LA PREUVE NUMÉRIQUE, ENTRE CONTINUITÉ ET CHANGEMENT DE PARADIGME

Par

Étienne VERGÈS
Professeur à l'Université Grenoble Alpes

La preuve numérique constitue-t-elle une nouveauté dans le paysage judiciaire ? Bouleverse-t-elle la physionomie du droit de la preuve et la pratique juridictionnelle ? Voici deux questions qui traversent toutes les contributions à ce dossier consacré au traitement de la preuve numérique par les magistrats. La réponse à ces questions est nécessairement nuancée. C'est pour cette raison que nous évoquerons, dans l'ouverture de ce dossier, deux idées contradictoires, mais qui coexistent. D'un côté, la preuve numérique s'inscrit dans une continuité. Elle ne présente pas de différence de nature avec les preuves classiques et son régime n'est pas dérogatoire au droit commun de la preuve. En ce sens, le recours à la technologie numérique constitue bien une spécificité, mais il ne provoque pas de changement majeur dans les règles de droit et dans la manière de traiter ces preuves en justice. D'un autre côté, certaines techniques probatoires particulières introduisent dans le système judiciaire et dans la manière de rendre la justice, des problématiques tout à fait nouvelles, auxquelles le juge est confronté, et qu'il doit résoudre dans une certaine solitude. En effet, de nouvelles techniques probatoires sont apparues en pratique et certaines ont été reconnues par le législateur, mais ce dernier n'a pas donné aux juges et magistrats du parquet les outils pour résoudre les difficultés juridiques engendrées par ces nouveaux modes de preuve. Plus encore, le législateur a créé des difficultés supplémentaires dans le traitement de ces preuves. Par conséquent, les juges sont confrontés à un véritable changement de modèle, qui se traduit principalement par le caractère inintelligible de ces nouveaux modes de preuve. Nous faisons ici allusion aux écrits et aux signatures électroniques, ainsi qu'à leurs modes de conservation et de certification.
Dans cette contribution, nous tenterons d'aborder ces deux aspects (la continuité et le changement de paradigme) sous l'angle du régime juridique de la preuve et celui de la mise en œuvre pratique de ce régime. Mais avant cela, il nous paraît important de préciser ce que recouvre le concept de preuve numérique et les différentes catégories qu'il contient.

Preuves numériques classiques et nouvelles

La preuve numérique n'est pas un concept défini par le droit. Le code civil parle bien de l'écrit électronique[1] et de la signature électronique[2], mais le concept général de preuve numérique est absent des textes et de la jurisprudence. La catégorie correspond donc à ce que l'on veut bien mettre dedans et ce contenu est hétérogène. Il est possible de distinguer deux grands ensembles de natures très différentes. Le premier est constitué par des preuves classiques qui ont été numérisées. Il en est ainsi des photographies, des vidéos ou des sons, que l'on recueillait précédemment sous une forme analogique[3] et qui sont aujourd'hui numérisés. Il en est encore ainsi de procédés qui ont changé sous l'effet de la technologie, mais dont la fonction ne diffère pas. Par exemple, la localisation d'un individu dans une enquête pénale peut se faire au moyen d'une filature, d'un témoignage ou d'une géolocalisation. La technologie apporte une grande richesse à la preuve. On peut géolocaliser une

[1] Art. 1366 du code civil.
[2] Art. 1367 du code civil.
[3] Des photographies argentiques, des bandes-son ou des vidéos gravées sur différents supports analogiques (bandes magnétiques, disques vinyles, etc.).

personne en temps réel ou reconstituer ses déplacements grâce aux traces laissées par son téléphone portable, mais ce que dit le mode de preuve est identique. Il indique où se trouve une personne à un moment donné. Le raisonnement est le même s'agissant des courriels (qui ne sont que des correspondances), du portrait-robot génétique (qui possède la même fonction que le portrait-robot dessiné) etc.

Ces preuves que l'on qualifie de "numériques", car elles ont recours à un procédé de numérisation, font, en réalité, partie d'une catégorie plus vaste de preuves qui sont obtenues avec l'aide d'une technologie. En cela, elles apparaissent comme nouvelles et donc différentes des preuves classiques. La question se pose de savoir si elles le sont réellement.

