PREUVES ÉLECTRONIQUES DANS LES PROCÉDURES CIVILES ET ADMINISTRATIVES

Instruments juridiques

Lignes directrices
et exposé des motifs

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

PREUVES ÉLECTRONIQUES DANS LES PROCÉDURES CIVILES ET ADMINISTRATIVES

Lignes directrices
adoptées par le Comité des Ministres
du Conseil de l'Europe
le 30 janvier 2019
et exposé des motifs

Conseil de l'Europe

Édition anglaise :

Electronic evidence in civil and administrative proceedings (Guidelines and explanatory memorandum)
ISBN 978-92-871-8929-5

Couverture et mise en page : Service de la production des documents et des publications (SPDP), Conseil de l'Europe

Éditions du Conseil de l'Europe
F-67075 Strasbourg Cedex
http://book.coe.int

ISBN 978-92-871-8928-8

Imprimé dans les ateliers du Conseil de l'Europe

Les Lignes directrices du Comité des Ministres aux États membres sur les preuves électroniques dans les procédures civiles et administratives ont été adoptées par le Comité des Ministres du Conseil de l'Europe le 30 janvier 2019, sur proposition du Comité européen de coopération juridique (CDCJ).

Cette publication contient les lignes directrices et leur exposé des motifs.

Table des matières

Lignes directrices

du Comité des Ministres aux États membres sur les preuves électroniques dans les procédures civiles et administratives

(adoptées par le Comité des Ministres le 30 janvier 2019, lors de la 1335e réunion des Délégués des Ministres)

Le Comité des Ministres,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses États membres, notamment en encourageant l'adoption de règles communes en matière juridique ;

Considérant la nécessité de fournir des conseils pratiques aux juridictions et autres autorités compétentes exerçant des fonctions juridictionnelles, aux professionnels, y compris aux praticiens du droit, et aux parties à la procédure, sur le traitement des preuves électroniques dans les procédures civiles et administratives ;

Considérant que ces lignes directrices visent davantage à l'établissement d'un cadre commun qu'à l'harmonisation des législations nationales des États membres ;

Considérant la nécessité de respecter la diversité des systèmes juridiques des États membres ;

Reconnaissant les avancées réalisées au sein des États membres dans la numérisation de leur système judiciaire ;

Notant, cependant, les obstacles auxquels se heurte la gestion efficace des preuves électroniques dans les systèmes judiciaires, comme l'absence de normes communes et la diversité et la complexité des procédures d'administration de la preuve ;

Soulignant la nécessité de faciliter l'utilisation des preuves électroniques dans les systèmes juridiques et la pratique juridictionnelle ;

Reconnaissant la nécessité pour les États membres d'examiner les lacunes actuelles dans l'utilisation des preuves électroniques et d'identifier les domaines dans lesquels les principes et la pratique en matière de preuves électroniques pourraient être mis en place ou améliorés ;

Notant que le but de ces lignes directrices est de fournir des solutions pratiques pour combler les lacunes actuelles du droit et de la pratique,

Adopte les lignes directrices ci-après, conçues comme un outil pratique destiné aux États membres, pour les aider à adapter le fonctionnement de leurs mécanismes – judiciaires ou autres – de règlement des litiges afin de remédier aux problèmes que posent les preuves électroniques dans les procédures civiles et administratives, et les invite à diffuser largement ces lignes directrices pour qu'elles soient mises en œuvre par quiconque est responsable du traitement des preuves électroniques ou assure autrement ce dernier.

Objet et champ d'application

Les lignes directrices portent sur :

- le recueil à distance des preuves orales ;
- l'utilisation des preuves électroniques ;
- la collecte, la saisie et la transmission de preuves ;
- la pertinence ;
- la fiabilité ;
- le stockage et la conservation ;
- l'archivage ;
- la sensibilisation, le suivi, la formation et l'éducation.

Les lignes directrices ne doivent pas être perçues comme un moyen de conférer une valeur probante particulière à certains types de preuves électroniques et ne doivent s'appliquer que dans la mesure où elles n'entrent pas en conflit avec la législation nationale.

Les lignes directrices ont pour but de faciliter l'utilisation et la gestion des preuves électroniques dans les systèmes juridiques et dans la pratique juridictionnelle.

Définitions

Aux fins des présentes lignes directrices :

Preuve électronique

On entend par « preuve électronique » toute preuve qui découle de données contenues ou produites par un dispositif dont le fonctionnement dépend d'un logiciel ou de données stockées ou transmises sur un système ou un réseau informatique.

Métadonnées

On entend par « métadonnées » les informations électroniques relatives à d'autres données électroniques, susceptibles de révéler l'identité de l'auteur, l'origine ou l'historique de la preuve, ainsi que les dates et heures concernées.

Service de confiance

On entend par « service de confiance » un service électronique qui consiste :

a. en la création, la vérification et la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; ou

b. en la création, la vérification et la validation de certificats pour l'authentification de site internet ; ou

c. en la conservation de signatures électroniques, de cachets électroniques ou de certificats relatifs à ces services.

Juridiction

Le terme « juridiction » inclut toutes autorités compétentes exerçant des fonctions juridictionnelles qui les amènent à traiter des preuves électroniques.

Principes fondamentaux

Il appartient aux juridictions de se prononcer sur l'éventuelle valeur probante des preuves électroniques, conformément au droit interne.

Les preuves électroniques devraient être appréciées de la même manière que les autres types de preuves, en particulier pour ce qui est de leur recevabilité, leur authenticité, leur exactitude et leur intégrité.

Le traitement des preuves électroniques ne devrait pas être défavorable aux parties ni donner à l'une d'elles un avantage indu.

Lignes directrices

Le recueil à distance des preuves orales

1. Le recueil des preuves orales peut se faire à distance, grâce à des dispositifs techniques, si la nature des preuves le permet.

2. Pour déterminer si le recueil à distance des preuves orales est possible, les juridictions devraient tenir compte notamment des facteurs suivants :

- l'importance de la preuve ;
- le statut de la personne qui témoigne ;
- la sécurité et l'intégrité de la liaison vidéo grâce à laquelle le témoignage doit être transmis ;
- les coûts et les difficultés occasionnés par la comparution de l'intéressé devant la juridiction.

3. Lorsque les preuves sont recueillies à distance, il est indispensable de veiller à ce que :

a. la transmission des preuves orales puisse être vue et écoutée par les personnes participant aux débats ainsi que par le public lorsque les débats lui sont ouverts ; et

b. la personne qui est entendue à distance puisse voir et écouter les débats autant que nécessaire afin de s'assurer que la procédure est équitable et effective.

4. La procédure et les technologies appliquées au recueil de preuves à distance ne devraient pas compromettre la recevabilité de ces preuves et la capacité de la juridiction à établir l'identité des personnes concernées.

5. Que la preuve soit transmise au moyen d'une connexion privée ou publique, il convient d'assurer la réalisation d'une visioconférence de qualité et de crypter les signaux vidéo pour les protéger de toute interception.

Utilisation des preuves électroniques

6. Les juridictions ne devraient pas refuser les preuves électroniques et ne devraient pas les priver d'effet juridique au simple motif qu'elles ont été collectées et/ou présentées sous forme électronique.

7. Les juridictions ne devraient pas, en principe, priver les preuves électroniques d'effet juridique au simple motif de l'absence d'une signature électronique avancée, qualifiée ou sécurisée de manière équivalente.

8. Les juridictions devraient être conscientes de la valeur probante des métadonnées et des éventuelles conséquences de leur non-utilisation.

