cela : l'énoncé des spécialités scientifiques et techniques qui sont suffisamment robustes pour pouvoir être mises au service de l'institution judiciaire[57]. L'arrêté constitue donc l'un des lieux où se joue l'attribution par le droit français d'un sceau de scientificité à des savoirs scientifiques et techniques. Assurément, les cours d'appel ne sont nullement obligées de pourvoir l'ensemble des spécialités de la nomenclature et c'est avant tout les besoins des juridictions du ressort qui dictent la décision de pourvoir ou non, et en plus ou moins grand nombre, telle ou telle spécialité. De même, les tribunaux peuvent nommer des experts « hors liste ». Il reste que la liste permet d'apercevoir l'ensemble des spécialités dont la Chancellerie estime qu'elles peuvent être utiles aux juges du fond lorsqu'ils ordonnent une mesure d'instruction exécutée par un technicien.

L'analyse de la nouvelle nomenclature ne peut se faire que par comparaison avec celle arrêtée en 2005[58]. Or, force est de constater que l'allure d'ensemble des deux nomenclatures est

---

[54] C. Vismann, *Files. Law and Media Technology*, Stanford University Press, 2008, p. 11.

[55] NOR : JUSC0520361A.

[56] Nous nous permettons de renvoyer sur ce point à notre ouvrage E. Vergès, G. Vial, O. Leclerc, *Droit de la preuve*, Paris, PUF, 2e ed., 2022, n° 718 et s.

[57] O. Leclerc, *Le juge et l'expert. Contribution à l'étude des rapports entre le droit et la science*, Paris, LGDJ, 2005, p. 230 et s.

[58] On notera que le vice-président du Conseil d'Etat est aussi chargé d'élaborer une nomenclature correspondant aux domaines d'activité dans lesquels les juridictions administratives sont susceptibles de recourir à une expertise (CJA, art. R. 221-9). La nomenclature actuellement en vigueur dans les juridictions administratives

très similaire. Dans le détail, on constate d'abord des changements dont la portée est minime, voire nulle. Ainsi certaines branches sont renommées (par exemple, la branche B. Arts – Culture – Communication – Médias est amputée du Sport ; la spécialité B.4.6. « Publicité » devient B.4.7. « Relations médias, presse, publics »). De même, des disciplines qui étaient jusqu'alors des « spécialités » sont remontées d'un niveau dans la nomenclature et deviennent des « rubriques ». C'est le cas, en particulier dans les branches « C. Bâtiment – Travaux publics – Gestion immobilière » et « G. Criminalistique – Sciences criminelles – Médico-légales ». Enfin, la branche « H. Interprétariat – Traduction », qui comportait jusqu'alors 3 rubriques et 14 spécialités, en compte maintenant, respectivement, 2 (interprétariat et traduction) et 154 (les langues ne sont plus regroupées par grandes familles mais énumérées l'une après l'autre).