D'un point de vue pratique, les différences entre preuves classiques et numériques sont nombreuses et évidentes. Les technologies numériques se répandent à très grande vitesse. D'une part, les acteurs de la justice (la police judiciaire, les magistrats, les experts, les avocats) ont recours à un nombre de plus en plus grand de technologies. Cette évolution est apparue assez nettement à partir des années 80. Ce fut d'abord l'avènement de la photocopie, en matière de preuve documentaire[4], puis les méthodes technologiques de recueil et d'établissement de la preuve ce sont multipliées en matière pénale : empreintes génétiques, interceptions de correspondances, sonorisation, captation d'image, géolocalisation, constitution de fichiers de police et utilisation des logiciels de rapprochement de ces fichiers. Cette évolution n'a pas de limite. Aujourd'hui ce sont les tests d'odeurs et le portrait-robot génétique qui sont en cours de développement. D'autre part, les acteurs extérieurs à l'institution judiciaire possèdent leurs propres preuves numériques qu'il s'agisse des contenus de téléphone portable détenus par les parties, mais également des images de vidéoprotection, que les communes, la SNCF et d'autres personnes publiques détiennent et produisent sur réquisition. Ces preuves peuvent être produites par les parties ou les tiers au procès, de façon volontaire ou sur réquisitions et saisies. De façon plus générale encore, en matière civile, toutes les données stockées dans les systèmes informatiques des entreprises sont susceptibles d'être communiquées en justice, notamment sur le fondement de l'article 145 du Code de procédure civile[5]. Sur autorisation d'un juge, un huissier et un expert en informatique peuvent saisir des données, cloner des disques durs, accéder aux téléphones portables des employés, etc. Ces nouvelles preuves, issues de la technologie numérique, démultiplient les possibilités probatoires. Elles permettent d'obtenir des informations de façon plus simple, plus variée et en plus grand nombre. Cela est significatif en matière pénale. Même pour des délits de moyenne gravité, le volume des preuves numériques contenues dans un dossier s'est considérablement accru ces dernières années.

D'un point de vue juridique, la transformation est beaucoup moins évidente. Si les preuves numériques créent de nouveaux défis, elles posent les mêmes questions que les preuves traditionnelles. En premier lieu, la preuve est-elle licite ? C'est-à-dire respecte-t-elle les principes généraux du droit de la preuve ? En second lieu, l'élément recueilli est-il probant ? C'est-à-dire apporte-t-il une information intelligible et fiable au juge ? Ces deux questions se posent exactement dans les mêmes termes à propos des preuves classiques et nouvelles, qu'elles soient numériques ou de toute autre forme. C'est en ce sens que nous parlons de continuité (I). Toutefois, dans un domaine particulier, les choses se présentent différemment. Il s'agit de l'écrit électronique, de son usage et de la force probante qui lui est accordée. La reconnaissance de cet écrit par le législateur transforme de façon substantielle la manière de contester et de vérifier l'authenticité de cet écrit. Plus récemment, l'irruption de la technologie *blockchain*, pose des questions plus aiguës encore. Sur ce terrain, le juge se trouve confronté, non pas à une preuve dont il perçoit la teneur, mais à une boîte noire. Se profile, alors, un véritable changement de paradigme.

[4] Qui a motivé l'adoption de la loi n° 80-525 du 12 juillet 1980, relative à la preuve des actes juridiques.

[5] Cf. notamment la mise en œuvre de ces mesures en relation avec le secret des affaires, décret n° 2018-1126 du 11 décembre 2018 relatif à la protection du secret des affaires.

I. La continuité : les questions posées par les preuves numériques ne sont pas nouvelles

De façon générale la théorie de la preuve n'a pas été bouleversée par le développement des preuves numériques. Au contraire, la multiplication de ces nouvelles techniques a souvent conduit la Cour de cassation à réaffirmer l'existence de principes ancrés dans le système juridique depuis de nombreuses années et à en densifier le contenu.