9. Les parties devraient être autorisées à présenter des preuves électroniques dans leur format électronique original, sans qu'il soit nécessaire d'en fournir une version imprimée.

Collecte, saisie et transmission

10. Les preuves électroniques devraient être collectées de manière appropriée et sûre, et transmises aux juridictions au moyen de services fiables, comme les services de confiance.

11. Comme le risque de destruction ou de perte éventuelle est plus élevé pour les preuves électroniques que pour les preuves non électroniques, les États membres devraient mettre en place des procédures de saisie et de collecte des preuves électroniques qui soient sûres.

12. Les juridictions devraient avoir conscience des problèmes particuliers qui se posent à l'occasion de la saisie et de la collecte des preuves électroniques à l'étranger, notamment dans les affaires transfrontières.

13. Les juridictions devraient coopérer au recueil transfrontière de preuves. La juridiction qui fait l'objet de la demande devrait informer la juridiction qui adresse cette demande de toutes les conditions, y compris des restrictions, auxquelles est soumise la collecte de preuves par la juridiction sollicitée.

14. Les preuves électroniques devraient être collectées, organisées et gérées de manière à faciliter leur transmission à d'autres juridictions, en particulier aux juridictions d'appel.

15. Il convient d'encourager et de faciliter la transmission des preuves électroniques par des moyens électroniques afin d'améliorer l'efficacité des procédures judiciaires.

16. Les systèmes et les dispositifs utilisés pour la transmission des preuves électroniques devraient être en mesure d'en préserver l'intégrité.

Pertinence

17. Les juridictions devraient prendre part à la gestion active des preuves électroniques pour, en particulier, éviter la production ou la demande excessive ou spéculative de preuves électroniques.

18. Les juridictions peuvent demander à des experts d'analyser des preuves électroniques, notamment lorsque des questions complexes sont soulevées en matière de preuve ou en cas d'allégations de manipulation des preuves électroniques. Il devrait appartenir aux juridictions de juger si ces experts disposent d'une expertise suffisante en la matière.

Fiabilité

19. En matière de fiabilité, les juridictions devraient prendre en compte tous les facteurs pertinents à propos de la source et de l'authenticité des preuves électroniques.

20. Les juridictions devraient avoir conscience de l'intérêt que présentent les services de confiance pour établir la fiabilité des preuves électroniques.

21. Dans la mesure où le système juridique national le permet, et sous réserve de l'appréciation de la juridiction, les données électroniques devraient être admises à titre de preuve, sauf si l'une des parties conteste l'authenticité de ces données.

22. Dans la mesure où le système juridique national le permet, et sous réserve de l'appréciation de la juridiction, les données électroniques devraient bénéficier d'une présomption de fiabilité, sous réserve que l'identité du signataire puisse être validée et que l'intégrité des données puisse être assurée, à moins qu'il n'existe des motifs raisonnables de penser le contraire.

23. Lorsque la législation applicable accorde une protection spéciale à des catégories de personnes vulnérables, cette législation devrait primer sur les présentes lignes directrices.

24. Dans la mesure où le système juridique national le prévoit, lorsqu'une autorité publique transmet des preuves électroniques indépendamment des parties, leur contenu a valeur probante, sauf démonstration du contraire.

Stockage et conservation

25. Les preuves électroniques devraient être stockées de manière à en préserver la lisibilité, l'accessibilité, l'intégrité, l'authenticité, la fiabilité et, le cas échéant, la confidentialité et le respect de la vie privée.

26. Les preuves électroniques devraient être stockées accompagnées de métadonnées normalisées, de manière à préciser clairement le contexte de leur production.

27. La lisibilité et l'accessibilité des preuves électroniques stockées devraient être garanties dans le temps, en tenant compte de l'évolution des technologies de l'information.

Archivage

28. Les juridictions devraient archiver les preuves électroniques conformément à la législation nationale. Les archives électroniques devraient satisfaire à toutes les exigences de sécurité et garantir l'intégrité, l'authenticité, la confidentialité et la qualité des données, ainsi que le respect de la vie privée.

29. L'archivage des preuves électroniques devrait être effectué par des spécialistes qualifiés.

30. Afin de préserver l'accessibilité des preuves électroniques, les données devraient, au besoin, être transférées vers de nouveaux supports de stockage.

Sensibilisation, suivi, formation et éducation

31. Les États membres devraient promouvoir la sensibilisation aux avantages et à l'intérêt des preuves électroniques dans les procédures civiles et administratives.

32. Les États membres devraient assurer un suivi des normes techniques relatives aux preuves électroniques.

33. Tous les professionnels confrontés à des preuves électroniques devraient avoir accès à la formation interdisciplinaire nécessaire sur le traitement de ces preuves.

34. Les juges et les praticiens du droit devraient avoir conscience de l'évolution des technologies de l'information susceptibles d'avoir des répercussions sur la disponibilité et l'intérêt des preuves électroniques.

35. L'enseignement du droit devrait comporter des modules consacrés aux preuves électroniques.

Exposé des motifs

Observations d'ordre général

Les raisons d'un nouvel instrument

1. Les juridictions sont de plus en plus appelées à traiter des preuves électroniques ou à autoriser la production de données électroniques par les parties et les autres personnes concernées par les procédures civiles ou administratives.

2. À ce jour, les normes relatives aux preuves électroniques aux niveaux international, européen et national sont rares. Le droit et la pratique en matière de preuves électroniques présentent d'importantes lacunes.

3. Les présentes lignes directrices sur les preuves électroniques n'ont pas pour objectif d'établir des normes juridiques contraignantes ; elles sont plutôt conçues comme un outil pratique destiné à permettre aux États membres du Conseil de l'Europe d'adapter le fonctionnement de leurs mécanismes judiciaires et autres mécanismes de règlement des litiges, afin de remédier aux problèmes que posent les preuves électroniques. À cet égard, les lignes directrices ont été établies pour renforcer l'efficacité et la qualité de la justice.

4. Les preuves électroniques se distinguent à bien des égards des autres types de preuves, et les juridictions et autres autorités compétentes exerçant des fonctions juridictionnelles confrontées aux preuves électroniques se heurtent à des difficultés particulières. Ces difficultés soulignent à quel point il est indispensable de mieux connaître les preuves électroniques et d'améliorer leur traitement dans les procédures civiles et administratives.

Méthode de travail et processus d'élaboration

5. La question des preuves électroniques relève de la compétence du Comité européen de coopération juridique (CDCJ), l'organe intergouvernemental du Conseil de l'Europe chargé des activités normatives de l'Organisation dans le domaine du droit public et privé, dont le droit civil et administratif.

6. Les lignes directrices ont été élaborées par un groupe de rédaction de membres du CDCJ et d'experts désignés, et reposent sur les propositions qu'ils ont formulées au cours des réunions que le groupe a tenues en 2018. À ces réunions ont également participé les organes pertinents du Conseil de l'Europe ayant la compétence et l'expertise dans ce domaine.

7. Le groupe de rédaction a tenu compte de l'expérience tirée du fonctionnement des mécanismes de justice électronique qui existent déjà dans les États membres.

Exemples dans des États membres

- Un système de justice électronique – *Lietuvos teismų informacinė sistema* (LITEKO) – a été mis en place en **Lituanie** en 2004. LITEKO a entraîné une diminution des dossiers en format papier en permettant aux parties à la procédure de soumettre l'ensemble des documents procéduraux en ligne et d'y suivre l'évolution de l'affaire.
- Un registre du commerce et un registre foncier électroniques ainsi qu'un système intégré de suivi des affaires (« eSpis ») sont en cours de développement en **Croatie**. eSpis facilitera la communication électronique entre les juridictions et les parties à la procédure.