D'autres changements retiendront, cependant, un peu plus l'attention. En premier lieu, certaines reformulations et certains ajouts peuvent sembler significatifs d'un changement de perception des enjeux liés aux contentieux dont connaissent les juridictions. Ainsi, ce qui était jusqu'alors désigné sous l'appellation risques naturels est maintenant saisi dans la perspective du changement climatique. A ce titre, la rubrique « A.9. Neige et avalanche » devient « A.9. Risques climatiques et météorologiques », la rubrique « E.3. Pollution » devient « E.3 Environnement », avec un ensemble plus étoffé de spécialités. En deuxième lieu, la nomenclature reflète les changements qu'a connu, au cours des dernières années, le droit de la responsabilité civile. C'est ainsi que la nomenclature mentionne maintenant dans la branche D non plus seulement « Economie et finance » mais aussi « Calculs préjudiciels » et dans la rubrique « A.3. Aménagements et équipements de l'espace rural – Atteintes à l'environnement », la spécialité « Préjudices écologiques ». En troisième lieu, certaines spécialités nouvelles font leur entrée dans la nomenclature. C'est le cas, par exemple, des productions culturelles et communication sur les plateformes digitales (B.4.1), de la publicité digitale (B.4.2), de la gestion de projets industriels (E.11). Dans le domaine de la santé (branche F), on notera également, à la lumière de l'actualité des dernières années et de ses suites judiciaires, l'intégration des spécialités « Médecine d'urgence et de catastrophe » (F.1.19), « vaccinologie » (F.5.13), « prévention des risques sanitaires, nucléaires, chimiques » (F.11.1), « recherche médicale et éthique » (F.11.2). Plus remarquable encore, si l'on a bien à l'esprit le fait que la nomenclature dit quelque chose des spécialités dont le crédit est suffisant pour que les tribunaux fassent appel à elles, est la place faite aux disciplines paramédicales, et surtout aux médecines alternatives. Concernant les premières, la nomenclature de 2005 présentait une rubrique « F.8. Sages-femmes et auxiliaires médicaux », comportant une spécialité « Auxiliaires réglementés » désignant les infirmiers, kinésithérapeutes, orthophonistes et orthoptistes. La nouvelle nomenclature est bien plus détaillée. Sont ajoutés les audioprothésistes, opticiens lunetiers, prothésistes, orthésistes (F.8.1.), les diététiciens (F.8.2), les pédicures, podologues (F.8.7), les psychomotriciens ergothérapeutes (F.8.8). Concernant les médecines alternatives, on observera avec intérêt la création d'une rubrique « Non professionnels de santé – bien-être – confort » (F.12), comportant les chiropracteurs (F.12.1) et les ostéopathes non médecins ni auxiliaires médicaux (F.12.2). La référence faite à ces pratiques de soin ne tranche certes pas le débat, qui ressurgit à intervalles réguliers en France, sur leur caractère scientifique mais il est du moins admis que les praticiens peuvent éclairer les juridictions sur des faits relevant de leur compétence.

Enfin, on signalera deux changements, qui relèvent moins du texte que du paratexte. Le premier est révélateur d'un (léger) déplacement des relations entre la Chancellerie et les

(arrêté du 19 novembre 2013 relatif à la nomenclature prévue à l'article R. 221-9 du code de justice. NOR : JUSE1328519A) est très proche de celle adoptée en 2005 pour les experts intervenant devant les juridictions de l'ordre judiciaire.

compagnies d'experts judiciaires. En effet, si la nomenclature de 2005 avait été conçue en concertation avec la Fédération nationale des compagnies d'experts judiciaires (FNCEJ, devenue en 2006 Conseil national du même nom), il n'en était pas fait explicitement mention. Dans la nouvelle mouture de la nomenclature, l'intitulé de chaque branche est suivi de la précision suivante : « Pour être plus amplement informés, les magistrats peuvent se référer à l'annuaire national des experts développé par le Conseil national des compagnies d'experts de justice (CNCEJ) qui répertorie des informations plus précises sur le profil, l'expérience et les spécialités de l'expert ». La mesure permet aux magistrats de disposer d'une information synthétique et facilement accessible sur les titres et l'expérience professionnelle de chaque expert inscrit. En retour, pour ces derniers, l'adhésion à une compagnie d'experts acquiert une importance qu'elle n'avait pas jusqu'alors. Le second changement tient au fait que la nomenclature comporte maintenant en annexe (ce qui n'était pas le cas en 2005) un formulaire que les experts devront utiliser pour indiquer la ou les rubriques ainsi que la ou les spécialités dans lesquelles ils souhaitent être inscrits à compter du 1er janvier 2024. Somme toute assez banale dans son contenu (coordonnées, spécialité actuelles, spécialités pour lesquelles l'inscription est demandée, justificatifs), cette annexe offre une nouvelle illustration de la diffusion de la régulation juridique jusque dans les formats des pièces administratives.

Olivier Leclerc