L'un de ces principes est le droit au respect de la vie privée appliqué à la matière probatoire. Ce principe est apparu dans la jurisprudence dès les années 70, à propos du constat d'adultère[6]. Mais sa véritable émancipation date du célèbre arrêt *Nikon*, dans lequel la Cour de cassation a jugé illicite la production en justice par l'employeur de courriels personnels échangés par des salariés[7]. Par la suite, le principe a été appliqué de la même manière à des preuves classiques (des rapports d'enquêteurs privés)[8] et à des fichiers numériques[9]. En matière pénale, la première application du droit au respect de la vie privée pour écarter une preuve date de 2007. Il s'agissait en l'espèce de photographies[10], mais l'arrêt ne dit pas si les photos prises par les enquêteurs étaient numériques ou argentiques ! Cette information était d'ailleurs indifférente, car l'atteinte à la vie privée provenait du fait que les enquêteurs avaient photographié l'intérieur d'une propriété privée non visible de l'extérieur. Par la suite, la vie privée en matière pénale a été utilisée, tant à l'égard de preuves classiques[11] qu'en matière de sonorisation et de fixation d'image[12].

Le constat est le même à propos de la loyauté de la preuve. La Cour de cassation utilise ce principe pour contrôler l'usage des preuves numériques. Tel est le cas à propos d'images issues d'une caméra de surveillance[13], de SMS qui s'affichent sur un téléphone portable[14] ou de la production de messages téléphoniques vocaux[15]. Mais la haute juridiction est tout aussi regardante à l'égard du témoignage d'un tiers qui relate le contenu d'une conversation téléphonique[16]. Encore une fois, ce n'est pas la nature de la preuve (numérique ou non) qui est en cause dans ces affaires, mais la manière de recueillir cette preuve (à l'insu de la personne ou au moyen d'un stratagème). En matière pénale, l'affaire la plus célèbre relative à la loyauté de la preuve concerne la sonorisation d'une cellule de garde à vue. La déloyauté du procédé a été posée par l'assemblée plénière de la Cour de cassation[17]. Dans cette affaire, les juges ont censuré un détournement de la procédure de sonorisation, qui constituait, à leurs yeux, un procédé déloyal. Mais la chambre criminelle a utilisé le même raisonnement à propos d'un stratagème qui visait à contourner la procédure de l'interrogatoire de première comparution. En l'espèce, des OPJ[18] avaient consigné dans un procès-verbal de constatation les aveux de la personne mise en examen, alors qu'ils la conduisaient à la maison d'arrêt[19]. Ainsi, que l'aveu soit obtenu par un procédé numérique ou classique importe peu. La Cour de cassation s'attache uniquement à regarder la manière dont le procédé probatoire a été mis en place. Elle s'interroge ainsi sur le fait de savoir s'il y a eu stratagème et tentative de détournement des règles du code de procédure pénale qui protège la personne mise en cause.

---

[6] Cass. civ. 1, 6 févr. 1979, n° 77-13.463.

[7] Cass. soc. 2 oct. 2001, n° 99-42.942.

[8] Cass. civ. 2, 3 juin 2004, n° 02-19.886.

[9] Cass. soc., 12 février 2013, n° 11-28.649, fichiers contenus dans une clé USB.

[10] Cass. crim., 21 mars 2007, n° 06-89.444.

[11] Cass. crim, 22 février 2017, n° 16-82412, pénétration dans un domicile suivant une autorisation de comparution sous la contrainte.

[12] Cass. crim, 6 janvier 2015, n° 14-85448, exigence d'une motivation spéciale.

[13] Cass. civ. 1, 24 septembre 2009, n° 08-19.482.

[14] Cass. soc., 23 mai 2007, n° 06-43.209.

[15] Cass. soc. 6 févr. 2013, n° 11-23.738.

[16] Cass. soc. 16 mars 2011, n° 09-43204, la cour de cassation a jugé que ce témoignage avait été obtenu de façon déloyale.

[17] Cass. ass. plén. 6 mars 2015, n° 14-84.339.

[18] Officiers de police judiciaire.

[19] Cass. crim., 5 mars 2013, n° 12-87.087.

Cette démonstration s'applique à d'autres principes du droit de la preuve. Ainsi, la multiplication des preuves numériques n'a pas modifié l'application du principe du contradictoire ou des droits de la défense. Elle n'a pas changé le principe de liberté de la preuve, ni même le pouvoir d'appréciation souveraine des juridictions du fond. Tous ces principes demeurent solidement inscrits dans le système juridique et les nouveaux modes de preuves doivent s'y conformer, au risque de se voir exclus du dossier ou d'être jugés non probants.