Structure et contenu

8. Les lignes directrices ne représentent pas seulement une déclaration de principes ; elles visent aussi à donner des conseils pratiques.

Préambule

9. Le préambule explique que les lignes directrices sont uniquement applicables dans la mesure où elles ne sont pas contraires à la législation nationale et qu'elles forment un instrument non contraignant. Elles ne cherchent pas à harmoniser la législation nationale des États membres. Les lignes directrices ne doivent pas s'interpréter comme conférant une valeur juridique particulière à certaines formes de preuves électroniques. Elles sont conçues de manière suffisamment générale pour s'adapter aux différences dans les systèmes juridiques des États membres dont la diversité est pleinement reconnue.

Objet et champ d'application

10. Les lignes directrices visent à apporter une solution aux difficultés particulières que présentent les preuves électroniques, comme l'éventuelle valeur

probante des métadonnées, la facilité avec laquelle les preuves électroniques peuvent être manipulées, altérées et effacées, et la participation des tiers (y compris celle des fournisseurs de services de confiance) dans la collecte et la saisie des preuves électroniques. Les lignes directrices sont applicables au règlement de litiges par des procédures aussi bien civiles qu'administratives.

Exemple dans un État membre

En **Slovaquie,** les services administratifs sont prêts à examiner les preuves électroniques en application du principe selon lequel tout élément ayant valeur probante peut, en vue de déterminer la réalité de la situation, être présenté à titre de preuve, sous réserve qu'il n'ait pas été obtenu en infraction à la législation.

Définitions

Preuve électronique

11. Les lignes directrices retiennent une définition large des « preuves électroniques » (également dénommées « preuves numériques »). Celles-ci peuvent prendre la forme de textes, de vidéos, de photos ou de contenus sonores. Les données peuvent provenir de différents supports ou d'accès, comme les téléphones portables, les pages internet, les ordinateurs de bord ou les enregistreurs GPS ; elles peuvent également être conservées dans un espace de stockage qui échappe au contrôle de la partie concernée. Les messages électroniques (courriels) offrent un parfait exemple de preuves électroniques, puisqu'ils proviennent d'un dispositif électronique (ordinateur ou appareils de type informatique) et comportent des métadonnées pertinentes (voir la définition de « métadonnées » ci-dessous).

Métadonnées

12. Les « métadonnées » désignent des données qui portent sur d'autres données, et elles peuvent être qualifiées d'« empreintes numériques » d'une preuve électronique. Elles peuvent comporter des données probantes importantes, comme la date et l'heure de la création ou de la modification d'un fichier ou d'un document, ou l'auteur et la date et l'heure de l'envoi des données. Les métadonnées ne sont habituellement pas directement accessibles.

Service de confiance

13. Les services de confiance jouent un rôle crucial dans l'identification, l'authentification et la sécurité des transactions en ligne. Les lignes directrices

adoptent la définition du « service de confiance » telle que formulée à l'article 3.16, du Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (le règlement eIDAS). Les présentes lignes directrices mentionnent également les services de confiance particuliers liés aux signatures et certificats électroniques « simples », « avancés » ou « qualifiés », ce qui suppose l'application possible d'autres définitions adoptées dans le règlement eIDAS.

Juridiction

14. Les lignes directrices retiennent une définition large de « juridiction » afin de s'appliquer à l'ensemble des autorités compétentes pour statuer dans les litiges juridiques entre les parties aux procédures civiles et administratives, comme les cours, les tribunaux ou les instances administratives.

Principes fondamentaux

15. Le premier principe précise que, malgré le rôle important joué par les experts dans l'évaluation des preuves électroniques, il appartient en définitive aux juridictions de décider de l'éventuelle valeur probante de ce type de preuves. Pour ce faire, les juridictions peuvent être liées par les présomptions légales applicables (qui confèrent, par exemple, une valeur probante particulière à certains types de preuves électroniques).

16. Le deuxième principe souligne que les preuves électroniques ne font l'objet d'aucune discrimination et ne bénéficient d'aucun privilège par rapport aux autres types de preuves. À ce propos, il importe que les juridictions adoptent une approche neutre du point de vue de la technologie utilisée, ce qui signifie que toute technologie qui prouve l'authenticité, l'exactitude et l'intégrité des données devrait être acceptée.

> Jurisprudence de la Cour européenne des droits de l'homme
>
> « Par ailleurs, si la Convention garantit en son article 6 le droit à un procès équitable, elle ne réglemente pas pour autant l'admissibilité des preuves ou leur appréciation, matière qui relève dès lors au premier chef du droit interne et des juridictions nationales. » (voir *García Ruiz c. Espagne,* n° 30544/96, paragraphe 28).

17. Le troisième principe évoque l'égalité des armes et l'égalité de traitement des parties à la procédure en matière de preuves électroniques. Le traitement des preuves électroniques ne devrait pas être défavorable aux parties à une

procédure civile ou administrative. Par exemple, une partie ne devrait pas être privée de la possibilité de contester l'authenticité d'une preuve électronique ; ou si une juridiction n'admet la soumission par une partie que de versions imprimées des preuves électroniques, cette partie ne devrait pas être privée de la possibilité de soumettre les métadonnées pertinentes afin de prouver la fiabilité des versions imprimées.

Jurisprudence de la Cour européenne des droits de l'homme

« Le principe de l'égalité des armes … suppose que chaque partie dispose d'une possibilité raisonnable de présenter sa cause – y compris ses éléments de preuve – dans des conditions qui ne la placent pas dans une situation de net désavantage par rapport à son adversaire. » (voir *Letinčić c. Croatie,* n° 7183/11, paragraphe 48).

Lignes directrices

Recueil à distance des preuves orales

18. Les preuves orales recueillies par liaison/connexion à distance sont considérées comme des preuves électroniques aux fins des présentes lignes directrices (voir la définition de « preuve électronique » ci-dessus). Cette partie des lignes directrices ne prend pas en compte cependant les témoignages oraux enregistrés au préalable. Elle concerne l'audition de témoins effectuée sous forme de visioconférence (ou vidéoconférence) (transmission de l'image et du son synchronisés en temps réel). Tous les témoignages oraux ne peuvent pas être recueillis au moyen d'une liaison à distance. Il convient d'être attentif aux dispositifs techniques utilisés pour la transmission des témoignages à distance. Ce recueil de témoignage oral peut être effectué à distance grâce à des dispositifs techniques analogiques ou numériques qui permettent la transmission de télécommunications, en particulier la communication bilatérale en temps réel permettant la transmission de l'image et du son. Si le témoignage exige la confidentialité, il peut s'avérer nécessaire d'appliquer des mesures ou des solutions techniques qui assurent l'accès à une forme intelligible de communication sûre aux seules personnes autorisées. Les dispositifs qui garantissent l'intégrité des télécommunications donnent à la juridiction et aux parties une possibilité satisfaisante de contredire et d'interroger le témoin « à distance ».

Exemples de l'Union européenne et de législation nationale dans un État membre

– L'article 10.4 du Règlement (CE) n° 1206/2001 du Conseil du 28 mai 2001 relatif à la coopération entre les juridictions des États membres dans le domaine de l'obtention des preuves en matière civile ou commerciale prévoit que la

juridiction requérante peut demander à la juridiction requise de recourir aux technologies de communication modernes pour procéder à l'acte d'instruction, en particulier à la vidéoconférence et à la téléconférence.