Cette tendance générale à la continuité des règles de droit et à la stabilité du socle juridique qui régissent les preuves ne doit pas masquer l'apparition de zones de turbulences. Lorsque la preuve est numérisée, le juge se trouve parfois confronté à une véritable difficulté : celle de l'intelligibilité de la preuve, qu'il s'agisse de son contenu ou de sa fiabilité.

II. Le changement de paradigme : le juge face à une boîte noire

Le juge se trouve face à une boîte noire, lorsqu'on lui présente une preuve qui est le résultat d'un processus technologie invisible on non intelligible. Par exemple, on lui présente un écrit électronique illisible ou encore une signature électronique qui ne présente pas la forme d'une signature classique. On se trouve alors face à un changement de paradigme, car la représentation de la preuve est radicalement modifiée. Il ne s'agit plus d'une image, d'un son, ou de la localisation d'un individu. Il s'agit simplement d'une suite de chiffres ou de symboles qui n'ont pas de signification immédiate. Ce phénomène est illustré depuis une vingtaine d'années par la signature électronique et plus récemment par la *blockchain*.

La signature électronique : un bouleversement porteur d'insécurité juridique

En 2000, lorsque le législateur a souhaité mettre en conformité le droit de la preuve avec l'apparition du commerce électronique[20], il a introduit dans le code civil la notion d'écrit et de signature électronique. L'objectif était de créer une équivalence entre le support électronique et le support papier. Cette équivalence devait s'exprimer, tant en termes d'admissibilité de la preuve électronique, qu'à l'égard de sa force probante. Pour ce faire, la loi n° 2000-230 du 13 mars 2000 a d'abord proposé une définition très générale de l'écrit, pouvant englober le support papier et électronique[21]. Elle a ensuite posé une double condition à la reconnaissance de la valeur juridique de l'écrit électronique. Il doit être possible d'identifier la personne dont il émane et il doit être établi et conservé dans des conditions de nature à en garantir l'intégrité. Enfin, pour rendre l'écrit parfait, et lui permettre de prouver l'existence d'un acte juridique (généralement un contrat), il doit être signé[22]. Exprimées de façon abstraite, ces conditions ne semblent présenter aucune spécificité. On pourrait même croire à une neutralité parfaite de la loi sur le terrain de la preuve. Toutefois, le législateur – suivant les prescriptions de la directive européenne – a ajouté une présomption de fiabilité du procédé d'identification inhérent à la signature électronique[23]. Cette présomption de fiabilité n'existe pas pour la signature manuscrite. Au contraire, la signature manuscrite est particulièrement fragile au regard de la procédure de contestation d'écriture. L'article 287 du code de procédure civile prévoit que si une partie dénie l'écriture qui lui est attribuée ou déclare ne pas reconnaître celle qui est attribuée à son auteur, le juge doit ordonner une vérification d'écriture. De

[20] Et avec plusieurs directives européennes : la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques et la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »).

[21] Article 1365 du code civil. Il s'agit d'une « suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible ».

[22] Article 1367 du code civil.

[23] Cette présomption s'applique désormais à la signature dite « qualifiée ». *Cf* décret n° 2017-1416 du 28 septembre 2017.

jurisprudence constante, la Cour de cassation décide que cette mesure d'instruction s'impose au juge[24]. Un juge serait ainsi mal inspiré de considérer qu'une dénégation d'écriture n'est pas sérieuse et de refuser le droit à la mesure d'instruction. Sa décision serait automatiquement censurée. La fragilité de la signature manuscrite découle de ce régime juridique, puisqu'il suffit à une partie de dénier toute valeur à la signature qu'on lui oppose, pour se débarrasser de la charge de la preuve et renvoyer au juge le soin de la vérification. Par ailleurs, la procédure de vérification d'écriture est classique. Elle repose, d'une part, sur la confrontation d'écrits et d'autre part, sur une procédure classique d'expertise en écriture.

Le régime de la signature électronique est tout autre. Si le procédé est conforme à l'article 1367 du code civil, elle est présumée fiable et donc opposable à son auteur. Le procédé en question a recours à l'intervention d'un tiers de confiance, qui a en charge d'identifier le signataire, de lui fournir un moyen technique de signature et enfin de vérifier l'intégrité du document[25]. Ce tiers de confiance utilise une procédure, en grande partie informatique, pour certifier que la signature électronique remplit les conditions légales. Ce procédé est externalisé. Le tiers de confiance ne connaît pas le signataire. Il ne l'a pas rencontré. Il s'agit d'un prestataire privé. Les moyens informatiques qu'il met en œuvre ne sont pas, en eux même intelligibles. S'il devait expliquer à un juge sa méthode de certification, il devrait user de schémas et d'explications complexes pour traduire des lignes de Code. Mais l'intégrité de l'opération elle-même est faillible.

Le code civil attribue une présomption de fiabilité à ce mécanisme complexe de certification, qui se déroule à l'extérieur du tribunal et également à l'écart des parties. Mettons-nous à présent dans la peau d'un justiciable, à qui l'on oppose sa signature électronique présumée fiable pour lui réclamer le payement d'une créance. Imaginons que celui-ci estime ne rien devoir, car il n'a rien signé. Sa clé numérique peut avoir été subtilisée. Il peut l'avoir confiée à un collaborateur. Son réseau peut avoir été piraté. Imaginons donc tout un ensemble d'évènements susceptible de perturber l'ensemble du mécanisme, sans même remettre en cause la confiance que l'on place dans le tiers certificateur[26]. La question se pose de savoir ce que peut faire ce justiciable pour renverser la présomption. Il ne peut pas dénier son écriture, car cela ne produira juridiquement aucun effet. Il doit apporter une preuve contraire, mais l'ensemble du processus s'est fait sans son intervention. Il ne dispose d'aucun moyen de preuve pour démontrer que la clé a été subtilisée, mal utilisée, ou encore qu'il est victime d'un piratage. Il sera donc contraint de solliciter en justice une mesure d'instruction. Ici, une nouvelle difficulté va surgir : quelle sera la mesure d'instruction pertinente ? Plus précisément, où doit-on chercher le dysfonctionnement ? Faut-il réaliser des investigations chez le justiciable ou chez le prestataire de service qui certifie la signature ? Peut-on demander à ce dernier de produire des pièces permettant d'avoir l'assurance qu'il a respecté les normes de sécurité ? Et en définitive, dans quelle mesure le juge va-t-il saisir et maîtriser la complexité du processus informatique que le tiers a mis en œuvre pour certifier la signature ?

Aucune de ces questions n'a pour l'instant été résolue. Comme l'indique Jean-François Le Coq[27], la signature électronique a été peu utilisée depuis l'entrée en vigueur de la loi. Plus encore, cette signature n'arrive que très rarement devant la Cour de cassation. Le cadre juridique qui lui est applicable demeure, près de 20 ans après sa mise en place, toujours aussi flou. Les procédés techniques de signature électroniques se sont diversifiés. Certains utilisent des clés USB pour s'identifier. D'autres, après avoir constaté visuellement l'identité des parties, utilisent un code transmis par SMS pour valider la procédure de signature (acte contresigné par avocat, contrats conclus par des assureurs). D'autres encore, comme les notaires, utilisent une signature manuscrite

[24] Cass. civ. 1ère, 7 avr. 1999, n° 97-13.476.

[25] Nous renvoyons à l'étude très claire de Jean-François LE COQ publiée dans ce dossier, et consacrée à la signature électronique.

[26] Celui-ci peut aussi commettre des erreurs.

[27] Dans cette revue.

par stylet sur un écran électronique. Enfin, certains acteurs font signer électroniquement divers contrats (des contrats d'auteurs), par un simple échange de clics dans des mails.
La question se pose à nouveau de savoir comment un juge peut reconnaître un procédé présumé fiable parmi toutes ces techniques. La simple lecture des textes (loi, décrets, arrêtés) ne permet pas de saisir les conditions exactes d'application de cette présomption. Par exemple, l'usage d'un stylet sur une tablette électronique est bien un procédé manuscrit, mais il est numérisé en temps réel et l'identité de l'individu est constatée au moment de la signature par le notaire qui assure l'efficacité de l'acte. Doit-on alors considérer que la signature est électronique, qu'elle est manuscrite, ou encore qu'elle ne suit aucun procédé reconnu par le code civil ?
L'écrit électronique, et la signature électronique qui en est la condition de perfection, constituent de véritables bombes à retardement. Nul ne peut dire aujourd'hui quels seront les procédés reconnus comme probants par la Cour de cassation et, lorsque la présomption sera reconnue à certaines signatures, quelle sera la méthode procédurale pour la combattre. Autant d'incertitude ne convient certainement pas à l'exigence de sécurité juridique qui domine le droit des contrats. Cette insécurité pourrait être sensiblement accrue avec l'irruption récente de la technologie *blockchain.*