– L'article 803 du Code de procédure civile **lituanien** prévoit que les juridictions de la République de Lituanie peuvent demander à une juridiction étrangère d'utiliser les technologies de communication (comme la visioconférence) pour l'audition de témoins.

19. Les facteurs déterminants de l'audition de témoins au moyen d'une liaison à distance sont des considérations économiques (par exemple, la réduction des coûts induits), des difficultés pratiques (par exemple, la maladie ou le handicap d'un témoin) et les mesures d'efficacité procédurale prises pour éviter la durée excessive des procédures. Si une personne est domiciliée dans un autre pays, il peut être plus opportun de l'interroger à distance. Le même principe vaut pour un groupe de témoins qui résident tous dans une localité distante de la circonscription judiciaire de la juridiction qui examine l'affaire. Si l'intéressé est un témoin essentiel, il peut être plus judicieux de l'interroger au tribunal. Les autres facteurs à prendre en compte par les juridictions sont la participation et le coût des traducteurs qui interviennent lors de l'audition. Il importe que les juges, les professionnels, y compris les praticiens du droit, et le personnel judiciaire soient conscients des différences entre le témoignage en personne et le témoignage à distance. Il est, par exemple, moins facile d'observer et d'interpréter le comportement du témoin lors d'une audition à distance.

20. Ces lignes directrices exigent d'être attentif au procédé utilisé pour l'audition du témoin à distance. Il importe, en particulier lorsque le témoignage est crucial pour la résolution d'une affaire, de veiller à ce que la technologie utilisée permette de poser des questions au moment où le témoin dépose (si les dispositions de la procédure le prévoient). Cette exigence ne peut pas être respectée lorsque la transmission est altérée en raison d'une faible connexion ou si l'accès aux moyens techniques est limité pour les parties. Cela peut conférer un avantage indu à l'une des parties. Lorsqu'elle est techniquement possible, l'audition de témoins à distance devrait être effectuée de la même manière que si elle avait lieu à l'intérieur du tribunal.

21. Les méthodes utilisées devraient préserver de manière satisfaisante la transmission de l'image ou du son de toute perte, altération ou divulgation non autorisée. La juridiction peut vérifier l'identité du témoin auditionné en lui demandant de présenter un document adéquat, comme une carte d'identité, un passeport ou un permis de conduire valides.

22. Tous les systèmes de communication disponibles, qu'ils soient publics ou privés, devraient garantir au moins la qualité de la visioconférence et le cryptage des signaux vidéo, afin de les protéger de toute interception. Il est possible de visionner un témoin au moyen d'une connexion privée, si la législation nationale le permet, sous réserve que les solutions utilisées offrent suffisamment de sécurité technique et respectent les garanties de la procédure. On entend ici par connexion privée un système de communication qui n'est pas un système administratif officiel spécialement créé pour l'audition de témoins par une juridiction.

Utilisation des preuves électroniques

23. Il importe que les juridictions soient conscientes de l'importance des données électroniques présentées par les parties à titre de preuve dans leur forme originale. Si une version imprimée d'une preuve électronique est déposée, la juridiction peut ordonner, à la demande d'une partie ou de sa propre initiative, que l'intéressé lui fournisse l'original de la preuve électronique. Les données de géolocalisation offrent un exemple de preuves qui peuvent avoir une grande importance pour la résolution d'une question, à condition d'être présentées dans leur forme originale. La plupart des juridictions du monde disposent déjà d'une législation qui prévoit expressément l'utilisation des preuves électroniques dans les procédures judiciaires. Le règlement eIDAS illustre ce type de dispositions.

Exemples

La Cour suprême de **Croatie** (affaire n° I Kž 696/04-7) a confirmé que les messages SMS pouvaient tenir lieu de preuve dans les procédures car ils représentent une source d'information égale à tout autre contenu écrit conservé sur un autre support.

Exemple de technologie utilisée tout spécialement pour sécuriser les preuves : blockchain

Une blockchain est une nouvelle technologie capable de renforcer la confiance à l'égard des preuves électroniques et la sécurité de ces dernières. Elle peut se définir comme un registre mis en distribution, qui renvoie vers une liste d'enregistrements (ensembles ou blocks) liés entre eux et sécurisés à l'aide d'une cryptographie, qui sont enregistrés sur un réseau décentralisé de pair à pair. De par sa conception, une blockchain résiste foncièrement à toute modification des données. Une fois enregistrées, les données d'un ensemble déterminé ne peuvent être modifiées rétroactivement sans altérer tous les ensembles ultérieurs, ce qui exige l'accord de la majorité du réseau. Une blockchain est donc adaptée à l'administration de la preuve.

Aux **États-Unis**, l'article 1913 du Règlement relatif aux éléments de preuve de l'État du Vermont est libellé comme suit : « (1) Un fichier numérique enregistré en format électronique sur une liste d'enregistrements (blockchain) présente un caractère authentique conformément à l'article 902 du Règlement relatif aux éléments de preuve de l'État du Vermont s'il s'accompagne d'une déclaration écrite faite sous serment par une personne qualifiée, qui indique la qualification de l'auteur de la certification et (a) la date et l'heure auxquelles le fichier a été inséré dans la liste d'enregistrements ; (b) la date et l'heure auxquelles le fichier a été obtenu de la liste d'enregistrements ; (c) le fait que la conservation du fichier dans la liste d'enregistrements s'inscrit dans le cadre d'une activité habituelle ; et (d) que cette activité habituelle confère à ce fichier la qualité de pratique habituelle. »

En **Chine**, dans un arrêt du 28 juin 2018, le tribunal de Hangzhou compétent pour les questions relatives à internet a estimé, dans l'affaire qu'il jugeait (un litige de propriété intellectuelle), que les données stockées dans une plate-forme de liste d'enregistrements (blockchain) étaient suffisamment fiables et exemptes d'interférence pour pouvoir être invoquées comme preuve et acceptées comme telles par le tribunal.

24. Aux fins de la ligne directrice 7, il faut entendre par « signature électronique avancée » une signature électronique qui satisfait aux exigences de l'article 26 du règlement, à savoir : (a) être liée au signataire de manière univoque ; (b) permettre d'identifier le signataire ; (c) avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et (d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable. Il faut entendre par « signature électronique qualifiée » une signature électronique avancée qui a été créée à l'aide d'un dispositif spécifique à cette fin (« dispositif de création de signature électronique qualifiée »). Ces dispositifs doivent avoir obtenu un « certificat qualifié de signature électronique » qui est un certificat délivré par une personne physique ou morale qui fournit un ou plusieurs services de confiance qualifiés (« prestataire de services de confiance qualifié ») et qui est autorisée par l'organe de contrôle à le faire.

25. Dans la pratique actuelle, la plupart des données électroniques sont dépourvues de signatures électroniques avancées ou qualifiées et ne sont pas sécurisées par d'autres moyens. Les juridictions devraient néanmoins continuer à les considérer comme des preuves électroniques (même si la valeur probante de la preuve varie en fonction de chaque situation), compte tenu, par exemple, de la diversité des services de confiance liés à la gestion électronique des documents et à l'identification des signataires qui existent à travers le monde. La signature biométrique en offre un exemple : il s'agit

d'une méthode qui permet à une personne d'obtenir la version électronique d'une signature manuscrite lorsqu'elle appose sa signature sur un appareil électronique à l'aide d'un stylo et d'une tablette spéciaux. Selon la législation applicable, la juridiction peut reconnaître que cette signature biométrique est équivalente à une signature manuscrite sur papier.

26. Les métadonnées fournissent le contexte nécessaire à l'appréciation de la preuve (c'est-à-dire des données), tout comme le cachet de la poste offre un élément contextuel pour l'appréciation d'un courrier ordinaire (en version papier) et de son contenu. Les preuves électroniques comportent systématiquement des métadonnées, et les juridictions devraient avoir conscience de la valeur probante qu'elles peuvent avoir. Elles permettent de retrouver la trace et d'identifier la source et la destination d'une communication, les données relatives au dispositif qui a généré la preuve électronique, la date, l'heure, la durée et le type de preuve. Les métadonnées peuvent être importantes, soit comme preuve indirecte (par exemple lorsqu'elles indiquent la version la plus pertinente d'un document), soit comme preuve directe (par exemple lorsque les données d'un fichier sont manipulées). Cette ligne directrice présente également un intérêt en cas de perte des métadonnées.

Exemples de jurisprudence relative aux métadonnées en **Irlande**

Les métadonnées ont été jugées importantes pour l'authentification de la provenance de documents ou de contenus créés par voie électronique (*Koger Inc. & Koger (Dublin) Ltd c. O'Donnell & Others* (2010) IEHC 350).

Les juridictions irlandaises ont conclu à une obligation pour une partie à la procédure civile d'informer l'autre (les autres) partie(s) des éléments de preuve stockés par des moyens électroniques qui contiennent (divulgation) les métadonnées des documents originaux, lorsque celles-ci présentent un intérêt (*Sretaw c. Craven House Capital PLC* (2017) IEHC 580 ; *Gallagher c. RTE* (2017) IEHC 237).

27. Les versions imprimées des preuves électroniques peuvent être facilement manipulées, car elles sont dépourvues de métadonnées ou d'autres données cachées. Par conséquent, la version imprimée de l'écran d'un navigateur ne peut pas être considérée comme une preuve électronique fiable car elle n'est rien d'autre qu'une capture d'écran, qui peut être modifiée très simplement, sans qu'il soit besoin de recourir pour ce faire à un logiciel ou à un matériel informatique particulier.

Exemple dans un État membre

La cour d'appel de **Lituanie** a conclu que les captures d'écran ne constituent pas des documents fiables (27 avril 2018, affaire n° e2A-226-516/2018).

Collecte, saisie et transmission

28. De par leur nature même, les preuves électroniques sont fragiles et peuvent être altérées, endommagées ou détruites par un maniement ou un examen impropre. C'est la raison pour laquelle des précautions particulières doivent être prises pour recueillir convenablement ce type de preuves. Sans ces précautions, ces éléments de preuve risquent de devenir inutilisables ou de conduire à une conclusion inexacte. Les parties sont en principe responsables d'un recueil correct des preuves électroniques dans les procédures civiles et administratives. Les différents types de données peuvent exiger de recourir à différentes méthodes pour les recueillir. Il importe que les mesures prises pour sécuriser et recueillir les preuves électroniques ne portent pas atteinte à l'intégrité de ces preuves. Lorsque la question revêt une importance considérable, les parties devraient envisager de recueillir les preuves électroniques en faisant appel à un spécialiste en informatique ou à des services notariaux. Les juges et les professionnels, y compris les praticiens du droit, devraient être conscients du fait que les données sont souvent stockées auprès de services en réseau. Cela concerne aussi bien l'informatique dématérialisée que la fourniture de services en ligne.

29. Les juges et les professionnels, y compris les praticiens du droit, connaissent mieux le traitement des preuves électroniques et ont acquis une plus grande expertise dans ce domaine, mais des normes spécifiques font encore défaut. La collecte et la saisie des preuves électroniques exigent parfois que des procédures et des outils spéciaux soient adoptés par les États membres. En attendant, les juges et les professionnels, y compris les praticiens du droit, devraient chercher à garantir l'intégrité, la confidentialité et la sécurité de ces données. Cela passe par la conservation de copies de sauvegarde sécurisées au cas où un incident surviendrait sur un autre moyen de stockage. Il est indispensable de conserver les données électroniques dans leur format original.

30. Bien que l'utilisation des données puisse être strictement nationale par nature, il devient de plus en plus probable que les données présentent un caractère transfrontière, impliquant ainsi d'autres pays. C'est, par exemple, le cas lorsque l'infrastructure utilisée pour le traitement ou le stockage des données, ou le fournisseur qui permet ce stockage ou ce traitement des données, se situe dans un autre pays. La coopération directe entre les juridictions et les services de confiance ou les services informatiques dématérialisés dans les affaires transfrontières doit être encouragée. Lorsqu'ils sont amenés à traiter des preuves électroniques, les juges et les professionnels, y compris les praticiens

du droit, devraient tenir compte de facteurs tels que le lieu d'établissement du fournisseur de service, le lieu de traitement des données et l'existence d'une législation locale qui règle l'accès aux données.

> Exemple de technologie transfrontière
>
> Le partage de données (l'informatique dématérialisée) consiste à stocker les différentes parties d'une base de données dans divers serveurs qui peuvent matériellement se situer à divers endroits. Cette technique de sécurité est devenue fréquente. Le caractère planétaire d'internet et l'utilisation croissante des services informatiques dématérialisés font qu'il est de plus en plus difficile de présumer que l'accès aux données est strictement national par nature.

31. Il existe des différences substantielles entre les règles de procédure nationales régissant le recueil des preuves. Les juridictions qui utilisent des preuves recueillies à l'étranger devraient tenir compte de ces différences. Il est recommandé que, lors du recueil transfrontière de preuves électroniques, les juridictions coopèrent étroitement. La juridiction qui adresse la demande devrait être informée des règles de procédure suivies par la juridiction qui fait l'objet de la demande afin d'adapter l'évaluation des preuves électroniques le cas échéant. En particulier, le recueil de preuves à l'étranger ne devrait pas conduire à une violation des principes et droits fondamentaux du droit procédural, tels que l'égalité des armes.

32. L'efficacité de la procédure est renforcée par la possibilité de transmettre les preuves électroniques à d'autres juridictions dans leur format original, au lieu de les imprimer et de les envoyer. Les données électroniques qui sont transmises devraient s'accompagner de leurs métadonnées. Cela englobe l'utilisation des métadonnées supplémentaires créées par les juridictions pour la bonne gestion des données et leur transmission sans heurts à d'autres juridictions. Le fait d'organiser les métadonnées permet aux juridictions de contrôler les éléments de preuve. Dans l'idéal, pour la transmission de preuves électroniques à une autre juridiction, il convient d'utiliser des copies.

33. La transmission des preuves électroniques par des moyens électroniques peut être encouragée et facilitée par la mise en œuvre de normes techniques communes et de formats de fichiers communs, et par la numérisation des systèmes judiciaires et administratifs nationaux. Compte tenu du risque plus élevé de destruction de preuves électroniques, il convient d'adopter au niveau national des procédures qui permettent de sécuriser la transmission de ces preuves.

34. L'intégrité, la capacité de survie et la sécurité des données doivent être prises en compte pour la transmission des preuves. L'existence de services fiables, comme les services de confiance, peut s'avérer essentielle pour assurer la bonne transmission des preuves électroniques. Si cette transmission exige le respect de la confidentialité, il peut être nécessaire d'appliquer des mesures ou des solutions techniques, comme le cryptage, qui permettent de limiter l'accès à une communication sécurisée aux seules personnes autorisées.