La blockchain : une preuve numérique équivoque

La *blockchain* est un procédé numérique qui sert à conserver la preuve d'informations de toutes natures. À l'origine, elle n'a pas été créée dans le but d'être intégrée dans un cadre légal. Au contraire, elle fonctionne dans un réseau de personnes qui opèrent des transactions en dehors d'une reconnaissance juridique. Le cas le plus typique est celui du *bitcoin*, qui est un système à la fois de monnaie, de transactions, mais également de stockages d'informations de toutes natures. En pratique, il est possible de stocker dans une *blockchain*, des informations relatives à contrat, mais aussi tout autre contenu (ex. une œuvre littéraire, le descriptif d'un savoir-faire), pourvu qu'il puisse être codé dans un format numérique. Le document numérique passe dans un processus de « haschage » et il ressort sous la forme d'une « empreinte », c'est-à-dire d'une suite de chiffres. Cette empreinte est inscrite dans un bloc qui contient de nombreuses empreintes et ce bloc prend sa place dans une chaîne de blocs[28].
Sans entrer dans la description technique de ce processus, on peut en retracer diverses caractéristiques en prenant l'exemple d'un contrat qui serait ainsi intégré dans une *blockchain* :
- le contenu du contrat n'est pas enregistré sur cette *blockchain* ; seule son empreinte l'est ;
- l'empreinte ne permet pas de reconstituer le contenu du contrat et donc d'en connaître la teneur ;
- la fiabilité de l'opération d'archivage n'est pas confiée à un prestataire de service de confiance certifié. La *blockchain* fonctionne grâce à un réseau d'acteurs privés, qui détiennent des serveurs informatiques et réalisent des opérations mathématiques ésotériques pour certifier les transactions[29]. La confiance dans ce système repose sur la masse de ces acteurs qui authentifient l'opération contractuelle. Mais certains réseaux d'acteurs font déjà l'objet de luttes de pouvoirs pour détenir la majorité des votes d'authentification, ce qui permet de douter de la fiabilité du système dans son principe même ;
- l'identité de celui qui enregistre le contrat n'est pas connue, car celui-ci opère au moyen d'un pseudonyme.
Toutes ces caractéristiques rendent l'usage de la *blockchain* peu compatible avec les règles de preuve et les pratiques juridictionnelles en la matière. Pour autant, cette technologie se développe à grands pas et nombreux sont les acteurs qui défendent son utilisation comme preuve dans les revues juridiques[30]. Les juristes, quant à eux, demeurent sur la réserve[31]. Malgré cela, on a tout de même

[28] Une suite de registres d'informations numériques.
[29] Ils résolvent des problèmes mathématiques complexes pour être mis en concurrence.
[30] Bien que ces acteurs ne soient pas toujours juristes. *Cf* par ex. Clément BERGÉ-LEFRANC, « La blockchain est une technologie très efficace pour se préconstituer une preuve », entretien *in Revue Lamy Droit civil*, n° 150, 1er juillet 2017.
[31] *Cf*, notamment, les opinions émises par les auteurs du dossier « Preuve et blockchain *», Dalloz IP/IT*, 2019, p. 73 et suiv. *cf* également l'étude de Thibault DOUVILLE, « Blockchains et preuve », *Recueil Dalloz*, 2018, p. 2193.

trouvé des parlementaires assez imprudents pour proposer que les opérations effectuées au sein d'une *blockchain* soient assimilées à des actes authentiques[32]. La force probante de la *blockchain* repose, en réalité, sur la structure du système de confiance qui existe sur le réseau. Le procédé de cryptographie qui permet d'introduire les éléments dans la *blockchain*, puis le système de validation par une majorité de plus de 50% des acteurs de ce réseau donne à ce processus de nombreux attraits. Toutefois au regard du cadre juridique français, il pose de nombreuses questions.

D'une part, sur le terrain de la preuve des actes juridiques, la *blockchain* ne remplit pas les conditions d'admissibilité posées par le code civil. D'abord, le procédé est loin d'être intelligible[33]. Ensuite, aucun élément ne permet d'identifier le signataire de l'acte. Seule l'existence de l'acte est inscrite dans la *blockchain* par une personne utilisant un pseudonyme. Cette personne peut introduire dans la *blockchain* n'importe quelle transaction, sans même que les parties désignées dans l'acte n'en soient informées. Enfin, le prestataire de service de confiance est absent du processus de la *blockchain*. Dès lors, la *blockchain* ne présente pas les caractéristiques d'une preuve électronique dont la signature serait présumée fiable. On peut même lui dénier le caractère d'écrit sous seing privé, puisque la signature n'est pas un élément intrinsèque à l'inscription d'un contrat dans une *blockchain*. Ainsi, quelle que soit la confiance qu'elle inspire aux acteurs économiques, sa valeur juridique demeure faible.

Dans un système de preuve libre, les choses sont différentes. Le juge n'a aucune raison de rejeter *a priori* un document issu d'une *blockchain*. Toutefois, ce document n'est pas intelligible en lui-même. Il s'agit d'une empreinte numérique issue d'une procédure de codage d'un document et cette empreinte ne permet pas de remonter jusqu'au document. En effet, le codage ne peut avoir lieu que dans un sens. Le document produit l'empreinte et l'empreinte ne produit rien. Pour retrouver le document, il faut réaliser une opération complexe. Celui qui prétend avoir archivé le document doit détenir une « clé » (un code secret) et une copie du document dont il se prévaut en justice. Avec cette copie et cette clé, il doit procéder à un nouveau codage de la copie dans la *blockchain*. Si ce codage génère une empreinte identique à celle qu'il possède déjà, cela signifie que la copie du document est conforme à l'original dont il se prévaut. La copie peut être produite en justice et être jugée conforme à l'original. Ce processus est loin d'être simple et il ne peut être réalisé qu'avec l'aide d'un huissier ou au moyen d'une mesure d'expertise judiciaire. Pour le juge, le processus se déroule à l'aveugle. Il ne voit pas le document qui a été archivé dans la *blockchain* et ne peut rien déduire de l'empreinte qu'on lui présente. Il doit simplement reconnaître à *l'issue* du processus que la copie qu'on lui présente est conforme à l'original qui a été codé et archivé dans la *blockchain*.

À l'issue de ce processus probatoire qui nécessite l'intervention d'un auxiliaire traditionnel de la justice (un huissier, un expert), le juge peut finir par être convaincu qu'une copie produite en justice est conforme à l'original. La *blockchain* n'a donc pas une force probante intrinsèque. Cette force est dépendante de modes de preuves traditionnels. De surcroît, sa valeur probante dépend de la capacité du juge à comprendre le processus de stockage et de déstockage du document. Elle dépend également de la confiance que le juge souhaite accorder à ce processus et à la *blockchain* elle-même.

Présentée comme économiquement peu coûteuse et comme technologiquement très fiable, la technique de préconstitution des preuves par *blockchain* remet en cause les principes essentiels de la preuve, en particulier lorsqu'il s'agit de prouver un acte juridique. Elle constitue un véritable changement de paradigme, car elle contient en elle-même un bouleversement des pratiques juridictionnelles. Elle demande au juge de croire ce qu'il ne peut pas voir, de faire confiance en l'absence d'un tiers de confiance, et de reconnaître l'identité d'un signataire qui a utilisé un pseudonyme. Autant de bouleversements qui nécessiteront, à l'avenir, l'intervention du législateur, pour donner à la *blockchain* un statut juridique spécifique si l'on souhaite qu'elle accède à la fonction probatoire à laquelle elle prétend.

[32] Cet amendement est cité par Mustapha MEKKI, *in* « Les mystères de la blockchain », *Recueil Dalloz*, 2017, p. 2160.

[33] En ce sens, déjà, Mustapha MEKKI, *précit*.