Pertinence

35. La production d'une quantité excessive de preuves électroniques par une partie, ce qui est malheureusement très facile à faire, rend leur traitement effectif par la juridiction et les autres parties concernées difficile, voire impossible. Il est donc essentiel que la juridiction gère activement les preuves électroniques en vue de restreindre leur production à ce qui est strictement nécessaire pour qu'elle puisse statuer. La gestion active des données doit respecter le principe de proportionnalité. Chaque demande de production de preuves électroniques devrait être examinée sur le fond, en particulier au vu de son utilité à des fins probantes, et les parties devraient avoir le droit de contester ces demandes.

36. Il importe que les juges et les professionnels, y compris les praticiens du droit, soient conscients d'un besoin éventuel d'une expertise technique et reconnaissent qu'il puisse être nécessaire de recourir à d'autres études ou aux connaissances d'autres spécialistes, par exemple en demandant une expertise. Les experts doivent être compétents et avoir une formation suffisante pour mener à bien la tâche qui leur est confiée.

Fiabilité

37. La distinction entre l'identité numérique et l'identité physique peut être source de problèmes pour la fiabilité de la preuve. Les juridictions devraient chercher à établir l'identité de l'auteur des données électroniques. Si la législation applicable ne précise pas comment l'établir, elle peut être déterminée par tout moyen objectif, comme une signature électronique, ou par la vérification de l'adresse de courrier électronique à partir de laquelle le document a été envoyé.

38. Les services de confiance peuvent fournir des mécanismes technologiques qui garantissent la fiabilité des preuves. Par exemple, les certificats de signature électronique, qui sont parfois qualifiés de « carte d'identité numérique » d'une personne, permettent de garantir à la fois l'authenticité et l'intégrité des données. Lorsque l'identité de l'auteur d'une signature électronique est

douteuse, la juridiction peut demander au fournisseur de service concerné par la signature électronique de faire une déclaration au sujet des questions sur lesquelles il est compétent pour apporter une preuve. L'horodatage (la certification de l'heure) peut s'avérer tout aussi importante pour prouver l'intégrité de données électroniques.

> Exemple de service de confiance
>
> L'horodatage est un mécanisme qui permet de prouver l'intégrité des données. Il démontre que les données existaient à un moment précis et qu'elles n'ont pas été modifiées. L'horodatage présente un intérêt pour les preuves électroniques, car il comporte les métadonnées pertinentes sur le moment de leur création.

39. Dans la mesure où la législation applicable le permet et sous réserve de l'appréciation de la juridiction, l'acceptation de tous les types de preuves électroniques est encouragée et recommandée dans la pratique juridictionnelle. En cas de litige, les parties identifient généralement les questions à régler et, à moins qu'une partie ne mette en doute l'authenticité d'une preuve électronique, il n'est pas nécessaire que la juridiction soulève cette question de sa propre initiative. La partie qui cherche à s'appuyer sur des preuves électroniques peut être tenue de démontrer leur authenticité uniquement lorsqu'une partie la conteste ; elle présente alors les métadonnées ou demande à un juge d'ordonner à d'autres personnes qu'elles fournissent des données supplémentaires, par exemple aux fournisseurs de services de confiance.

40. La référence spécifique au pouvoir discrétionnaire des juridictions dans les lignes directrices 21 et 22 souligne le rôle important de ce pouvoir discrétionnaire en ce qui concerne l'objet de ces lignes directrices.

41. Une partie à la procédure peut, comme pour n'importe quel autre type de preuve, contester l'authenticité d'une preuve électronique. Dans ce cas, cette partie peut demander au juge d'exclure la preuve en question, par exemple au motif qu'il est impossible de clairement identifier l'auteur des données. La fiabilité des données électroniques peut être prouvée de quelque manière que ce soit, par exemple par des signatures électroniques qualifiées ou des méthodes d'identification similaires qui garantissent l'intégrité des données. Il appartient cependant à la législation applicable de définir l'effet juridique des signatures électroniques, par exemple en prévoyant que seule la signature électronique qualifiée produit un effet juridique équivalant à celui de la signature manuscrite (à l'encre) ou en exigeant que les dispositifs utilisés pour produire des signatures soient exclusivement contrôlés par le signataire.

Les signatures électroniques qualifiées de l'Union européenne

Pour garantir l'intégrité des données, les juridictions n'ont pas besoin de procéder à une analyse particulière de la technologie utilisée pour la création des signatures électroniques qualifiées. Il leur suffit de vérifier le registre des fournisseurs de services de confiance qualifiés de l'Union européenne.

42. La ligne directrice 23 concerne la charge de la preuve. Les consommateurs et les personnes vulnérables, comme les enfants, ne sont pas techniquement et/ou économiquement en mesure de produire des preuves électroniques.

Lorsqu'elles bénéficient de dispositions légales qui facilitent ou renversent la charge de la preuve, ces dispositions l'emportent sur les présentes lignes directrices. Il importe que les juridictions jouent un rôle actif dans les affaires qui concernent des personnes vulnérables.

43. En fonction de l'ordre juridique national, la valeur probante des systèmes électroniques publics (officiels) qui génèrent des preuves électroniques doit être respectée. Ainsi, les données provenant de registres publics électroniques peuvent être traitées comme un document officiel, ce qui leur confère une présomption de fiabilité. L'enregistrement électronique d'autres procédures peut être considéré comme une représentation fiable des faits, exempte du risque d'erreur humaine (par exemple par rapport à un contenu dicté au procès-verbal par le juge).

Exemples dans des États membres de services de confiance publics

Plusieurs types particuliers de services de confiance sont mis à disposition au niveau national, comme « Profil de confiance » (**Pologne**), « Archivage électronique et numérisation » (**Belgique**) et « Conservation durable des informations et documents, plate-forme LEXNET d'échange d'informations entre les instances judiciaires et un large éventail de professionnels du système judiciaire » (**Espagne**).

Stockage et conservation

44. Le stockage, au sens des présentes lignes directrices, s'entend comme le stockage effectué pendant toute la durée de la procédure civile ou administrative. Les preuves électroniques peuvent être stockées par des juridictions, par exemple sur des dispositifs portables (cartes mémoires), des serveurs, des systèmes de sauvegarde et d'autres lieux de stockage des données (y compris l'informatique dématérialisée). Il importe que les juridictions stockent les preuves électroniques dans leur format original (et non en version imprimée), conformément à la législation applicable. Les questions de cybersécurité doivent également être prises en compte, ce qui signifie que les juridictions devraient agir en amont pour protéger l'intégrité des preuves électroniques

contre les cybermenaces, notamment contre les dommages et l'accès non autorisé. Le fait de privilégier la prévention permet aux juridictions d'empêcher que les cybermenaces ne portent atteinte à l'intégrité des preuves électroniques et d'atténuer en général les risques en matière de cybersécurité. Indépendamment de la méthode utilisée pour le stockage, les personnes non autorisées ne devraient pas avoir accès aux preuves électroniques.

45. Les preuves électroniques stockées peuvent être associées à des métadonnées normalisées qui précisent le contexte de leur création, ainsi que les liens existant avec d'autres fichiers électroniques. La mise en œuvre des normes internationales applicables aux métadonnées assure au stockage des preuves électroniques un certain degré de cohérence. Comme la création de métadonnées normalisées peut s'avérer difficile et demander beaucoup de temps, les juridictions peuvent recourir à des outils qui aident à la production de ces métadonnées normalisées.

> Exemple de solution utilisée pour normaliser les métadonnées
>
> Il existe un certain nombre d'outils qui permettent de créer des métadonnées normalisées. Par exemple, l'outil de gestion des métadonnées permet de créer un fichier XML *(eXtensible Markup Language)* qui comporte les métadonnées relatives aux preuves électroniques. Les fichiers XML ne nécessitent aucun logiciel professionnel de pointe. Il s'agit d'un format à la fois normalisé et suffisamment souple pour être appliqué à différents systèmes informatiques. Cet outil peut simplifier à la fois le stockage et la recherche des preuves électroniques.
>
> Il convient, à ce propos, d'appliquer les normes internationales relatives aux métadonnées, par exemple celles de l'Organisation internationale de normalisation (ISO).

46. La ligne directrice 27, qui concerne la conservation des preuves électroniques, est applicable à la fois au stockage et à l'archivage des preuves électroniques, une fois la procédure achevée. Il importe de stocker et d'archiver les preuves électroniques dans le format original dans lequel elles ont été créées, transmises et reçues, et d'une manière qui ne modifie pas matériellement les données. Les preuves électroniques devraient être mises à disposition dans un format lisible pendant toute la durée de la procédure. L'intégrité des preuves électroniques devrait être préservée à toutes les étapes.

Archivage

47. Les lignes directrices consacrées à l'archivage portent sur la période qui fait suite à la procédure et tiennent compte de la Recommandation Rec(2003)15 du Comité des Ministres du Conseil de l'Europe aux États membres relative à

l'archivage des documents électroniques dans le secteur juridique. La législation nationale prévoit habituellement les périodes de conservation et les conditions techniques de l'archivage. Les systèmes utilisés pour l'archivage doivent être sûrs et garantir la traçabilité de l'utilisation et le respect de la vie privée. Il convient de mettre en œuvre des mesures techniques et organisationnelles de manière à garantir la protection des preuves électroniques et à empêcher tout accès non autorisé. En cas d'utilisation d'un support électronique, celui-ci devrait être muni d'un certificat d'identification qui comporte les données essentielles le concernant. Ce support devrait être convenablement protégé, surtout contre la perte, les effets préjudiciables des produits chimiques, de la chaleur, de la lumière, des radiations, des champs magnétiques ou électriques et contre les dommages mécaniques.

48. Les services d'archivage peuvent vérifier, éventuellement en utilisant des signatures électroniques ou d'autres procédures électroniques, que les preuves électroniques sont archivées par des spécialistes qualifiés ou des organisations compétentes et que ces dernières n'ont pas modifié des données. Les données relatives aux signatures électroniques avec lesquelles les documents électroniques ont été signés et les données de vérification de ces signatures doivent toutes deux être convenablement archivées. Il importe que les États membres fournissent les ressources nécessaires à l'archivage des preuves électroniques aux organisations du secteur juridique chargées légalement de l'archivage.

49. La migration consiste à changer de support de stockage afin de préserver l'accessibilité des preuves électroniques. Le fait de négliger cette migration peut entraîner l'illisibilité des données. Les documents électroniques peuvent être archivés par des transferts périodiques de données d'un support de stockage à un autre ou d'un format à un autre. La migration devrait également concerner les métadonnées qui portent sur les documents électroniques archivés. Il convient de procéder régulièrement à une migration vers de nouveaux supports de stockage, en tenant compte, par exemple, de la dégradation et de l'usure du support en question, avant qu'il ne devienne obsolète en raison de l'évolution technologique des supports et du matériel informatiques. La migration vers de nouveaux supports ou formats de stockage devrait être effectuée, le cas échéant, en tenant compte de l'évolution technologique.

Exemple de solution durable

La migration des données peut être effectuée vers des dispositifs en réseau, comme l'informatique dématérialisée. Ces dispositifs sont constamment améliorés grâce à l'évolution technologique des supports et du matériel informatiques.

L'archivage dématérialisé permet également de mieux contrôler les coûts, en payant uniquement pour l'espace nécessaire.

Exemple de solution obsolète

Les CD, DVD ou autres disques optiques deviennent illisibles en raison de leur détérioration matérielle ou chimique dont les causes sont variables : elles vont de l'oxydation de la couche réfléchissante aux marques d'usure et à l'abrasion des surfaces ou des bords des disques, y compris sous forme de rayures visibles, en passant par d'autres types de réactions à des contaminants.

Sensibilisation, suivi, formation et éducation

50. La promotion de ces lignes directrices inclut leur large diffusion auprès des juridictions et des praticiens du droit, leur traduction ainsi que l'organisation de séminaires et de conférences sur les preuves électroniques.

51. Le suivi des normes techniques relatives aux preuves électroniques peut, par exemple, porter sur les nouveaux moyens de stockage, de conservation et d'archivage.

52. L'accès à une formation interdisciplinaire sur le traitement des preuves électroniques est nécessaire pour les juges et les professionnels, y compris les praticiens du droit. Cette formation peut porter sur les difficultés particulières que présentent les preuves électroniques, comme l'importance des métadonnées et de l'horodatage, l'utilisation de l'informatique dématérialisée ou des listes d'enregistrements (blockchains) pour la collecte et la saisie des preuves, ou la nécessité de présenter les preuves électroniques dans leur format original au lieu de simples images scannées ou d'exemplaires de versions imprimées.

53. Il importe de sensibiliser les juges et les professionnels, y compris les praticiens du droit, au contexte numérique au sens large et à l'utilisation des technologies, comme l'informatique dématérialisée, les services de confiance ou les listes d'enregistrements.

54. L'enseignement des questions matérielles et procédurales dans le domaine des preuves électroniques devrait représenter un élément essentiel de l'enseignement du droit.

Sélection de références bibliographiques et autres sources

Albert J. (2013), "Study on possible national legal obstacles to full recognition of electronic processing of performance information on construction products (under the construction products regulation), notably within the regimes of civil liability and evidentiary value", Commission européenne, Final General Report, 30-CE-0517177/00-3630-CE-0517177/00-36.

Biasiotti M., Mifsud Bonnici J., Cannataci J. et Turchi F. (éd.) (2018), *Handling and Exchanging Electronic Evidence across Europe*, Springer International Publishing, Cham.

Biasiotti M. A., Turchi F. et Epifani M. (2015), "The EVIDENCE Project : Bridging the Gap in the Exchange of Digital Evidence Accross Europe", SADFE 2015, disponible à l'adresse suivante : http://bit.ly/31ZPA8I.

Capriolli E. (2007), *Droit international de l'économie numérique*, Paris, Litec.

Comité des Ministres (2003), Recommandation Rec(2003)15 du Comité des Ministres du Conseil de l'Europe aux États membres relative à l'archivage des documents électroniques dans le secteur juridique.

Forgó N., Hawellek C., Knoke F. et Stoklas J. (2017), "The Collection of Electronic Evidence in Germany – a Spotlight on Recent Legal Developments and Court Rulings" in *New Technology, Big Data and the Law*, Springer, Singapour.

Hofmann E., Strewe U. et Bosia N. (2018), *Supply Chain Finance and Blockchain Technology. The Case of Reverse Securitisation*, Springer, Munich.

Mason S. (2016), *Electronic Signatures in Law*, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, Londres.

Mason S. (2016), *L'utilisation des preuves électroniques dans les procédures civiles et administratives et son impact sur les règles et modes de preuves. Étude comparative et analyse,* rapport préparé par Stephen Mason, avec le concours de Uwe Rasmussen, Strasbourg, 27 juillet 2016, CDCJ(2015)14-final.

Mason S. (2015), *Electronic Disclosure A Casebook for Civil and Criminal Practitioners*, PP Publishing 2015.

Mason S. (éd.) (2008), *International Electronic Evidence*, British Institute of International and Comparative Law, Londres.

Mason S. et Seng D. (éd.) (2017), *Electronic Evidence*, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, Londres.

Morabito V. (2017), *Business Innovation Through Blockchain. The B³ Perspective*, Springer International Publishing AG, Cham.

Schünemann W. et Baumann M. (éd.)(2017), *Privacy, Data Protection and Cybersecurity in Europe*, Springer International.

Singer P. et Friedman A. (2014), *Cybersecurity and cyberwar : What everyone needs to know*, Oxford University Press, Oxford.

Union internationale des télécommunications (2012), *Electronic Evidence : Model Policy Guidelines & Legislative Texts, Establishment of Harmonized Policies for the ICT Market in the ACP countries,* HIPCAR project "Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures", http://bit.ly/ITU-ElecEvid.

Voigt P. et von dem Bussche A. (2017), *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer International.

Sales agents for publications of the Council of Europe
Agents de vente des publications du Conseil de l'Europe

BELGIUM/BELGIQUE
La Librairie Européenne -
The European Bookshop
Rue de l'Orme, 1
BE-1040 BRUXELLES
Tel.: + 32 (0)2 231 04 35
Fax: + 32 (0)2 735 08 60
E-mail: info@libeurop.eu
http://www.libeurop.be

Jean De Lannoy/DL Services
c/o Michot Warehouses
Bergense steenweg 77
Chaussée de Mons
BE-1600 SINT PIETERS LEEUW
Fax: + 32 (0)2 706 52 27
E-mail: jean.de.lannoy@dl-servi.com
http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
22-1010 Polytek Street
CDN-OTTAWA, ONT K1J 9J1
Tel.: + 1 613 745 2665
Fax: + 1 613 745 7660
Toll-Free Tel.: (866) 767-6766
E-mail: order.dept@renoufbooks.com
http://www.renoufbooks.com

CROATIA/CROATIE
Robert's Plus d.o.o.
Marasoviçeva 67
HR-21000 SPLIT
Tel.: + 385 21 315 800, 801, 802, 803
Fax: + 385 21 315 804
E-mail: robertsplus@robertsplus.hr

CZECH REPUBLIC/RÉPUBLIQUE TCHÈQUE
Suweco CZ, s.r.o.
Klecakova 347
CZ-180 21 PRAHA 9
Tel.: + 420 2 424 59 204
Fax: + 420 2 848 21 646
E-mail: import@suweco.cz
http://www.suweco.cz

DENMARK/DANEMARK
GAD
Vimmelskaftet 32
DK-1161 KØBENHAVN K
Tel.: + 45 77 66 60 00
Fax: + 45 77 66 60 01
E-mail: reception@gad.dk
http://www.gad.dk

FINLAND/FINLANDE
Akateeminen Kirjakauppa
PO Box 128
Keskuskatu 1
FI-00100 HELSINKI
Tel.: + 358 (0)9 121 4430
Fax: + 358 (0)9 121 4242
E-mail: akatilaus@akateeminen.com
http://www.akateeminen.com

FRANCE
Please contact directly /
Merci de contacter directement
Council of Europe Publishing
Éditions du Conseil de l'Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81
Fax: + 33 (0)3 88 41 39 10
E-mail: publishing@coe.int
http://book.coe.int

Librairie Kléber
1, rue des Francs-Bourgeois
F-67000 STRASBOURG
Tel.: + 33 (0)3 88 15 78 88
Fax: + 33 (0)3 88 15 78 80
E-mail: librairie-kleber@coe.int
http://www.librairie-kleber.com

NORWAY/NORVÈGE
Akademika
Postboks 84 Blindern
NO-0314 OSLO
Tel.: + 47 2 218 8100
Fax: + 47 2 218 8103
E-mail: support@akademika.no
http://www.akademika.no

POLAND/POLOGNE
Ars Polona JSC
25 Obroncow Street
PL-03-933 WARSZAWA
Tel.: + 48 (0)22 509 86 00
Fax: + 48 (0)22 509 86 10
E-mail: arspolona@arspolona.com.pl
http://www.arspolona.com.pl

PORTUGAL
Marka Lda
Rua dos Correeiros 61-3
PT-1100-162 LISBOA
Tel: 351 21 3224040
Fax: 351 21 3224044
E mail: apoio.clientes@marka.pt
www.marka.pt

RUSSIAN FEDERATION/
FÉDÉRATION DE RUSSIE
Ves Mir
17b, Butlerova.ul. - Office 338
RU-117342 MOSCOW
Tel.: + 7 495 739 0971
Fax: + 7 495 739 0971
E-mail: orders@vesmirbooks.ru
http://www.vesmirbooks.ru

SWITZERLAND/SUISSE
Planetis Sàrl
16, chemin des Pins
CH-1273 ARZIER
Tel.: + 41 22 366 51 77
Fax: + 41 22 366 51 78
E-mail: info@planetis.ch

TAIWAN
Tycoon Information Inc.
5th Floor, No. 500, Chang-Chun Road
Taipei, Taiwan
Tel.: 886-2-8712 8886
Fax: 886-2-8712 4747, 8712 4777
E-mail: info@tycoon-info.com.tw
orders@tycoon-info.com.tw

UNITED KINGDOM/ROYAUME-UNI
The Stationery Office Ltd
PO Box 29
GB-NORWICH NR3 1GN
Tel.: + 44 (0)870 600 5522
Fax: + 44 (0)870 600 5533
E-mail: book.enquiries@tso.co.uk
http://www.tsoshop.co.uk

UNITED STATES and CANADA/
ÉTATS-UNIS et CANADA
Manhattan Publishing Co
670 White Plains Road
USA-10583 SCARSDALE, NY
Tel: + 1 914 472 4650
Fax: + 1 914 472 4316
E-mail: coe@manhattanpublishing.com
http://www.manhattanpublishing.com

Council of Europe Publishing/Éditions du Conseil de l'Europe
F-67075 STRASBOURG Cedex
Tel.: + 33 (0)3 88 41 25 81 – Fax: + 33 (0)3 88 41 39 10 – E-mail: publishing@coe.int – Website: http://book.coe.int

Les *Lignes directrices sur les preuves électroniques dans les procédures civiles et administratives* ont été conçues comme un outil pratique pour faciliter l'utilisation de ce type de preuves dans les procédures judiciaires. Leur objectif premier est d'aider les États membres du Conseil de l'Europe à adapter le fonctionnement de leurs mécanismes de règlement des litiges afin de remédier aux problèmes que posent les preuves électroniques dans les procédures civiles et administratives, et ainsi à renforcer l'efficacité et la qualité de la justice.

Les lignes directrices portent sur le recueil à distance des preuves orales, l'utilisation des preuves électroniques, la collecte, la saisie et la transmission de preuves, la pertinence, la fiabilité, le stockage et la conservation, l'archivage, la sensibilisation, le suivi des normes techniques pertinentes, et la formation et l'éducation.

Elles constituent le premier instrument international en la matière.

PREMS 021919

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 47 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

http://book.coe.int
ISBN 978-92-871-8928-8
8 €/16 $US

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE