COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg le 27 juillet 2016 CDCJ(2015)14 final

COMITE EUROPEEN DE COOPERATION JURIDIQUE
(CDCJ)

L'UTILISATION DES PREUVES ELECTRONIQUES DANS LES PROCEDURES CIVILES ET ADMINISTRATIVES ET SON IMPACT SUR LES REGLES ET MODES DE PREUVE

Etude comparative et analyse

Rapport préparé par Stephen MASON

avec le concours de Uwe RASMUSSEN

SOMMAIRE

Page

Les auteurs 3
Introduction 4
But de l'étude : changer de perspective 5
Proposition 6
Questionnaire initial 7
Questionnaire révisé 7
Cadre européen d'échange de données informatiques pour les tribunaux et les preuves 7
Réponses reçues 8
Notes pratiques 9
Analyse des réponses 10
Partie A Obtention de la preuve électronique 10
Tableau 1 Réponses aux questions 1 à 5 13
Partie B Obtention de l'identité présumée d'un utilisateur 17
Tableau 2 Réponses aux questions 6 et 7 18
Partie C Les questions de fond relatives à la nature de la preuve électronique 19
Tableau 3 Réponses aux questions 8 et 9 20
Partie D L'admissibilité et l'authenticité de la preuve électronique 28
Tableau 4 Réponses aux questions10 à 13 31
Partie E L'archivage de la preuve après le procès 32
Tableau 5 Réponses à la question 14 35
Observations en guise de conclusion 46
Recommandations existantes du Comité des Ministres 51
Annexe A: Mandat pour l'étude comparative 52
Annexe B : Questionnaire 53

Les auteurs

Stephen Mason

Stephen Mason, barrister, est chercheur associé à l'Institute of Advanced Legal Studies à Londres, et membredu Panel TI du Conseil general du Barreau d''Angleterre & Pays-de-Galles.

Il a assuré la direction éditoriale des ouvrages *Electronic Evidence* (3e éd., LexisNexis Butterworths, 2012) et *International Electronic Evidence* (British Institute of International and Comparative Law, 2008).

Il est également l'auteur de *Electronic Signatures in Law* (3e éd., Cambridge University Press, 2012); *Electronic Disclosure A Casebook for Civil et Criminal Practitioners* (PP Publishing, 2015); *Email, social media et the Internet at work: A concise guide to compliance with the law* (7e éd., PP Publishing, 2014), et *When Bank Systems Fail Debit cards, credit cards, ATMs, mobile et online banking: your rights and what to do when things go wrong* (2e éd., PP Publishing, 2014); et

Il a fondé la revue internationale en open source *Digital Evidence and Electronic Signature Law Review*, devenue incontournable pour les juges, les avocats et les chercheurs.

Stephen a été correcteur des examens des diplômes de Master (post-graduate) pour les preuves électroniques : LLM à l'Université d'Oslo (2006) ; Doctorat à l'Université d'Exeter (2013), et un Doctorat intitulé « authentification des preuves électroniques » (*authentification of Electronic Evidence*) à l'Université de Technologie du Queensland, Brisbane, Australie (octobre/novembre 2015).

Uwe Rasmussen

Uwe Rasmussen est un avocat français spécialisé dans le droit des technologies de l'information, de la preuve électronique, de la protection des données à caractère personnel, de la conformité et des droits relatifs aux bases de données.

Il a co-signé le Guide du Conseil de l'Europe sur la preuve électronique.

Conseiller régional d'une grosse multinationale éditrice de logiciels, pour les questions liées au droit de l'internet et aux processus de coopération en matière de preuves, M. Rasmussen est diplômé de l'Université de la Sorbonne (Paris) et de l'Université de Copenhague. Il a étudié le droit de la propriété intellectuelle à l'Université de Santa Clara (Californie) et est en outre Ingénieur systèmes Microsoft certifié.

Introduction

1. Le Conseil de l'Europe a commandité un rapport sur une étude comparative et une analyse des dispositions légales nationales en vigueur qui ont été adoptées ou adaptées concernant l'impact de la preuve électronique sur les règles et modes de preuve, portant spécifiquement sur les procédures civiles, administratives et commerciales (afin de rendre l'analyse légèrement plus facile, il est considéré que les « procédures civiles » couvrent le « droit civil » et le « droit commercial »).

2. L'étude a pour but d'identifier les problèmes que rencontrent les différents systèmes juridiques des Etats membres dans ce domaine, et pour lesquels ils ont besoin de recours ou de solutions ou en ont mis en place.

3. La mission confiée à l'origine (voir Annexe A au présent rapport) prévoyait que l'étude porterait notamment, mais pas exclusivement, sur des problèmes liés aux thèmes suivants :

- l'admissibilité de la preuve électronique
- la valeur probante accordée à la preuve électronique
- les implications en matière de règles relatives à la qualification, telles que :
  - la charge de la preuve
  - les présomptions
  - l'authenticité/la fiabilité
  - l'archivage et la préservation des preuves
  - la gestion de l'affaire et du procès
  - le rôle du juge
  - la perquisition préalable au procès pour la recherche de preuve
  - le rôle des experts indépendants ou judiciaires.

4. Dans l'idéal, l'étude devait couvrir les 47 Etats membres du Conseil de l'Europe. C'est pourquoi une série de question avaient été élaborées pour transmission aux membres du Comité européen de coopération juridique, afin qu'ils puissent répondre dans un délai suffisant pour que les auteurs soient en mesure de préparer le projet de rapport à présenter avant fin 2014.

But de l'étude : changer de perspective

5. L'étude a pour but d'encourager les juges, avocats et juristes à comprendre qu'il est nécessaire de changer de perspective en ce qui concerne cette nouvelle forme de preuve[1].

6. Lorsqu'on enregistre un contenu sur papier, le contenant et le contenu sont liés l'un à l'autre. En revanche, pour les informations numériques, il en va tout autrement[2]. Au niveau le plus basique, les « bits et octets » constituent le contenu, formé par des 0 et des 1. De plus, le contenant peut être constitué de nombreux dispositifs disparates, et un logiciel écrit par des êtres humains est nécessaire pour lire et interpréter les données. Il faut donc bien comprendre qu'un changement conceptuel s'impose. La preuve électronique ayant des caractéristiques uniques, des questions complexes sont susceptibles de se poser en matière d'intégrité et de sécurité de ce type de preuve, même si l'authentification sera différente selon que l'on a affaire à des formes complexes de preuves électroniques ou à des formes plus simples telles que des courriels ou des SMS, par exemple.

7. La taxonomie pour les formes traditionnelles de preuve est bien établie. En revanche, pour la preuve électronique, elle évolue encore et couvre à l'heure actuelle les éléments suivants[3] :

Compréhension du monde numérique
- Sources de la preuve numérique
- Caractéristiques de la preuve numérique
- Données cryptées

Authenticité
- Preuve (y compris l'investigation, la saisie et l'examen de la preuve numérique)
- 'Fiabilité' et présomptions
- Authenticité
- Intégrité

Les logiciels comme témoins (connu sous l'expression « ouï-dire » dans les systèmes de common law).

8. Comme on le notera d'emblée, certains domaines de connaissances figurant dans la liste ci-dessus ne sont pas traités dans un manuel conventionnel sur la preuve. Les thèmes supplémentaires reflètent la nature de la preuve électronique. Ainsi, il convient d'être plus réfléchi en ce qui concerne la manière dont on opère pour la saisie, l'investigation et l'examen de la preuve électronique. Cela s'explique par le fait que ce processus initial peut être altéré à un point tel que la preuve en devient inadmissible ou peut prêter le flanc à contestation, en particulier pour ce qui est de son authenticité.

[1] Pour une discussion de l'importance du sujet dans l'enseignement du droit, voir Denise Wong, 'Educating for the future: teaching evidence in the technological age', *Digital Evidence and Electronic Signature Law Review*, 10 (2013), p.16-24 et Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', *Digital Evidence and Electronic Signature Law Review*, 10 (2013), p. 23-28.

[2] Pour l'heure, il n'y a pas de terme généralement accepté concernant la forme de la prevue qui provident de notre utilisation de la technologie, spécifiquement les logiciels. Dans un souci de concision, les termes "électronique" et "numérique" sont utilises de manière interchangeable. Pour une discussion détaillée de ces termes, voir Burkhard Schafer et Stephen Mason, Chapitre 2, 'The characteristics of electronic evidence in digital format' in Stephen Mason, éd. gen, *Electronic Evidence* (3e éd., LexisNexis Butterworths, 2012).

[3] Extrait de Stephen Mason, 'A framework for a syllabus to teach electronic evidence', *Digital Evidence and Electronic Signature Law Review* 10 (2013), p. 7 – 15; Voir également Stephen Mason, 'The structure of electronic evidence: have we got it right?', *Editorial, Amicus Curiae* The Journal of the Society for Advanced Legal Studies, Numéro 99, automne 2014, 1.

Proposition

9. Le mandat exigeait :

(i) de réaliser une analyse des lois nationales existantes qui ont été adoptées ou adaptés à l'impact d'internet et des nouvelles technologies sur les règles de preuve et les modes de preuve, axée sur les procédures en matière civile, administrative et commerciale ;

(ii) d'identifier des problèmesauxquels les différents systèmes juridiques des Etats membres sont confrontés à cet égard, et pour lesquels ils aimeraient bien trouver une solution ou ont trouvé des solutions ;

(iii) d'énoncer des propositions de solution sur la base d'approches et de meilleures pratiques déjà adoptées dans certains Etats membres et non membres, dans le but de réduire ou du moins d'alléger l'engorgement des tribunaux civils et administratifs confrontés à des preuves électroniques.

10. Le premier questionnaire avait au départ prévu d'aborder les problématiques ci-dessus, énumérées dans l'ordre dans lesquelles elles seraient traitées à partir du démarrage d'une procédure. Le juge entre en scène dès lors qu'une recherche de preuve est sollicitée, si tant est que celle-ci soit nécessaire.. A cet égard, il est considéré comme acquis que le rôle du juge doit être envisagé tout au long du processus et en lien avec chacune des problématiques identifiées ci-dessous :

la perquisition préalable au procès pour la recherche de preuve

la préservation des preuves

la gestion de l'affaire et du procès

le rôle du témoin expert indépendant ou judiciaire

la charge de la preuve (cet élément sera pertinent lors de l'élaboration de plaidoiries, tout comme il l'est lors de la conduite de l'affaire devant le tribunal)

les questions de fond concernant la nature de la preuve :
- Admissibilité
- Présomptions
- Authenticité et fiabilité
- Valeur probante

L'archivage des preuve après le procès.

11. L'étude a pour but d'identifier les *problèmes* auxquels les différents systèmes juridiques des Etats membres sont confrontés à cet égard, ainsi que les *solutions* mises en place.

12. Avant de démarrer l'étude, il a fallu établir quelle action les Etats avaient éventuellement déjà entreprise dans les domaines susmentionnés. Un certain nombre de recommandations, formulées sur la base de l'analyse, ont été examinées afin de décider s'il y a lieu d'aller plus loin.

Questionnaire initial

13. Les auteurs ont préparé une série de questions concernant chacune des problématiques à prendre en compte dans l'étude. Pour aider les Etats membres à y répondre, ils ont préparé un modèle d'analyse de la situation en Angleterre et auPays-de-Galles ainsi qu'en France, qui a fait l'objet de deux documents annexes au questionnaire proposé. Ces questions avaient pour but une compréhension raisonnablement précise de la manière dont chaque Etat membre avait répondu aux problèmes soulevés.

Questionnaire révisé

14. A la 89e réunion du Comité européen de coopération juridique (CDCJ), qui s'est tenue à Strasbourg du 29 au 31 octobre 2014, les membres du Comité ont demandé aux auteurs de préparer un questionnaire simplifié (ciblant uniquement les défis et les changements procéduraux [voir B-11].

15. Les auteurs ont ainsi préparé un questionnaire révisé (reproduit en Annexe B au présent rapport), qui a été posté sur le site web du Conseil du Conseil de l'Europe par le Secrétariat et envoyé le 13 mars 2015 aux organisations suivantes :

Associations des barreaux dans les Etats membres du Conseil de l'Europe
Chambres des Notaires des Etats membres du Conseil de l'Europe
Conseil des Notariats de l'Union européenne
Association européenne des magistrats
Conseil des Barreaux européens (CCBE)
Magistrats Européens pour la Démocratie et les Libertés (MEDEL), un groupe de magistrats, juges et procureurs européens.

Cadre européen d'échange de données informatiques pour les tribunaux et les preuves *(European Informatics Data Exchange Framework for Courts and Evidence*)

16. Stephen Mason a signalé aux membres du CDCJ l'existence du projet de l'Union européenne (UE) *European Informatics Data Exchange Framework for Courts and Evidence* (e-Evidence)[4]. Le Comité a demandé de prendre note des travaux de ce projets et d'y faire mention dans l'étude.

17. Le projet, qui a commencé ses travaux à Florence en mars 2014, produira ses résultats finaux en octobre 2016. Il examinera la possibilité d'une réponse juridique commune, et envisagera de recommander des procédures standards pour l'utilisation, la collecte et l'échange de preuves électroniques dans tous les Etats membres de l'UE. Des lignes directrices, des recommandations et des normes techniques seront proposées, avec notamment une proposition d'échange de preuves numériques selon des normes et des règles communes.

18. Les objectifs suivants sont considérés comme essentiels :

(i) développer une base de connaissances commune et partagée de ce qu'est la preuve électronique et des concepts associés en la matière (analyse forensique numérique, droit pénal, procédure pénale, coopération internationale pénale) (WP2 : catégorisation pour carte heuristique) ;

[4] http://www.evidenceproject.eu.

(ii) établir des règles et des critères pour le traitement des preuves électroniques dans les Etats membres de l'UE, et sur la manière dont l'échange de preuves devrait être régulé (WP3 : questions juridiques) ;

(iii) dégager des critères et des normes pour garantir la fiabilité, l'intégrité et les conditions relatives à la chaîne de mise en sûreté des preuves électroniques dans les Etats membres et l'échange de ces preuves (WP4 : questions normatives) ;

(iv) déterminer les conséquences en procédant à l'évaluation globale et actuelle de la collecte, de la préservation et de l'échange des preuves électroniques du point de vue des services de police, et en proposant des lignes directrices qui pourraient être intégrées dans un Cadre européen commun régissant ce domaine (WP6 : questions d'application de la loi) ;

(v) analyser les conséquences en matière de confidentialité des données (WP8 : questions de protection des données) ;

(vi) identifier et développer des fonctionnalités technologiques pour un Cadre européen commun en matière de recueil et d'échange de preuves électroniques (WP5 : questions techniques) ;

(vii) analyser les problématiques liées à la saisie de preuves électroniques (WP7 : taille du marché).

19. Les étapes (i), (v) et (vii) sont pratiquement achevées. Les étapes (ii), (iii), (iv) et (vi) sont en cours de développement.

Réponses reçues

20. Les ministères de la Justice d'Andorre ; de l'Arménie ; de la Belgique ; de la Croatie (qui a actualisé sa réponse au questionnaire initial) ; de la République tchèque ; du Danemark ; de la Finlande ; de la France ; de l'Allemagne ; de la Hongrie ; de l'Irlande ; de l'Italie (qui avait répondu au questionnaire initial) ; de la Lettonie ; de la Lituanie ; de Malte ; du Monténégro ; de la Norvège ; de la Pologne ; du Portugal ; de la Roumanie ; de la Fédération de Russie ; de la Serbie ; de la République slovaque ; de l'Espagne ; de la Suède ; de la Suisse ; de la Turquie ; de l'Ukraine et du Royaume-Uni (concernant l'Angleterre & le Pays-de-Galles) ont répondu.

21. Des réponses supplémentaires ont été reçues du *Col.legi d'Advocats d'Andorra* pour Andorre ; du Conseil supérieur de la magistrature de Bulgarie pour la Bulgarie ; du Haut Conseil de Justice pour la Géorgie ; de la Chambre fédérale des Notaires pour l'Allemagne; et des Services juridiques du *Consejo General de la Abogacía española* pour l'Espagne.

22. Des réponses ont été transmises, à titre individuel, par Anahit Beglaryan, Avocat, membre du Barreau d'Arménie, M. Maksim Greinoman, associé dans le cabinet Advokaadibüroo Greinoman & Co, Tallinn (Estonie) et par M. Michael G. Rachavelias, Avocat, membre de l'Association du Barreau de Larissa (Grèce).

Notes pratiques

23. Le questionnaire visait l'utilisation de la preuve électronique dans les procédures civiles et administratives. Lorsqu'une réponse contenait une référence aux procédures pénales, l'élément reçu à cet égard a été ignoré.

24. La Croatie et l'Italie ayant déjà répondu aux questions du premier questionnaire, autrement dit, elles n'ont pas répondu à certaines des questions du questionnaire révisé n'ont pas été renseignées par ces Etats membres.

25. Certaines des réponses d'un certain nombre d'Etats membres n'étaient pas claires, au sens où la réponse (oui /non) ne semblait pas cohérente par rapport aux commentaires ajoutés, ou encore certaines réponses à des questions étaient à la fois « oui » et « non ». Quelques questions ont été interprétées de différentes manières par ceux qui ont répondu au nom de leur Etat, ce qui pourrait expliquer les différences dans les réponses. En outre, certaines réponses laissaient penser que nous avions posé la mauvaise question : il est tout à fait possible que cette impression soit correcte, vu la portée du droit matériel et des règles de procédure que nous souhaitions passer au crible via le questionnaire. De plus, certains Etats membres n'ont pas répondu à chaque question. Certaines réponses ont donc été extrapolées.

26. Lorsqu'il y avait une différence entre deux réponses à une question pour un même Etat membre, la réponse retenue a été celle émanant du ministère de la Justice de cet Etat.

Analyse des réponses

27. Dans la partie sur l'analyse des réponses, le préambule et les questions du questionnaire révisé sont reproduits entièrement.

Partie A Obtention de la preuve électronique

Préambule

28. Il existe trois types d'éléments de preuve qui pourraient être obtenus lors d'une procédure judiciaire :

(i) les preuves en provenance de sites internet accessibles au public, tels que (cette liste n'est qu'indicative) les blogs et les images publiées sur les réseaux sociaux ;

(ii) les preuves substantielles (ou probantes), comme l'e-mail ou des documents en format numérique qui ne sont pas rendus publics et détenus sur un serveur ;

(iii) l'identité présumée d'un utilisateur et des données de trafic («métadonnées») qui sont utilisées pour aider à identifier une personne en découvrant la source de la communication, mais pas le contenu.

29. Par exemple, un problème de compétence se pose si une entreprise française estime qu'un employé a volé des secrets d'affaires et qu'il a conservé les données sur un serveur privé dématérialisé britannique.

30. Question 1
Si une partie souhaite produire des preuves à partir de sites Internet accessibles au public, un tribunal peut-il exiger la production de copies des sites sous un format spécifique afin de garantir l'authenticité notamment par la désignation d'un huissier ou d'un expert auprès du tribunal spécialisé en preuves numériques ?

Analyse des réponses à la question 1

31. Dans cinq Etats membres : Andorre, Croatie, France, Lituanie et Turquie, la règle dans chaque juridiction est plus nuancée qu'un simple « oui », comme indiqué ci-dessous :

(i) En Andorre, la preuve ne doit être recueillie de manière spécifique qu'en cas de contestation par une partie adverse. Il sera en général demandé à un notaire de certifier le site web.

(ii) En Croatie, l'article 234 de la loi sur la procédure civile prévoit que, lorsqu'un juge demande une preuve, une tierce partie se voit demander de soumettre le document. Ce dernier devient alors un document joint pour la personne qui l'a fourni et pour la partie qui se réfère au document.

(iii) En France, une partie peut soumettre une copie de site web ou de capture d'écran, en particulier pour prouver l'existence d'un fait légal. Le tribunal peut cependant considérer qu'il est nécessaire d'ordonner des mesures supplémentaires pour clarifier des questions de faits, conformément à l'article 10 du Code de procédure civile. Dans ce cadre, le tribunal peut désigner la personne de son choix pour le conseiller sous forme de constats, de

consultation ou d'expertise. Ainsi, un huissier peut aussi être désigné par le tribunal pour produire un rapport, mais la portée de cette mission est extrêmement restreinte puisqu'elle est limitée à l'apport de simples constats de faits, rapportés dans un rapport officiel. Le rapport de l'huissier fait autorité en l'absence d'éléments (de preuve) contraires. Le tribunal peut également désigner un expert pour le conseiller sur la fiabilité d'une copie de site web ou de capture d'écran, ou pour procéder à la réalisation de ces copies.

(iv) En Lituanie, la règle veut que soient soumis des documents originaux, et que, si des copies sont soumises, elles soient alors certifiées par un tribunal, un notaire ou un avocat participant à l'affaire.

(v) En Turquie, le tribunal n'exigera que les copies de site web soient recueillies de manière spécifique afin d'en garantir l'authenticité que dans les cas où le tribunal saisi de l'affaire a des doutes sur l'authenticité de la preuve ou que les parties font valoir des objections sur cette question.

32. Les autres Etats membres ayant répondu au questionnaire ont indiqué qu'il n'y avait pas d'exigence de recueillir les preuves électroniques d'une manière spécifique.

33. Nous avons compris de la réponse de l'Arménie qu'il n'y a pas de procédure spécifique, cependant, en pratique, les avocats ayant répondu au titre de ce pays ont indiqué qu'ils mentionnent le lien Internet pour que le tribunal ait la possibilité de vérifier la preuve en suivant ce lien et de s'assurer de l'authenticité des données. De plus, l'article 60 du Code de procédure civile et l'article 37 du Code de procédure administrative prévoient que, pour clarifier des questions exigeant des connaissances spécialisées qui se posent au cours d'un procès, le tribunal peut, sur demande d'une partie, des deux parties ou de sa propre initiative, ordonner une expertise, qui peut être confiée soit à un bureau professionnel d'expertise, soit à un expert professionnel.

(i) La réponse de la Grèce indiquait qu'auparavant, il existait des conditions à remplir mais il semble qu'actuellement, celles-ci n'aient plus cours ; auparavant, l'accent était placé sur la nécessité d'obtenir des preuves tangibles.

(ii) La délégation polonaise a indiqué que le droit polonais ne donne pas de définition de la « preuve électronique », les codes de procédure administrative, civile ou pénale ne contenant aucune définition ou son équivalent. Toute demande de production de la preuve et la preuve elle-même est envisagée dans la perspective de son utilité pour prouver ou réfuter l'allégation (article 75 du Code de procédure administrative, ou article 227 du Code de procédure civile). Toutes les preuves (chaque demande de production de preuve) sont soumises à l'appréciation de l'autorité chargée de la procédure. Les parties peuvent contester les preuves. Elles ont également le droit de présenter de nouvelles demandes concernant une preuve particulière. Le droit procédural polonais ne suit pas la théorie de la preuve légale, même si certaines contraintes peuvent être rencontrées dans la jurisprudence.

34. Question 2
Est-il possible pour une partie de demander à un tribunal l'obtention d'une copie numérique des données collectées (tels que les fichiers informatiques conservés sur un ordinateur d'un tiers localisé dans le ressort de la juridiction) avant qu'une action en justice soit initiée sur le fond ?

Analyse des réponses à la question 2

35. En Arménie, à Malte et en Serbie, une partie ne peut pas obtenir une copie de données électroniques avant qu'une action en justice soit initiée sur le fond. En Andorre, le ministère a indiqué que cette obtention n'était pas possible, mais le Col.legi d'Advocats d'Andorra a, lui, indiqué le contraire.

36. Les autres juridictions ayant répondu à cette question ont indiqué qu'une partie peut demander à un tribunal d'obtenir une copie de données électroniques, même s'il est possible que des règles différentes s'appliquent selon que la preuve est demandée lorsqu'une partie a des chances d'être partie à l'action en justice, ne va pas être partie à l'action justice, lorsqu'une personne est impliquée dans un méfait, ou lorsque les règles de procédure pertinentes fixent des critères qui doivent être examinés avant toute demande

37. En Angleterre & au Pays-de-Galles, les Règles de procédure civile et la jurisprudence couvrent cette éventualité, mais, dans certaines juridictions, comme l'Estonie, elle n'est possible que dans des circonstances exceptionnelles par la procédure de recueil préliminaire de preuves, et très rarement accordée en pratique. En Lettonie, une partie peut saisir le tribunal pour sécuriser des preuves tant dans les procédures administratives que civiles lorsqu'elle est fondée à penser qu'il pourrait être impossible ou problématique de les obtenir par la suite. La situation est similaire en Lituanie, où une partie peut saisir le tribunal pour obtenir des mesures conservatoires afin de sauvegarder des preuves en vertu des articles 144 et 221 du Code de procédure civile.

38. Question 3
Est-il possible pour une partie qui ne réside pas dans votre pays d'avoir accès au même recours auprès d'un tribunal comme mentionné dans le point 2 ci-dessus, et est-il également possible, même si c'est peu probable que l'action en justice sur le fond soit plaidée devant une juridiction nationale ?

Analyse des réponses à la question 3

39. A l'exception de Malte et de la Serbie, il est possible pour une partie d'un autre Etat membre qui ne réside pas dans la juridiction de demander la même ordonnance judiciaire que celle mentionnée à la question 2 plus haut. En Andorre, le ministère a indiqué que cela n'est pas possible, alors que Col.legi d'Advocats d'Andorra a indiqué le contraire.

40. Question 4
Lorsqu'en vertu d'une ordonnance d'un tribunal, une saisie de preuves électroniques est réalisée, faut-il que la partie qui demande la preuve suive un ensemble particulier de dispositions juridiques ou de lignes directrices pour la saisie de ces preuves électroniques?

Analyse des réponses à la question 4

41. Aucune ligne directrice ne s'applique à la saisie de preuves électroniques dans les procédures civiles, même si en Croatie, il faut passer par un tribunal pour saisir des preuves ; en République tchèque, toutes mesures concernant des preuves doivent être prises conformément au Code de procédure civil, et les preuves sont sauvegardées par le

tribunal ; en Estonie, un huissier exécutera la décision ; en France, l'huissier notifie la personne en possession des preuves et c'est lui qui les recueille, et, au Portugal, il peut être nécessaire que le tribunal assure ce type de formalités.

42. Question 5
En ce qui concerne la procédure administrative, veuillez indiquer s'il existe des règles spécifiques concernant la production d'éléments de preuve, notamment en matière de signatures électroniques, et si un format particulier de signature électronique est requis lors de la production de preuves par voie électronique.

Analyse des réponses à la question 5

43. Bon nombre des juridictions ayant répondu au questionnaire ne connaissent pas de règles particulières. En Croatie, une tierce partie se voit notifier de soumettre des preuves à la demande du tribunal. En Estonie, les documents devraient être signés au moyen de la signature numérique estonienne, même si, en pratique, il est possible de produire des documents sans signature. En Pologne, les documents produits doivent être certifiés conformément aux dispositions de la loi sur la numérisation des activités des autorités publiques et respecter un format spécifique ainsi que contenir l'adresse électronique de l'expéditeur.

Tableau 1

Réponses aux questions 1 à 5

	1		**2**		**3**		**4**		**5**
	Oui	Non	Oui	Non	Oui	Non	Oui	Non	
Andorre	✓			✓		✓		✓	Le ministère n'a pas répondu, mais le Col.legi d'Advocats d'Andorra a indiqué qu'il n'y avait pas de dispositions dans la législation.
Arménie		✓		✓	✓			✓	Il n'y a pas de règles spéciales sur la production de preuves électroniques, mais des amendements devraient être faits aux Codes de procédure civile et Administrative.
Belgique		✓	✓		✓		✓		Il n'y a pas de règles spéciales sur la production de preuves électroniques.
Bulgarie	✓		✓		✓			✓	Il n'y a pas de règles spéciales sur la production de preuves électroniques.
Croatie	✓		✓		✓			✓	La Loi sur la procédure civile prévoit qu'un document électronique doit être signé par une signature électronique avancée, produit sur un formulaire idoine et envoyé par voie électronique au système d'information central.

République tchèque		✓	✓		✓		✓		Les procédures administratives sont en général soumises aux règles imposées par le Code de procédure administrative (Loi n° 500/2004 Coll.). La section 37 paragraphe 4 du Code exige qu'un document soumis à une autorité administrative par voie électronique porte une signature électronique. La Loi n° 300/2008 Coll. sur les actes électroniques et sur la conversion autorisée de documents prévoit les cas d'exemptions, lorsqu'une personne physique ou morale n'est pas obligée de produire les documents demandés avec une signature électronique. En vertu des dispositions de la section 18 paragraphe 2, un document produit au moyen d'une messagerie dont les données sont certifiées n'a pas à porter une signature électronique. Un tel acte produit les mêmes effets qu'un acte effectué par écrit et signé.
Danemark		✓	✓		✓			✓	Il n'y a pas de règles spéciales.
Estonie		✓	✓		✓			✓	Les documents devraient être signés par la signature numérique estonienne. En pratique, les documents produits peuvent ne pas porter de signature.
Finlande		✓	✓		✓			✓	Il n'y a pas de règles spéciales. Voir la réponse pour des informations supplémentaires concernant les mesures conservatoires, y compris la réponse à la question 2.
France	✓		✓		✓			✓	Pas de réponse.
Géorgie		✓	✓		✓			✓	Pas de réponse.
Allemagne		✓	✓		✓			✓	De manière générale, il est possible de soumettre des données électroniques dans des procédures administratives sans à avoir à respecter une forme spécifique. Si la loi exige une forme écrite, les documents électroniques doivent être signés par une signature électronique qualifiée. Voir para 3a de la Loi allemande sur les procédures administratives. Voir compilation jointe des

									réponses pour plus de détails.
Grèce		✓	✓		✓			✓	Conformément à l'article 4 du Décret présidentiel 150/2013, chaque dossier électronique devant être produit en justice, quel que soit son format, doit être produit avec une signature électronique avancée. Voir la réponse pour plus de détails.
Hongrie		✓	✓		✓			✓	Il n'y a pas de procédures spécifiques prévues pour la production de preuves électroniques, bien que certaines présomptions s'appliquent aux documents privés et publics en cas d'utilisation de formes particulières de signature électronique. Voir la compilation jointe des réponses pour plus de détails.
Irlande		✓	✓		✓			✓	Il n'y a pas de procédures spécifiques prévues pour la production de preuves électroniques.
Italie					✓				Pas de réponse.
Lettonie		✓	✓		✓			✓	Lorsque les preuves sont produites électroniquement, il faut que les données soient signées avec une signature électronique avancée.
Lituanie	✓		✓		✓			✓	Pas de règles spéciales. Voir la compilation jointe des réponses pour plus de détails.
Malte		✓		✓		✓		✓	Pas de règles spéciales concernant les procédures administratives et la production de preuves électroniques.
Monténégro		✓	✓		✓			✓	Pas de règles spéciales. Voir la compilation jointe des réponses pour plus de détails.
Norvège			✓		✓				Voir la compilation jointe des réponses pour plus de détails.
Pologne		✓	✓		✓			✓	Pas de règles spéciales. Voir la compilation jointe des réponses pour plus de détails.
Portugal		✓	✓		✓		✓		Pas de règles spéciales. Voir la compilation jointe des réponses pour plus de détails.

Roumanie	✓		✓		✓			✓	Les dispositions pertinentes concernant la production de preuves électroniques, en particulier concernant les signatures électroniques, sont contenues dans la Loi n° 455/2001 sur la signature électronique. Dans les procédures administratives, les dispositions concernant le statut légal des documents écrits électroniques s'appliquent (Loi n° 455/2001 sur la signature électronique, articles 5 à 11).
Fédération de Russie		✓	✓		✓			✓	Pas de règles spéciales. Voir la compilation jointe des réponses pour plus de détails.
Serbie		✓		✓		✓		✓	L'article 21 de la Loi sur les contentieux administratifs contient des dispositions relatives à la production et au traitement de documents électroniques qui sont étroitement définies par le Règlement intérieur des tribunaux.
République slovaque		✓	✓		✓			✓	Pas de règles spéciales. Voir la compilation jointe des réponses pour plus de détails.
Espagne		✓	✓		✓			✓	Voir la compilation jointe des réponses pour plus de détails.
Suède		✓	✓		✓			✓	Pas de règles spéciales.
Suisse		✓	✓		✓			✓	Pas de règles spéciales.
Turquie	✓		✓		✓			✓	La Loi sur les procédures des juridictions administratives. Le Code ne prévoit pas de dispositions spécifiques pour la production de preuves.
Ukraine		✓		✓		✓		✓	Pas de règles spéciales.
Royaume-Uni (Angleterre & Pays-de-Galles)		✓	✓		✓			✓	Pas de règles spéciales.

Partie B. Obtention de l'identité présumée d'un utilisateur

Préambule

44. Le problème se pose quand une partie prétend qu'un courriel lui a causé un dommage (diffamation, secrets commerciaux, etc.), mais que l'identité de l'expéditeur ne peut être établie. La partie qui a subi ce mauvais agissement souhaiterait utiliser les informations d'identification détenues par le fournisseur d'accès (métadonnées) pour prouver le lien entre un compte de message électronique et une personne physique, qui est l'utilisateur du courriel.

45. Question 6
Est-il possible pour une partie de faire une requête auprès d'un tribunal pour identifier l'utilisateur d'un service électronique fourni par une entreprise dans votre juridiction, comme l'utilisateur d'un compte de messagerie électronique, service d'accès à Internet, ou un compte VoIP ?

Analyse des réponses à la question 6

46. Tous les répondants, à l'exception de la Croatie, de la Finlande, de la Géorgie, de Malte, de la Serbie, de la République slovaque et de l'Ukraine, ont indiqué qu'une partie pourrait faire une requête auprès d'un tribunal pour identifier l'utilisateur d'un service électronique fourni par une entreprise dans leur propre juridiction. Pour Andorre, le ministère a indiqué que cela n'est pas possible, alors que le Col.legi d'Advocats d'Andorra a indiqué que cela était possible. En Belgique, il existe un certain nombre de méthodes alternatives pouvant être utilisées pour obtenir des informations, et le lecteur est renvoyé à la réponse belge au questionnaire pour plus de détails. En République tchèque, le facteur décisif est la juridiction et le fait que l'affaire relève ou non de la juridiction du tribunal, et, en Hongrie, la situation dépend de la manière dont la Loi sur l'information est interprétée.

47. Question 7
Est-il possible pour une partie qui ne réside pas dans votre pays d'avoir recours à la même ordonnance d'un tribunal, et est-il également possible même si c'est peu probable que l'action en justice sur le fond soit plaidée devant une juridiction nationale ?

Analyse des réponses à la question 7

48. Tous les Etats membres qui ont répondu, à l'exception de la Belgique, de la Croatie, de la Finlande, de la Géorgie, de Malte, de la Fédération de Russie, de la Serbie, de la République slovaque et de l'Ukraine, ont indiqué qu'une partie ne résidant pas dans leur juridiction nationale peut déposer une requête auprès du tribunal pour identifier l'utilisateur d'un service électronique fourni par une société située dans la juridiction, et qu'il est possible d'intenter une action en justice sur le fond. Pour Andorre, le ministère a indiqué que cela n'était pas possible, alors que le Col.legi d'Advocats d'Andorra a indiqué que cela était possible.

49. En République tchèque, le facteur décisif est la juridiction et si la question relève ou non de la compétence du tribunal. En Hongrie, la situation dépend de la manière dont la Loi sur l'information est interprétée.Pour la Lettonie, le requête ne peut être soumise qu'une fois que le tribunal a accepté l'auteur de la requête et qu'une action a été intentée. En Lituanie, une partie peut demander au tribunal d'appliquer des mesures conservatoires avant qu'une action en justice ne soit intentée pour sauvegarder des preuves, conformément aux articles 144 et 221 du Code de procédure civile.

Tableau 2

Réponses aux questions 6 et 7

	6		7	
	Oui	Non	Oui	Non
Andorre		✓		✓
Arménie	✓		✓	
Belgique		✓		✓
Bulgarie	✓		✓	
Croatie		✓		✓
République tchèque	✓		✓	
Danemark	✓		✓	
Estonie	✓		✓	
Finlande		✓		✓
France	✓		✓	
Géorgie		✓		✓
Allemagne	✓		✓	
Grèce	✓		✓	
Hongrie	✓		✓	
Irlande	✓		✓	
Lettonie	✓		✓	
Lituanie	✓		✓	
Malte		✓		✓
Monténégro	✓		✓	
Norvège	✓		✓	
Pologne	✓		✓	
Portugal	✓			
Roumanie	✓		✓	
Fédération de Russie	✓		✓	
Serbie		✓		✓
République slovaque		✓	✓	
Espagne	✓		✓	
Suède	✓		✓	
Suisse	✓		✓	
Turquie	✓		✓	
Ukraine		✓		✓
Royaume-Uni (Angleterre & Pays-de-Galles)	✓		✓	

Partie C. Les questions de fond relatives à la nature de la preuve électronique

Préambule

50. Dans une certaine mesure, la preuve électronique est encore un concept relativement nouveau. L'objectif, dans cette section, est de soulever des questions qui permettent d'évaluer comment les différentes juridictions appréhendent les preuves électroniques dans les procédures judiciaires. L'article 9 de la Directive européenne 2000/31 sur le commerce électronique impose aux États membres d'intégrer dans leurs systèmes juridiques les contrats électroniques de sorte que cela ne crée pas d'obstacles pour leur validité ; voir aussi l'article 4-2 de la Directive européenne 1999/93 sur les signatures électroniques.

51. Question 8
Veuillez définir les classifications des preuves, le cas échéant, comment la preuve électronique s'inscrit dans cette classification. Par exemple, existe-t-il certains types de preuves électroniques qui sont présumés authentiques et fiables et existe-t-il d'autres formes de preuve dites imparfaites ?

Analyse des réponses à la question 8

52. Pour les explications détaillées concernant chaque juridiction, voir les réponses individuelle et la synthèse présentée dans le tableau concernant cette question ; toutefois, en général, la preuve est présumée fiable à moins de contestation.

53. Question 9
Existe-t-il dans votre juridiction une présomption en vertu de laquelle les preuves électroniques sont considérées comme « fiables », « recevables », « précises », « convenablement définies ou calibrées » ou « fonctionnant convenablement » ?

Analyse des réponses à la question 9

54. Il existe une présomption de ce type en Angleterre & au Pays-de-Galles, introduite par la Commission des Lois, qui est critiquée[5]. La présomption que toute preuve est présumée fiable s'applique en Estonie, étant entendu cependant que si la partie adverse conteste la preuve, cette dernière doit alors être authentifiée. En Hongrie, la situation dépend des méthodes utilisées pour la signature du document. Il n'y a pas de certitude en ce qui concerne la situation au Monténégro. En Roumanie, l'article 265(a) du Nouveau Code de procédure civile dispose que « l'entrée de données à partir d'un instrument légal sur un ordinateur est présumée donner des garanties suffisamment pertinentes de sa fiabilité si cette entrée est réalisée de manière systématisée et sans ruptures et lorsque les données informatisées sont protégées contre toutes altérations et contrefaçons de sorte que l'intégrité du document est totalement assurée ». En Fédération de Russie, il y a une présomption lorsque les données électroniques sont obtenues de la manière prévue par la loi. Au Portugal et en Espagne, une présomption s'appliquera, si les données sous forme numérique sont « signées » par une signature électronique avancée. Dans les autres juridictions ayant transmis une réponse, il n'y a pas de présomption de ce type.

[5] Pour une critique détaillée, voir Stephen Mason, éditeur de l'ouvrage, *Electronic Evidence* (3e édition, LexisNexis Butterworths, 2012) chapitre 5.

Tableau 3

Réponses aux questions 8 et 9

	8	**9**	
		Oui	Non
Andorre	Les parties doivent produire les preuves électroniques en tant que preuve documentaire privée, ce qui permet à la partie adverse de la contester en produisant des preuves de nature similaire.		✓
Arménie	La preuve électronique est classée dans les preuves écrites, voir pour ces dernières l'article 54 du Code de procédure civile.		✓
Belgique	Le Code civil belge reconnaît cinq types de preuve : la preuve documentaire (documents certifiés, accords privés signés), la preuve orale, la présomption, la confession et les déclarations faites sous serment. La loi n'établit aucune catégorie de preuve pour les preuves électroniques. L'article 1322 du Code civil, et l'article XII.15 du Code de droit économique, répètent la définition des documents électroniques posée dans la Loi du 11 mars 2003 sur un certain nombre d'aspects légaux relatifs aux services de la société de l'information.		✓
Bulgarie	L'évaluation de l'authenticité ou de la fiabilité de la preuve est établie dans le cadre des articles 193 et 194 du code de procédure civile		✓
République tchèque	L'utilisation de preuves électroniques n'est pas expressément réglementée en droit civil ou dans la branche administrative du droit tchèque. La Loi n° 300/2008 Coll. sur les actes électroniques et sur la conversion autorisée de documents contient des dispositions sur la conversion autorisée de documents. Les documents écrits originaux peuvent être convertis par une conversion autorisée en une version numérique et dans l'autre sens. Les documents convertis sont produits avec une clause d'authentification certifiant l'unité des documents entrés et sortis. De ce fait, il est possible de présenter des preuves écrites sous forme électronique et réciproquement. La Loi n° 300/2008 Coll. prévoit aussi qu'un document créé au moyen d'une conversion a les mêmes effets juridiques qu'une copie	✓	

	certifiée du document original.		
Danemark	Il n'y a pas de classification des preuves.		✓
Estonie	Toute preuve est présumée fiable à moins que la partie adverse ne la conteste, auquel cas la partie ayant présenté la preuve devrait communiquer des métadonnées ou introduire une requête auprès d'un tribunal pour obtenir les métadonnées.	✓	
Finlande	Conformément au Code de procédure judiciaire, les catégories de preuve sont les suivantes : (i) audition d'une partie à des fins de recueil de preuve, (ii) témoins, (iii) témoins experts, (iv) documents et (v) inspection judiciaire d'un objet. La preuve électronique est jugée être un document lorsqu'une question concerne son contenu. Dans les autres cas, la preuve électronique peut être soumise à une inspection judiciaire.		✓
France	Le droit français fait la distinction entre la preuve écrite, la preuve testimoniale, la présomption, l'admission et le serment. La preuve écrite peut prendre la forme d'un document privé ou d'un document authentique, en vertu de la distinction opérée par l'article 1317 du Code civil. La valeur probante de l'instrument est particulièrement forte puisqu'il est considéré comme faisant autorité jusqu'à preuve du contraire. L'écrit sous forme électronique a la même valeur que l'écrit sous forme papier, comme prévu à l'article 1316-1 du Code civil. Un instrument authentique peut en outre être établi sur un support électronique, en vertu des termes du deuxième paragraphe de l'article 1317, comme cité plus haut. Toutes les formes de preuve n'ont pas la même force probante, l'écrit prenant le pas sur la preuve par témoignage. Une admission est une déclaration par laquelle une personne reconnaît comme vrai, et devant être considéré comme prouvé à son égard, un fait susceptible d'entraîner des conséquences légales pour elle. La déclaration peut être judiciaire ou extrajudiciaire. Dans le premier cas, elle est indivisible et constitue une preuve concluante, puisqu'en vertu de l'article 1356 du Code civil, elle est réputée être une preuve pleinement authentique à l'encontre de la personne auteur de l'admission. Dans le deuxième cas, sa valeur probante est laissée à la discrétion de la cour.		✓

Géorgie	Le Code de procédure pénale de la Géorgie prévoit 5 types de preuves : les clarifications des parties, la preuve écrite, la preuve matérielle, le témoignage et l'opinion d'expert. Les dispositions relatives à la preuve électronique figurent sous l'intitulé Preuve écrite. Conformément à l'article 134 du Code, un document électronique confirmé par l'utilisation d'une signature électronique telle que définie dans la Loi géorgienne sur la signature électronique et sur les documents électroniques devrait avoir force probante. L'article 3 de la Loi prévoit que le tribunal ne peut déclarer la preuve irrecevable au simple motif qu'elle est produite sous forme électronique.		✓
Allemagne	La section 371a para.1 du ZPO prévoit que les règles concernant la valeur probante de registres et documents privés s'appliquent mutatis mutandis aux documents électroniques privés portant une signature électronique qualifiée. L'apparence de l'authenticité d'une déclaration disponible sous forme électronique, telle qu'obtenue après son examen selon la Loi sur la signature électronique Signaturgesetz), ne peut être mise en doute que par des faits faisant sérieusement doute du fait que la déclaration a été faite par le détenteur de la clé de signature. En l'absence de signature électronique qualifiée, les règles de la preuve visuelle s'appliquent (Sect. 371 Para. 1 ZPO). Si des documents électroniques sont créés conformément aux exigences de forme (documents électroniques publics) par une autorité publique dans le cadre de ses missions officielles, ou par une personne physique ou morale investie de la confiance du public dans la sphère d'activités qui lui est assignée, la section 317a para. 3 prévoit que les règles relatives à la valeur probante de registres et documents publics s'appliqueront mutatis mutandis. Un document portant une signature électronique qualifiée de l'autorité publique qui l'a créé sera présumé authentique. Ceci vaut aussi dans le cas d'un fournisseur de services accrédité qui fournit un document au nom de l'autorité publique qui a créé ce dernier, lorsque le document est fourni au nom de la personne physique ou morale détentrice de la confiance publique qui a créé ledit document avec sa signature électronique qualifiée conformément à la section 5 (5) de la Loi sur *De-Mail*, et que l'authentification de l'expéditeur identifie l'autorité publique auteur du document ou la personne physique ou morale détentrice de	✓	

	la confiance publique comme utilisatrices du compte De-Mail, ou la personne physique ou morale détentrice de la confiance publique. Pour ce qui est de registres ou documents publics qui ont été transformés, par l'utilisation d'une technologie relevant de l'état de l'art, en documents électroniques par une autorité publique, ou par une personne détentrice de la confiance publique, et de documents électroniques créés par une autorité publique dans le cadre de ses missions officielles, les règles concernant la valeur probante des registres et documents publics s'appliquent lorsqu'il est possible d'obtenir conformation que le document électronique est une copie fidèle et correcte de l'original, tant sous la forme d'une image que pour son contenu. Lorsque le document et la confirmation portent une signature électronique qualifiée, l'authenticité est présumée (section 371b ZPO).		
Grèce	Le Code de procédure civile grec ne contient aucune disposition spéciale concernant l'utilisation de la preuve électronique. Son article 339 prévoit ce qui suit : « Les moyens de preuve sont les suivants : la confession, l'autopsie, l'expertise, les documents, l'examen des positions des parties au litige, les témoins et les présomptions judiciaires. », ce qui veut dire que la preuve électronique relève, dans la structure des preuves, de la définition des documents. Voir la compilation jointe des réponses pour plus de détails.		✓
Hongrie	L'article 166 (1) du code de procedure civile dispose que les moyens de preuve englobent les témoignages, avis d'experts, inspections, documents et autres preuves matérielles. Dans cette liste d'exemples, la preuve électronique peut être classée comme objet soumis à inspection, document électronique ou autre preuve matérielle, mais elle peut aussi former une catégorie indépendante indéterminée.	✓	
Irlande	La classification des preuves en droit irlandais prévoit le témoignage oral, la preuve réelle et la preuve documentaire. Les données électroniques peuvent être des preuves réelles dans la mesure où elles sont un objet dont l'existence ou le caractère sont pertinents pour la question objet du procès. De ce point de vue, elle bénéficie du même traitement que les documents.		✓

Italie	Le système italien permet aux parties de produire tout document ou autre preuve sous toute forme possible.		✓
Lettonie	Les catégories de preuve sont les explications des parties et de tiers, les témoignages de témoins, la preuve documentaire, la preuve par démonstration, l'examen d'experts et l'opinion d'associations de personnes. La preuve électronique est assimilée à la preuve documentaire. La cour évalue la recevabilité de la preuve. Une preuve produite par une autorité publique est considérée comme fiable et crédible. La cour examine avec davantage d'attention les preuves produites par des personnes privées si elle a des raisons de douter de ces preuves.		✓
Lituanie	Voir la compilation de réponses jointe.		✓
Malte	La preuve peut être soit une preuve orale, soit une preuve documentaire: code de l'organisation et de la procédure civile – Chapitre 12 des Lois de Malte. La preuve électronique relève de la catégorie des preuves documentaires.		✓
Monténégro	Il n'y a pas de classification des preuves. Toutes ont le même pouvoir en droit. S'agissant de documents publics – autrement dit émis sous la forme prescrite par une autorité publique dans le cadre de ses compétences – et de documents émis sous cette forme par une entreprise ou autre groupement dans l'exercice de ses pouvoirs publics conférés par la loi, ils sont considérés comme fidèles, bien qu'il soit possible de prouver le contraire (article 226 de la Loi sur la procédure civile). Si un document public est produit sous forme électronique, ces mêmes dispositions s'appliquent.		✓
Norvège	La Loi sur les litiges classe les preuves en trois catégories : témoignages, preuve fournie par expertise et preuve réelle. La preuve électronique est une forme de preuve réelle. La classification décide uniquement quel jeu de règles de procédure devrait être suivi lors de la présentation de la preuve en justice et n'entraîne aucune présomption d'authenticité ou de fiabilité de la preuve. Le droit norvégien ne fonctionne pas avec des règles générales de preuve. L'authenticité et la fiabilité des preuves sont tranchées au cas par cas par la cour, qui		✓

	évalue librement les faits. Il n'y a pas de présomptions concernant la fiabilité ou l'authenticité de la preuve électronique.		
Pologne	Il n'y a pas de classification spécifique de la preuve électronique. A titre d'exemple, le courriel standard (depuis l'adresse de l'utilisateur@nom de domaine) peut être considéré comme une communication anonyme. L'indication du nom dans l'adresse électronique ne sera probablement pas considérée comme équivalent à une signature. Le même raisonnement s'appliquera à l'indication de details personnels dans le message. Il est possible également que le contrôle exercé par l'utilisateur sur l'accès à un compe de messagerie (partagé ou non avec d'autres personnes) puisse être pris en compte.		✓
Portugal	Le Décret-Loi 290 D/99, du 02-08 (amendé et republié par le Décret-Loi 88/2009, du 09-04), régit la légalité, l'efficacité et la valeur probante des documents électroniques et signatures numériques. Les formulaires électroniques et autres communications électroniques sont considérés comme des documents électroniques. L'article 2(a) du Décret-Loi 290 D/99, du 02-08 (amendé et republié par le Décret-Loi 88/2009, du 09 avril) précise qu'un document électronique est un document produit par traitement électronique de données.	✓	
Roumanie	Des instruments juridiques ou des faits peuvent être prouvés au moyen de documents écrits, de témoins, de présomptions, de déclarations par l'une des parties, faites spontanément ou durant un interrogatoire, par des rapports d'experts, au moyen de preuves matérielles, d'investigation sur les lieux et par tous autres moyens prévus par la loi (article 250 du Nouveau Code de procédure civile). Pour ce qui est de la preuve écrite, le nouveau Code de procédure civile a introduit des règles concernant des documents en format lisible informatiquement (article 266 et articles 282-284) et en format électronique (article 267).	✓	
Fédération de Russie	Dans la législation de la Fédération de Russie, la preuve électronique ne fait pas l'objet d'une classification distincte dans les divers moyens de preuve et elle est examinée comme un document (preuve documentaire) ou une preuve physique.	✓	

	En vertu de l'article 26.7 Partie 2 du CAO de la FR, le document peut contenir des informations enregistrées à la fois par écrit et sous une autre forme, par exemple les matériaux obtenus par photographie et film, enregistrements sonores et vidéo, extraits de bases de données et banques de données et autres supports. Lorsque les documents portent les signatures visées à l'article 26.6 du CAO de la FR, ils sont considérés comme une preuve physique. *Voir la réponse pour une analyse détaillée de la situation*.		
Serbie	Pas de réponse.		✓
République slovaque	La classification des preuves est énumérée à l'article 125 du Code de procédure civile. La preuve est tout moyen permettant d'établir l'état d'une affaire, essentiellement par déposition ou témoignages, opinions d'expert, déclarations et opinions émanant d'autorités publiques, de personnes physiques ou morales, documentation écrite, examen sur les lieux et interrogatoire des participants à l'affaire. Il n'y a pas de règle spécifique s'appliquant à la preuve électronique en ce qui concerne son authenticité ou sa fiabilité. Des règles générales s'appliquent tout comme pour tous les documents écrits. La cour décide de la manière dont la preuve doit être administrée, à moins que cette dernière ne soit produite dans un but spécifique.		✓
Espagne	Toutes les questions touchant la preuve électronique sont régies par des règles générales ou des dispositions établies pour la preuve classique ou normale. Il n'y a pas de règles spécifiques ou différentes devant être appliquées à la preuve électronique.		✓
Suède	Le droit procédural suédois s'appuie sur les principes de la libre production et de la libre évaluation de la preuve. En vertu de ces principes, tout ce qui peut avoir valeur de preuve dans une affaire peut, en principe, être présenté à l'audience principale. De plus, la preuve ne se voit pas accorder de valeur probante particulière sui generis. Le juge, en tenant compte des circonstances en l'espèce, évalue la valeur probante.		✓

Suisse	Il n'y a pas de classification des preuves. Le principe de la libre appréciation et évaluation de la preuve s'applique (Article 157 CPC).		✓
Turquie	Les types de preuve sont établis dans le Code de procédure civile numéroté 6100. Il s'agit de documents et factures, commencement de preuve, serment, témoin, expert, visionnage et opinion d'expert. Les données électroniques sont acceptées comme documents conformément à l'article 199 de ce Code. En vertu de l'article 205, les données électroniques portant une signature électronique sécurisée sont considérées comme une facture électronique.		✓
Ukraine	Pas de réponse.		✓
Royaume-Uni (Angleterre & Pays-de-Galles)	Il y a globalement deux types de preuves : la preuve directe et la preuve indirecte. L'existence d'un objet physique est une preuve directe ; la preuve indirecte couvre des faits pouvant être inférés de la preuve directe. Il existe aussi une définition de juristes comme dans « preuve réelle », définie comme une preuve matérielle produite sans intervention humaine. La preuve électronique relève de toutes ces classifications. Pour ce qui est de la preuve, les règles générales sont que le juge admettra pratiquement toute preuve et qu'il revient aux parties de faire valoir leur point de vue quant à la valeur probante qu'il conviendrait de lui accorder.	✓	

Partie D L'admissibilité et l'authenticité de la preuve électronique

Préambule

55. De nombreuses juridictions ont introduit l'admissibilité de la preuve électronique dans leurs procédures juridiques. Cette question a également été abordée à l'échelle régionale, telles que les dispositions de l'article 5 (2) de la Directive de l'Union européenne 1999/93/CE du Parlement européen et du Conseil du 13 Décembre 1999 sur un cadre communautaire pour les signatures électroniques[6], qui prévoit que « l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que la signature se présente sous forme électronique ». De même, la disposition de l'article 9 (1) de la Directive européenne 2000/31 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 »)[7], prévoit que les contrats ne seront pas privés de leur efficacité et de leur validité juridique parce qu'ils ont été conclus par voie électronique. Il est généralement admis que les preuves sous forme électronique sont recevables dans les procédures judiciaires. La règlementation incluerait :

(i) si la preuve doit être obtenue conformément à une orientation technique, (par exemple, des lignes directrices applicables en procédure pénale, et elles pourraient s'avérer utiles pour les procédures civiles et administratives)[8], et

(ii) la manière dont l'authenticité et la fiabilité de la preuve électronique est déterminée - à savoir s'il existe des lignes directrices admises pouvant aider un juge à déterminer l'authenticité de la preuve électronique, et s'il y a une présomption quant à la «fiabilité» de la preuve électronique.

56. Question 10
Si une partie souhaite soumettre des éléments de preuve électronique dans les procédures civiles ou administratives, est-il nécessaire de recourir à une procédure spécifique, tel que requis par la loi ou autres textes règlementaires?

Analyse des réponses à la question 10

57. Aucun Etat membre n'a d'obligation légale d'obtenir la preuve électronique selon une procédure spécifique.

58. En-dehors de l'obligation d'obtenir la preuve au moyen d'une procédure spéciale, en Croatie, la Loi sur les documents électroniques traite des copies de documents électroniques (on suppose qu'il s'agit du contenu de ces documents, puisqu'il n'y a pas de référence aux métadonnées) imprimées en version papier. En Angleterre & au Pays-de-Galles, les règles procédurales civiles s'appliquent à toutes les actions en justice civiles. En Grèce, les dispositions du Décret présidentiel 150/2013 fixent les principes et conditions

[6] JO L 13 du 19.1.2000, p.12. La directive est abrogée par le 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 et abrogeant la directive 1999/93/CE, JO L 257, 28.8.2014, pp. 73-114.
[7] JO L 178, 17.7.2000, pp. 0001 – 0016.
[8] Par exemple : *Guidelines for Best Practice in the Forensic Examination of Digital Technology*, Version 6 (20 April 2009), European Network of Forensic Science Institutes, Forensic Information Technology Working Group, consultable sur http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf; UK Association of Chief Police Officers 'Good Practice Guide for Digital Evidence', Version 5 (octobre 2011), consultable sur http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf.

qu'une partie est tenue de respecter lorsqu'elle produit une preuve électronique. Le premier article du Décret exige que la preuve électronique dans une procédure civile soit accompagnée d'une signature électronique avancée. En Fédération de Russie, la preuve électronique doit respecter les conditions édictées dans les lois fédérales applicables, notamment le Code civil et la Loi fédérale du 6 avril 2011 n° 63-FZ sur la signature électronique.

59. Question 11
Si la preuve électronique n'est pas obtenue, conformément à une procédure standard ou spéciale, le tribunal prendra-t'il en considération cet élément lorsqu'il jugera de l'opportunité d'admettre la preuve en question ?

Analyse des réponses à la question 11

60. En général, le tribunal évaluera la preuve qui lui est présentée dans le cours normal de la procédure judiciaire, en prenant en considération toutes les preuves techniques présentées. Dans certaines juridictions, le juge décidera quelle preuve recevoir et quelle preuve devra être testée sur le plan de l'authenticité.

61. En Grèce, tout dépend des faits en l'espèce. Bien que le Décret présidentiel 150/2013 ne contienne pas de dispositions spécifiques, lors de l'examen d'une interprétation analogue d'autres procédures du Code civil, à savoir un document privé –, lorsque la preuve électronique n'est pas obtenue selon une norme ou une procédure données, elle n'a pas la valeur probante d'un document privé et peut être considérée comme un document qui ne contient pas tous les éléments prérequis par la loi, et le juge peut donc librement estimer qu'il s'agit d'une preuve qui n'est pas conforme aux exigences en vue de la production de document privé.

61. Question 12
Si ce n'est pas déjà mentionné ailleurs dans vos réponses, existe-t-il des lignes directrices techniques ou des bonnes pratiques publiées dans votre pays et qui décrivent comment la preuve électronique peut être obtenue tout en conservant son intégrité?

Analyse des réponses à la question 12

63. Des lignes directrices ont été élaborées en Pologne (en polonais seulement – voir la compilation des réponses jointe pour plus de détails), mais on ne sait clairement si elles se réfèrent aux procédures civiles ou aux procédures pénales. En Angleterre & au Pays-de-Galles, il existe des lignes directrices pour les affaires pénales, mais pas pour les affaires civiles, comme indiqué dans le questionnaire.

64. En Belgique, il existe des présomptions liées à l'utilisation d'une signature électronique avancée. En Allemagne, il existe une présomption limitée concernant l'intégrité lorsqu'un individu s'est enregistré de façon sécurisée pour l'ouverture d'un compte « De-Mail » dont il est l'unique détenteur (section 4(1), deuxième phrase, de la Loi sur De-Mail). L'apparence d'authenticité que présente un message électronique expédié depuis un compte 'De-Mail », obtenue grâce à la vérification de l'authentification de l'expéditeur conformément à la section 5(5) de la Loi sur De-Mail, ne sera contestée que s'il existe des faits permettant de remettre sérieusement en doute le fait que le message avec ce contenu a bien été envoyé par cet individu (section 371a Para 2 Code de procédure civile).

65. Au Monténégro, la Loi sur la signature électronique permet de créer un ensemble de règles concernant les signatures électroniques avancées qui, si elles sont appliquées, assure une présomption de fiabilité.

66. Question 13
Est-ce que les règles sur la recevabilité de la preuve électronique varient selon la complexité ou la simplicité de la preuve ?

Analyse des réponses à la question 13

67. Les règles sur la recevabilité de la preuve électronique ont tendance à ne pas varier en fonction de la complexité ou de la simplicité de la preuve. En Belgique et en Espagne, l'utilisation d'une signature électronique avancée annexée ou intégrée à des données numérique permettra de faciliter la démonstration de l'authenticité.

Tableau 4

Réponses aux questions10 – 13

	10		11		12		13	
	Oui	Non	Oui	Non	Oui	Non	Oui	Non
Andorre		✓		✓		✓		✓
Arménie		✓		✓		✓		✓
Belgique		✓		✓		✓		✓
Bulgarie		✓		✓		✓		✓
Croatie	✓		✓			✓		✓
République tchèque		✓		✓		✓		✓
Danemark		✓		✓		✓		✓
Estonie		✓		✓		✓		✓
Finlande		✓		✓		✓		✓
France		✓		✓				✓
Géorgie		✓		✓		✓		✓
Allemagne		✓		✓		✓		✓
Grèce		✓	✓			✓		✓
Hongrie		✓		✓		✓		✓
Irlande		✓		✓		✓		✓
Lettonie		✓		✓		✓		✓
Lituanie		✓		✓		✓		✓
Malte		✓		✓		✓		✓
Monténégro		✓		✓		✓		✓
Pologne		✓		✓	✓			✓
Portugal		✓		✓		✓		✓
Roumanie		✓		✓				✓
Fédération de Russie		✓		✓		✓		✓
Serbie		✓		✓		✓		✓
République slovaque		✓		✓		✓		✓
Espagne		✓		✓		✓		✓
Suède		✓		✓		✓		✓
Suisse		✓		✓		✓		✓
Turquie		✓		✓		✓		✓
Ukraine		✓		✓		✓		✓
Royaume-Uni (Angleterre & Pays-de-Galles)		✓		✓		✓		✓

Partie E L'archivage de la preuve après le procès

Préambule

68. La preuve électronique doit être traitée différemment des fichiers papier et des pièces à conviction. En imprimant des documents électroniques, les métadonnées pertinentes qui tendent à prouver l'authenticité du document seront perdues. Cela signifie qu'il est nécessaire de conserver les données électroniques sous leur forme originale de la même manière que la conservation d'un dossier physique. Dans une certaine mesure, il est nécessaire pour les avocats et les administrateurs judiciaires d'assurer la confidentialité et la sécurité de ces données électroniques, y compris la conservation des copies de sauvegarde sécurisées dans le cas où il surviendrait un incident sur un autre moyen de stockage.

69. Le Conseil des barreaux européens (CCBE) a produit un ensemble de directives traitant spécifiquement du «cloud computing», qui tendent à rejoindre cette étude, cependant il n'y a pas d'autres directives produites par le CCBE qui couvrent directement ce sujet[9].

70. Question 14

Quelles sont les normes ou conduites professionnelles, le cas échéant, relatives à l'obligation et aux exigences à respecter pour le stockage et la préservation de preuves électroniques ?

En répondant à cette question, veuillez couvrir les domaines suivants:

Archivage par les avocats ;

Archivage par les greffes du tribunal ;

Exigences à mettre en place pour la sécurité des preuves après le procès.

Analyse des réponses à la question 14

71. Les réponses à la question 14 varient sensiblement. La large gamme des réponses reflète le fort degré d'incertitude qu'il semble y avoir à l'égard des dispositions relatives à l'archivage, et plus inquiétant, de la sécurité qui devrait accompagner les documents électroniques. Ainsi, une des juridictions, l'Angleterre & le Pays-de-Galles (choisie du fait que Stephen Mason y exerce), est donnée en exemple plus en détail ci-après :

Archivage par les avocats

Il y a obligation de préserver les preuves tant que la procédure judiciaire est en cours et qu'il existe une possibilité de recours.

De manière général, les sollicitors ont toujours été responsables de la conservation des dossiers des clients (et donc des preuves présentées au procès). Une fois le procès terminé, le barrister, s'il y en a un, rendra les fichiers au solicitor. Or le numérique a complexifié ce processus, puisque le barrister sera en possession des copies électroniques des preuves et instructions, à moins qu'il ne soit décidé d'expurger toute preuve de ces données des ordinateurs ou serveurs. En pratique, les barristers conserveront la plus grande partie des preuves sous forme électronique.

[9] Lignes directrices du CCBE sur l'usage des services d'informatique en nuage par les avocats consultables sur le site http://www.ccbe.eu.

La Law Society d'Angleterre & Pays-de-Galles et le Barreau d'Angleterre & Pays-de-Galles donnent des orientations distinctes concernant la conservation d'archives – et par extension, de celle des preuves après le procès. Un texte couvre ce domaine[10], et il existe un certain nombre de guides pratiques : *Information security* (11 octobre 2011),[11] *File retention: trusts* (6 octobre 2011),[12] et *File retention: wills and probate* (6 octobre 2011)[13].

Il n'y a pas de conseils spécifiques concernant la conservation des preuves après le procès, mais la Law Society d'Angleterre & Pays-de-Galles se réfère aux dispositions pertinentes de la Loi sur la prescription (Limitation Act) de 1980, à la Loi sur la taxe à la valeur ajoutée (Value Added Tax Act) de 1994, à la Loi sur la protection des données (Data Protection Act) de 1998 et aux réglementations en matière de blanchiment de capitaux (Money Laundering Regulations) de 2007 (2007 SI 2157). En général, le solicitor indique sur le dossier la période à la fin de laquelle celui-ci doit être revu et l'envoie au partenaire responsable pour décision à la fin de la période indiquée. Dans la pratique, la plupart des partenaires n'ont pas le temps de procéder à cet examen, et on se contente en général de stocker les dossiers physiques et leur contenu et de ne plus y toucher.

Le Barreau d'Angleterre & Pays-de-Galles a publié sur ce sujet les Lignes directrices sur la sécurité de l'information (*Guidelines on Information Security)*[14] et les Lignes directrices concernant les courriels pour le Barreau (*Email Guidelines for the Bar*)[15]. Les *barristers* qualifiés pour donner des conseils juridiques et assurer une représentation directe au public peuvent se référer au document *Public Access Guidance for Barristers* (janvier 2014) qui contient des conseils sur ce sujet[16].

Archivage par les tribunaux

Les documents des dossiers de tribunaux doivent être conservés pendant l'année en cours plus 7 à 12 ans, selon la juridiction. Toutefois, les pièces sont en général rendues avant ce délai ou conservées, selon la nature des preuves et la possibilité d'une poursuite de l'action.

On ne dispose pas d'informations détaillées sur cette question.

[10] Andrew Hopper QC, Cartwright Black et Iain Miller, gen eds, *Cordery on Legal Services* (LexisNexis Butterworths), monographie.

[11] http://www.lawsociety.org.Royaume-Uni/advice/practice-notes/information-security/.

[12] http://www.lawsociety.org.Royaume-Uni/advice/practice-notes/file-retention-trusts/.

[13] http://www.lawsociety.org.Royaume-Uni/advice/practice-notes/file-retention-wills-probate/.

[14] http://www.barcouncil.org.Royaume-Uni/for-the-bar/professional-practice-and-ethics/it-panel-articles/guidelines-on-information-security/.

[15] http://www.barcouncil.org.Royaume-Uni/for-the-bar/professional-practice-and-ethics/it-panel-articles/email-guidelines-for-the-bar/.

[16] https://www.barstandardsboard.org.Royaume-Uni/media/1580337/public_access_guidance_for_barristers_-_jan_2014.pdf.

Exigences d'assurer la sécurité des preuves après un procès

Les dispositions de la Loi de 1998 sur la protection des données s'applique à tous les avocats, et il est donc possible de faire valoir que tous les avocats doivent assurer la sécurité des données électroniques, indépendamment de toutes règles ou lignes directrices professionnelles.

Le document *Information security* (11 octobre 2011) de la Law Society[17] contient des observations qui couvrent un champ très large, avec peu de fonds, concernant la sécurité des données électroniques. Les Solicitors sont renvoyés à un texte spécifique, de Keith Mathieson, *Privacy Law Handbook* (Law Society Publishing, 2010).

De plus, le Code de déontologie de la *Solicitors Regulation Authority*[18] pose un certain nombre de Principes contraignants qu'un solicitor est tenu d'appliquer. Au Chapitre 7, 'Gestion de votre activité', on trouve un certain nombre d'objectifs que tout solicitor doit respecter. Une série d'indicateurs comportementaux, s'ils sont suivis, peuvent prouver que le solicitor a atteint les objectifs et s'est donc conformé aux Principes. Les principes ci-dessous sont applicables pour garantir la sécurité des données électroniques :

> IB(7.1)
> Garder en lieu sûr les documents et éléments de valeur confiés au cabinet ;
>
> IB(7.3)
> Identifier et suivre les risques financiers, opérationnels et en matière de continuité des activités, notamment les plaintes, les risques et l'exposition en termes de crédits, les plaintes en vertu de dispositions légales relatives à des questions telles que la protection des données, les pannes et abus informatiques et les dommages aux locaux professionnels.

Le Barreau d'Angleterre & Pays-de-Galles (*Bar of England & Wales)* donne des orientations en matière de sécurité des données électroniques dans les Lignes directrices sur la sécurité de l'information (*Guidelines on Information Security*[19]*).* Toutefois, ces lignes directrices ne font pas partie du Code de déontologie et le fait de les suivre ne protège pas nécessairement desz plaintes pour violation ou respect insuffisant des obligations de service professionnel. Le barrister est responsable personnellement de la préservation de la confidentialité des affaires de ses clients.

72. La réponse du ministère de la Justice du Royaume-Uni montre que l'archivage et la sécurité ne semblent pas entièrement inconnus mais que, pour ce qui est des données en format électronique, les conséquences ne semblent pas encore totalement comprises.

[17] http://www.lawsociety.org.Royaume-Uni/advice/practice-notes/information-security/.

[18] http://www.sra.org.Royaume-Uni/solicitors/handbook/code/content.page.

[19] http://www.barcouncil.org.Royaume-Uni/for-the-bar/professional-practice-and-ethics/it-panel-articles/guidelines-on-information-security/, pp. 18 – 27.

Tableau 5

Réponses à la question 14

	Réponse
Andorre	L'article 60 de la Loi qualifiée sur la justice, du 3 septembre 1993, telle que modifiée fin 2014, prévoit que la responsabilité de la préservation et du stockage de tous les documents et archives, ainsi que de la conservation de biens et objets faisant partie des dossiers des affaires, ou qui y ont été assignés, incombe au greffier de chaque tribunal.
Arménie	Il n'y a pas de réglementation légale ou de dispositions relatives à la conduite professionnelle applicables aux tribunaux ou aux avocats concernant le stockage et la préservation des preuves électroniques. L'article 7 de la Loi sur le document électronique et la signature électronique dispose : Article 7. Stockage des documents électroniques Un document électronique est réputé avoir été stocké de manière adéquate s'il n'a subi aucun changement depuis son stockage initial, ou si les éventuels changements subis sont dus aux contraintes liées à son stockage, et s'il est possible de restaurer le document sous sa forme antérieure au stockage. Le document électronique dont la vérification se fait par une signature électronique est réputé avoir été stocké de manière adéquate si les données relatives à sa vérification par la signature ont également été conservées. Les propriétaires des systèmes d'information assurent la protection des documents électroniques stockés dans leurs systèmes d'information.
Belgique	Le droit belge ne prévoit pour l'instant pas de dispositions régissant l'archivage électronique. **Avocats** L'article 2276bis du Code civil régit l'archivage par les avocats ; il prévoit au § 1 que : « Les avocats sont déchargés de leur responsabilité professionnelle et de la conservation des pièces cinq ans après l'achèvement de leur mission. Cette prescription n'est pas applicable lorsque l'avocat a été constitué expressément dépositaire de pièces déterminées. » **Tribunaux** La Loi du 24 juin 1955 sur les archives [*Journal officiel le Moniteur belge*, 12 août 1955 et Décret royal du 18 août 2010 pour l'application des Articles 1, 5 et 6 bis de la Loi du 24 juin 1955 sur les archives (*Journal officiel le Moniteur belge*, 23 septembre 2010, Addendum, *Journal officiel le Moniteur belge*, 22 octobre 2010)] régit l'archivage en particulier par les greffiers des tribunaux.
République tchèque	**Avocats** Les avocats sont tenus de stocker la documentation et les dossiers des clients durant 5 ans après la fin de leur mission de représentation (article 3 de la Résolution du Conseil d'administration de l'Association tchèque du Barreau n° 9/1991). Cette règle s'applique également aux preuves électroniques. Il n'existe pas de règles particulières sur la manière de stocker ces dernières. **Tribunaux** Les preuves reçues sous forme électroniques sont archivées sur des disques portatifs et dans le système d'information des tribunaux. Dans d'autres cas, par exemple lorsque la preuve est le contenu d'une communication par messagerie électronique ou une copie d'écran actualisée d'une page de réseaux sociaux, elle est recueillie comme suit : la page est observée durant l'audition par le juge qui fait ensuite une copie écran imprimable du contenu affiché, laquelle sera ensuite

	imprimée sur papier et archivée dans le dossier de l'affaire. **Sécurité de la preuve après un procès** Les règles générales sur le stockage de la preuve s'appliquent aux preuves archivées sur des disques portatifs ; le stockage dans le système d'information des tribunaux est régi par les règles internes du ministère de la Justice.
Danemark	Il n'y a pas de normes de ce type, en particulier pour la preuve électronique.
Estonie	Les métadonnées d'un courriel/d'une page web sont normalement converties en PDF et/ou imprimées et stockées sous cette forme. Les dossiers concernant des signatures numériques sont stockés dans la base de données du tribunal (par exemple e-curia); des versions imprimées sont stockées en version papier.
Finlande	Les tribunaux sont tenus d'archiver les documents, documents visuels ou verbaux/oraux y compris les documents électroniques en vertu de la loi 831/1994 ("Loi sur l'archivage", pas de traduction transmise), qui doivent être préservés de manière à ce qu'ils ne soient pas détruits, endommagés ou utilisés à mauvais escient. Le Code de déontologie pour les avocats établi par l'Association du Barreau de Finlande prévoit des dispositions sur lasécurité des systèmes d'information (article 11.6) : « Un avocat doit s'assurer que la sécurité des systèmes d'information de son cabinet est telle qu'elle ne permet pas à des tiers de prendre connaissance des informations sur ses clients sans autorisation. » L'Association du Barreau de Finlande a également communiqué une ordonnance concernant la sécurité des informations et un manuel à l'appui de la situation (pas de traductions disponibles). L'ordonnance couvre, par exemple, les règles pour sécuriser l'ordinateur et autres dispositifs (mot de passe, protection antivirus, protection d'un ordinateur portable et du Wifi etc.) ainsi que des règles relatives à l'obligation de s'assurer de la sécurité des informations lors de la signature d'un contrat, par exemple avec une société informatique extérieure, et des règles de sécurité des archives.
France	En général, pour ce qui est des preuves, le principe de l'équivalence entre des documents électroniques et sur version papier découle du respect des conditions d'archivage nécessaires pour préserver l'intégrité desdits documents (article 1316 – 1 du Code civil). De même, un instrument authentique peut être établi sur un dispositif électronique uniquement s'il est stocké dans des conditions qui préservent son intégrité et sa lisibilité (article 1317 du Code civil). Un instrument notarié établi sur un support électronique est en conséquence enregistré dans un registre central des minutes notariales, en vue de sa conservation, dès qu'il a été établi par le notaire qui en atteste, lequel conserve l'accès exclusif à l'instrument (article 28 du décret du 26 novembre 1971, tel qu'amendé). En ce qui concerne la procédure, la capacité des processus techniques à garantir la conservation des transmissions réalisées est également une condition préalable à l'utilisation des communications électroniques (article 748 – 6 du Code de procédure civile). Pour ce qui concerne les huissiers de justice, la législation (article 26 du décret du 29 février 1956, tel qu'amendé par le décret du 10 août 2005) exige que les instruments originaux établis sur un support électronique le soient au moyen d'un système de traitement, d'archivage et de transmission des informations approuvé par la Chambre nationale des huissiers et garantissant l'intégrité et la confidentialité de leur contenu. **Avocats** Les documents originaux sont rendus au client après la clôture des procédures. L'article 2225 du Code civil prévoit une durée de cinq ans durant laquelle le client peut intenter une action en justice à l'encontre de son avocat en cas d'erreur. Cette période de prescription de cinq ans est une disposition légale relativement

	récente, introduite par une loi du 17 juin 2008. Les avocats sont tenus de conserver une copie des documents, y compris sous forme électronique, pendant au minimum cinq ans après la procédure. Toutefois, il convient de noter que, dans la pratique, les avocats conservent des copies de ces documents pour une période plus longue à titre de précaution. Un certain nombre d'affaires ont créé des précédents sur ce point, en particulier pour ce qui est de la détermination du moment où devrait commencer à courir la période de cinq ans. **Greffes des tribunaux** Conformément aux règles applicables aux autorités de l'Administration publique, tout archivage numérique réalisé par les tribunaux doit se faire dans le respect du modèle OAIS (Modèle de référence pour un Système d'information et d'archivage ouvert, publié par l'ISO sous la référence ISO 14721:2003).
Géorgie	Il n'y a pas de règles spécifiques sur cette question.
Allemagne	**Avocats** La norme relative aux devoirs et aux exigences des avocats en matière d'archivage et de préservation des dossiers est pour l'essentiel contenue dans le paragraphe 50 de la Loi fédérale sur les avocats (Bundesrechtsanwaltsordnung, BRAO), qui prévoit ce qui suit : BRAO § 50 Les dossiers du Rechtanswalt (1) Un Rechtsanwalt doit être en position de rendre compte convenablement de ses activités professionnelles. Pour cela, il faut créer des dossiers. (2) Le Rechtsanwalt doit conserver les dossiers pendant cinq ans après la fin d'une affaire. Toutefois, cette obligation tombe, même avant l'échéance des cinq ans, si le cabinet d'avocats a demandé au client de récupérer les dossiers et que le client n'a pas donné suite à cette demande dans les six mois de sa réception. (3) Un Rechtsanwalt peut refuser de remettre les dossiers au client tant qu'il n'a pas été réglé de ses frais et décaissements. Cette disposition ne s'applique pas dans le cas où il serait déraisonnable dans les circonstances en l'espèce de retenir les dossiers ou certains documents individuels. (4) Au sens des paragraphes 2 et 3 de cette disposition, il convient d'entendre par dossiers uniquement les documents que le Rechtsanwalt a reçus pour ou au nom du client dans le cadre de sa pratique professionnelle, mais non la correspondance entre le Rechtsanwalt et le client ni les documents pour lesquels le client a déjà reçu l'original ou une copie. (5) Les dispositions du paragraphe 4 s'appliquent en conséquence dès lors que le Rechtsanwalt utilise un traitement de données électroniques pour conserver des dossiers. En dehors de cette disposition, le Rechtsanwalt est soumis à l'obligation de base de respecter le secret professionnel (§ 43a, paragraphe 2 BRAO). **Tribunaux et exigence d'assurer la sécurité des preuves après un procès** Le Code de procédure civile ne contient pas de règles générales concernant des normes d'archivage par les tribunaux. Les règles sur l'archivage relèvent des différents Länder, qui ont chacun élaboré leurs propres règles (« Aktenordnung »). La section 298 a ZPO, dans sa version actuelle, précise par ailleurs ce qui suit: (1) Les archives du tribunal sur le litige peuvent être conservées sous forme électronique. Le Gouvernement fédéral et les gouvernements des Länder fixent, par instrument ayant force contraignante, dans leur champ de compétence, la durée pendant laquelle il convient de conserver les dossiers électroniques, ainsi que les conditions cadre en matière organisationnelle et technique régissant la création, l'administration et l'archivage des dossiers électroniques. Les gouvernements des Länder peuvent conférer, par instrument contraignant,

	l'autorisation correspondante aux services de la justice du Land. (2) Tous documents et autres archives soumis sous forme papier doivent être transférés sous forme électronique pour remplacer l'original. Si les documents et archives restent encore nécessaires sous format papier, ils doivent être archivés au moins jusqu'à ce que l'affaire ait été jugée. (3) Le document électronique doit inclure la mention de la date et de la personne qui a mis les documents sous forme électronique.
Grèce	**Avocats** Les avocats sont tenus de respecter certaines obligations en ce qui concerne leurs clients et les procédures devant un tribunal. Une fois que le procès a démarré (même si l'affaire est classée sans suite et n'est pas poursuivie, quelle qu'en soit l'issue), les avocats sont obligés de conserver tous les documents pertinents pendant au moins cinq ans (article 37 §8 du Code de conduite des avocats) ; la même obligation existe pour l'archivage des dossiers dans les greffes des tribunaux qui sont également conservés pendant au maximum 5 ans puis détruits. Le non-respect de ces dispositions peut entraîner pour l'avocat qui les a violées une action disciplinaire. En cas de violations graves, des sanctions pénales peuvent aussi être prononcées. Il a été soutenu qu'une fois qu'un avocat produit des preuves et des documents au tribunal, il n'en est plus propriétaire ; cela signifie qu'il ne peut les détruire délibérément ou les altérer par n'importe quel moyen, auquel cas il se rendrait responsable d'un détournement de documents et serait poursuivi pour ce délit pénal (article 222 du Code pénal) ou pour falsification (article 216 du Code pénal) respectivement, voir pour cela Cour suprême (5e chambre pénale) 566/2006 (AP (chambre pénale) 566/2006). **Tribunaux** Conformément aux dispositions de l'article 6 du Décret présidentiel 150/2013 concernant la procédure électronique devant les tribunaux civils, les tribunaux sont tenus d'obtenir et de conserver un fichier électronique de toutes les plaidoiries et de tous documents pertinents (preuves et documents de procédure) qui ont été présentés ainsi que de tout autre document électronique pertinent pour l'affaire. Toutes les archives électroniques préservées devraient respecter toutes les exigences et conditions en matière de sécurité et garantir l'intégrité, l'authenticité, la confidentialité et la qualité des documents et des données qu'ils comportent.
Hongrie	**Avocats** Les cabinets d'avocats et leur personnel, les services du ministère public, les représentants de ce dernier et leur personnel, de même que les personnes physiques et morales chargées de conserver, archiver, sauvegarder et traiter les données figurant dans des documents électroniques ou imprimés contenant des données relevant des informations confidentielles échangées entre le client et son conseil sont soumis à des obligations de confidentialité: paragraphe (4) de l'article 8 de la loi XI de 1998 régissant la profession d'avocat. En vertu de l'article 2(1) de l'arrêté n° 114/2007 (29 décembre) pris par le Ministre de l'Economie et des Transports concernant les règles en matière d'archivage digital, la partie tenue de sauvegarder des documents doit s'assurer que les documents électroniques le soient de manière à éviter tout risque de modification ultérieure et à empêcher que ces documents puissent être effacés, supprimés, détruits accidentellement ou endommagés, ou que l'on puisse y avoir accès sans autorisation. **Tribunaux** Aux termes de l'article 6(5) de la directive n° 17/2014 (23 décembre) de l'Office national de la Justice concernant les règles relatives aux documents gérés par les tribunaux, ceux-ci sont tenus de conserver les documents électroniques ainsi que les pièces de dossiers archivées électroniquement et les documents compilés

	dans le cadre de ses opérations courantes dans des archives électroniques. L'article 195(1) dispose que les documents que détiennent les tribunaux doivent être sauvegardés jusqu'à l'expiration du délai de garde ou jusqu'à la date de leur remise aux services d'archivage compétents.
Irlande	***Solicitors*** Dans les procédures civiles, les preuves originales sont versées au dossier du tribunal. Les *solicitors* conservent des copies des documents admis comme preuves dans leur dossier. La *Law Society of Ireland*, qui est l'organe professionnel dont relèvent les *solicitors* dans ce pays, a publié un Guide de conduite professionnelle pour les *solicitors* en Irlande, (*Guide to Professional Conduct of Solicitors in Irlande Law Society*, 2e édition 2002) qui prévoit au point 9.13 : « Afin de protéger les intérêts des clients qui peuvent faire l'objet d'une action en justice intentée par des tiers, mais également de protéger les intérêts du cabinet des *solicitors*, contre lequel d'anciens clients ou des tiers peuvent se retourner en justice, un *solicitor* doit veiller à ce que tous les dossiers, documents et autres archives soient conservés pour les périodes appropriées. » La référence à des « périodes appropriées » concerne les périodes de prescription à l'issue de procès, qui sont en général de 6 ans, mais peuvent aller jusqu'à 12 ans pour des contrats portant un sceau. Le Comité Technologies de la *Law Society of Ireland* a publié une Note pratique qui demande aux *solicitors* de conserver des documents liés à un litige en justice pendant au moins 6 ans, durée pendant laquelle les clients peuvent intenter une action en justice à l'encontre du *solicitor* concernant le contrat qui les lie à ce dernier, ainsi que pour assurer la disponibilité du dossier pour les assureurs professionnels du *solicitor.* La Note pratique précise que : « lorsque la documentation est convenablement archivée sous forme électronique (et sous réserve de toute période statutaire ou réglementaire de prescription concernant l'archivage ou la conservation sous forme électronique), la version papier (s'il en existait une) n'a pas à être conservée. Les trois problèmes principaux affectant l'archivage électronique sont la permanence ou la durabilité du format ; l'accessibilité du format ; la sécurité du format. » Lorsque des documents sont archivés sous forme électronique, la Note pratique exige que l'archivage se fasse dans un format ouvert afin de ne pas compromettre sa future accessibilité et disponibilité. ***Barristers*** Lorsque des *barristers* sont commis dans des affaires contentieuses, la documentation pertinente est incluse dans le dossier préparé pour le procès ou pour l'appel. Les dossiers sont retournés au *solicitor* qui a fait appel au *barrister* à la fin du procès ou de l'appel. Lorsque des *barristers* sont saisis de manière consultative, en général, ils renverront les documents annexés à l'affaire pour laquelle ils ont été retenus pour le conseil au *solicitor* qui les a saisis, avec l'opinion juridique ou les conseils selon le cas. **Tribunaux** Après la conclusion d'une procédure civile, le dossier papier contenant les plaidoiries et certains autres documents dont certains ont le caractère de preuves, par exemple des témoignages sous serment, est conservé sous la garde du Service des tribunaux (*Court Service*), une organisation indépendante établie par la Loi sur le Service des tribunaux, 1998, qui, entre autres choses, gère les tribunaux et apporte des services d'appui aux juges. Les pièces à convictions qui ont été présentées comme preuves sont rendues à la partie qui les a présentées. De même, dans la procédure pénale, les preuves

	telles que le disque ou la bande contenant des images vidéo sont rendues à l'autorité de poursuite ou à la partie défenderesse selon le cas. Il convient de noter que la nouvelle Cour d'appel a lancé un projet (financé par des fonds publics) pour faciliter l'archivage électronique, ce qui signifie qu'une bonne partie des informations d'une affaire, telles que les plaidoiries, pourraient être accessibles sous forme électronique. Les dossiers des tribunaux sont soumis aux dispositions de la Loi nationale sur l'archivage de 1986, et relèvent des « archives de services » (*Departmental Records*) régis par la sous-sous-section 1(2)(b) de la Loi. La section 7 de la Loi sur les archives nationales, de 1986, traite de la conservation et de la destruction des archives de services. La sous-section 7(1) prévoit que les archives de services qui n'ont pas été transférées aux Archives nationales conformément à la section 8 ou détruites conformément à la sous-section 7(5) doivent être conservées et préservées au sein du Ministère où elles ont été émises ou sont détenues. La sous-section 7(2) permet au Directeur ou à « l'agent désigné » d'autoriser dans certaines circonstances la destruction des archives de services, par exemple sur demande écrite du Ministère concerné lorsque les archives ne sont pas nécessaires pour l'administration de ce dernier ; lorsque le Directeur des Archives nationales ou l'agent désigné juge que les archives n'exigent pas une conservation par les Archives nationales. Dans le cas des archives de tribunaux, la sous-sous-section 7(4)(c) prévoit que le juge responsable du tribunal, dans le cas d'archives de la Cour suprême, ou le président de la Haute cour, pour les archives de la Haute cour, doit avaliser l'autorisation.
Lituanie	Il n'y a pas de règles spéciales concernant les obligations et les conditions d'archivage et de préservation des preuves électroniques. Les preuves électroniques soumises via le système d'information judiciaire de la Lituanie sont archivées par les tribunaux conformément au règlement n° 13P–74–(7.1.2) du 20 juin 2013 du Conseil judiciaire relatif aux règles applicables au traitement, à l'archivage et au stockage de données électroniques liées à des procédures judiciaires utilisant les technologies de l'information et de la communication.
Lettonie	Il n'y a pas de règles spéciales pour les tribunaux civils et administratifs concernant le stockage des preuves électroniques présentes dans les éléments du dossier d'une affaire. Les preuves électroniques doivent être stockées par enregistrement sur des CD ou autres supports de données, par exemple des mémoires flash. La procédure est déterminée par le règlement du Cabinet n° 748 « Règlement relatif à l'enregistrement et à la gestion des archives », adopté le 6 novembre 2012. Ce Règlement détermine que, pour les documents électroniques, la lisibilité des dossiers doit être vérifiée. En fonction du type de support des données, la température de stockage peut changer.
Malte	**Obligation d'archivage incombant aux avocats** Aux termes de l'article 101A de la Constitution maltaise, la Commission pour l'administration de la justice établit le code d'éthique et de conduite des avocats. La règle n° 6 au Chapitre III dudit code est ainsi libellé: « A la clôture du dossier, l'avocat est tenu de remettre à son client tous documents et biens qui lui reviennent, sauf ceux entourés d'une protection particulière et/ou faisant l'objet d'un droit de rétention, et doit rendre compte de l'utilisation de tous les fonds de son client qu'il détient. » Le Chapitre VI du code d'éthique traite de la question de la confidentialité. **Obligation d'archivage incombant aux tribunaux** Les dossiers des tribunaux doivent être conservés en vertu de la loi sur les archives nationales (Chapitre 477 des Lois de Malte) car ils sont considérés

	comme étant des archives et dossiers publics.
Monténégro	L'archivage des preuves électroniques sous forme de documents électroniques est régi par l'article 21 de la loi sur le document électronique, qui dispose ce qui suit : Les personnes morales, personnes physiques et organes compétents sont tenus de stocker les documents électroniques à l'origine dans les systèmes d'information ou sur le support qui assure la continuité de l'enregistrement électronique pendant un temps de stockage déterminé, conformément à la loi, notamment pour une affaire portée en justice. Les documents électroniques visés au paragraphe 1 de cet article sont stockés dans des archives électroniques. Ces dernières doivent garantir : 1) que les documents électroniques sont stockés sous la forme dans laquelle ils ont été créés, diffusés, reçus et stockés et que le stockage ne change pas matériellement le contenu des documents; 2) que les documents électroniques sont disponibles sous une forme lisible durant toute la durée du temps de stockage pour les personnes qui ont le droit d'y accéder ; 3) que les données relatives aux signatures électroniques grâce auxquelles les documents électroniques ont été signés, ainsi que les données pour la vérification de ces signatures, sont stockées ; 4) que les signatures électroniques sont stockées sous une forme et par une technologie et des procédures qui, si les signatures électroniques sont incorporées, garantissent raisonnablement leur authenticité et leur intégrité durant l'intégralité du temps de stockage et garantissent que celles-ci ne puissent être changées ou retirées sans autorisation durant la période de temps prévue par la loi et par une affaire portée en justice ; 5) qu'il est possible de déterminer de manière authentique pour tout document électronique l'origine, le créateur, la date, la manière et la forme dans laquelle il a été reçu dans le système pour stockage ; 6) que les procédures de maintenance et de remplacement des supports de stockage des documents électroniques ne portent pas atteinte à l'intégrité et à l'inviolabilité des documents électroniques. La protection des documents électroniques est prévue à l'article 24 : Il convient, conformément à la loi, d'utiliser dans le cycle de documentation du document électronique des procédures technologiques et un équipement technique appropriés garantissant la protection du document électronique. Si un intermédiaire a été utilisé pour des procédures, appareils et systèmes de communication et d'information, celui-ci doit garantir la protection des documents électroniques.
Norvège	Les preuves demeurent archivées à Lovisa après la fin du procès. Seul le personnel du tribunal ayant un mot de passe personnel peut consulter Lovisa. Toutes les versions papier des preuves sont détruites après le procès. **Avocats** Il n'y a pas de dispositions légales générales régissant l'archivage de documents légaux par les avocats. Les procédures en la matière sont couvertes par divers articles de dispositions législatives spécifiques (les plus importantes étant la Loi relative à la vie privée et la Loi relative à la lutte contre le blanchiment d'argent) et normes de conduite professionnelle. La loi du 14 avril 2000 n° 31 relative au traitement des données personnelles (Loi sur les données personnelles) exige

	des avocats qu'ils mettent en place des mesures adéquates de sécurisation des données pour protéger des informations sensibles de leurs clients. La pertinence des mesures de sécurité doit être réévaluée en permanence et l'avocat est tenu de prendre les mesures nécessaires pour remédier aux éventuels dysfonctionnements ou faiblesses. À la fin d'une affaire, les normes professionnelles exigent que l'avocat passe en revue toute documentation amassée et décide ce qui devrait être archivé, détruit ou retourner aux clients. Les archives des clients sont en général conservées pendant 10 ans, ceci pour permettre de justifier la manière dont l'affaire a été traitée, au cas où le client demanderait ultérieurement des dommages et intérêts pour conseils juridiques inadaptés. Après 10 ans, les documents d'origine sont renvoyés à leurs propriétaires et le reste du dossier client détruit. Les normes professionnelles exigent que les avocats archivent des documents originaux. La manière dont les preuves électroniques sont stockées dépendra cependant des capacités d'archivage de l'avocat (physiques ou électroniques). L'archivage par l'avocat de la version des preuves électroniques contenant les métadonnées complètes dépendra également de la source de la preuve. Le client est souvent celui qui apporte la preuve. Il peut l'apporter sous forme électronique, mais souvent, le premier réflexe est de l'imprimer puis de le scanner, ou de le télécharger sur un autre format avant de l'envoyer à l'avocat. Il se peut également que l'avocat découvre indépendamment l'élément de preuve électronique et l'archive directement.
Pologne	Il n'y a pas de règles légales communes applicables à la preuve électronique, et notamment à sa sécurisation et conservation.
Portugal	Les règles sont les mêmes que celles applicables aux preuves documentaires, à savoir le Règlement pour la conservation des archives des tribunaux de droit civil et pénal et des tribunaux administratifs et fiscaux (approuvé par l'Ordonnance 368/2013, du 24 décembre), qui s'applique aux documents produits et reçus dans le cadre des obligations et des compétences des tribunaux de droit civil et pénal et des tribunaux administratifs et fiscaux (en particulier, article 12).
Roumanie	**Avocats** Conformément aux dispositions pertinentes de la Décision n° 64/03 du 12 2011 de l'Union nationale des Associations des barreaux de Roumanie concernant l'adoption des conditions de service régissant les professions juridiques, les avocats sont tenus d'enregistrer tout instrument créé, et de le stocker dans les archives professionnelles, dans l'ordre dans lequel les instruments ont été créés. Dans les trois jours suivant la date de l'établissement des instruments, l'avocat doit enregistrer l'opération dans le registre électronique des instruments établis par les avocats, faute de quoi il ne pourra pas être opposable aux tiers. Les avocats sont tenus de conserver une preuve écrite de toutes opérations réalisées dans le cadre d'un mandat fiduciaire ou en lien avec celui-ci. Lorsque le client exige l'original de ces documents, l'avocat a le droit de conserver des copies papier ou électronique. **Tribunaux** Conformément aux dispositions applicables de la Décision n° 387/22. 09. 2005 portant adoption du Règlement des tribunaux, les présidents et vice-présidents des tribunaux et les greffiers en chef organisent et supervisent l'archivage électronique des dossiers des affaires au niveau du tribunal dont ils relèvent. Les archivistes et greffiers sont responsables de l'archivage électronique des dossiers des affaires, lorsque cela est faisable, et le personnel informatique responsable de la gestion du système d'archivage électronique ; ils établissent les documents requis pour obtenir les signatures électroniques pour les tribunaux et les agents des tribunaux, les certificats prévus par la loi n° 455/ 2001 sur la signature électronique.

Fédération de Russie	Les preuves sous forme électronique sont soumises aux conditions légales générales en matière de garantie de leur sécurité. Conformément à l'article 26.7 du Code de la Fédération de Russie sur les délits administratifs, le juge, l'organe ou un agent en charge des procédures administratives doit prendre les mesures nécessaires pour garantir la sécurité des documents avant la décision d'une affaire sur le fond, ainsi que rendre une décision sur ce qu'il adviendra des preuves à la fin de la procédure. Conformément à l'article 26. 6 partie 3 du Code de la Fédération de Russie sur les délits administratifs, le juge, l'organe ou un agent en charge des procédures administrative doit prendre les mesures nécessaires pour garantir la sécurité des preuves matérielles avant la décision d'une affaire sur le fond, ainsi que rendre une décision sur ce qu'il adviendra des preuves à la fin de la procédure. Les preuves doivent être stockées conformément aux ordonnances du greffe de la Cour suprême de la Fédération de Russie, en date du 15 décembre 2004, n° 161 sur l'autorisation de l'instruction en matière de procédures judiciaires devant les cours suprêmes des républiques, les cours territoriales et régionales, les cours des villes fédérales, les cours des régions autonomes et des territoires autonomes, et en date du 29 avril 2003 n° 36 sur l'autorisation d'instruction en matière de procédures judiciaires devant les cours de district.
Serbie	L'Assemblée nationale a adopté une Loi sur le document électronique, qui couvre l'archivage et le stockage des documents électroniques. Conformément aux dispositions de cette Loi, les personnes morales et physiques de même que les autorités sont tenues de préserver et d'archiver les documents électroniques dans le système d'information ou sur un support suffisamment pérenne pour que les informations soient conservées pendant toute la période prévue, et conformément à la Loi régissant les archives, à la Loi régissant la signature électronique et les réglementations en matière de fonctionnement des services. Des personnes morales et physiques peuvent effectuer le stockage de documents électroniques pour le compte d'une personne morale pour qui cette tâche relève d'une obligation légale. La personne morale chargée de préserver les documents électroniques n'est pas responsable du contenu des documents originaux. **Protection des documents électroniques** Il convient d'utiliser les procédures et équipements technologiques appropriées pour garantir la protection des documents électroniques, conformément à la loi régissant les archives, aux réglementations relatives au fonctionnement des services et aux normes internationales en matière de gestion des documents.
République slovaque	L'Ordonnance n° 543/2005 Col. (Ordre administratif au sein des tribunaux (de district, régionaux et cour martiale)) pose les règles relatives à l'archivage et au stockage des dossiers judiciaires. Les mêmes règles couvrent les pièces versées au dossier par voie électronique (dont les preuves électroniques). De manière générale, le dossier d'une affaire au civil doit être conservé en archives pour une durée de 20 ans après la fin de la procédure. Ensuite, soit il est programmé pour destruction, soit il est transmis aux Archives nationales si cela est jugé pertinent. Pour les pièces versées électroniquement au dossier avec une signature électronique certifiée, les emails sont stockés sur les serveurs du tribunal en même temps que toute la documentation électronique présentée (mémoires, preuves, etc.) depuis la mise en œuvre d'un système d'archivage électronique.
Espagne	Il n'y a pas de règles distinctes régissant le stockage et la préservation des preuves électroniques, de manière générale. Cela dépend de la spécificité de certains secteurs ou de certaines preuves. La règle générale en vertu de l'article 148 LEC 1/2000 est que les greffiers sont responsables du stockage et de la préservation des pièces des affaires archivées par les tribunaux. L'arrêt de la Cour européenne de justice du 8 avril 2014 portant les références C-293/2012 et

	C-594/2012, une demande de décision préjudicielleaffectant la légalité de la Directive 2006/24/CE peut changer la donne. Il n'est pas tout à fait clair si la Loi espagnole d'application 25/2007, du 18 octobre 2007, sur la conservation de données liées aux communications électroniques et aux réseaux publics de communicationsera affectée.
Suède	Les tribunaux – ainsi que d'autres autorités – sont tenus d'archiver les documents publics. Ceux-ci peuvent être triés après un certain temps, ainsi les archives d'une audition en tribunal peuvent être détruites six semaines après que la sentence soit devenue définitive. Il n'y a pas de règles particulières régissant les documents électroniques. La législationest neutre à l'égard des questions de technologie. En vertu du Code de conduite professionnelle pour les membres de l'Association suédoise du Barreau, ces derniers sont tenus d'archiver tous les documents pertinents versés au dossier pour lequel ils sont mandatés, soit sous leur forme originale, soit en copie. Cette obligation ne s'applique cependant pas aux duplicatas, imprimés ou matériel similaire qui peuvent être facilement obtenus ailleurs. La durée d'archivage est de 10 ans ou plus, selon la nature du mandat. Les documents autres que les documents originaux qui appartiennent au client peuvent être archivés sous forme photographique ou électronique.
Suisse	**Avocats** Il existe plusieurs lois prévoyant pour les avocats une obligation de stockage et de conservation des preuves en général, notamment des données et fichiers électroniques. Des réglementations sur la conduite professionnelle comprennent des dispositions sur la durée de conservation des documents, notamment l'article 11 de la Loi cantonale de Berne sur les avocats, qui prévoit que les avocats doivent conserver les documents d'une affaire pendant 10 ans. Selon certaines doctrines, cette règle (de conservation pendant 10 ans) devrait s'appliquer aux avocats d'autres cantons également. Pour ce qui concerne la période de conservation des documents, il n'y a pas de règles particulières concernant les données et fichiers électroniques. **Tribunaux fédéraux** Les tribunaux fédéraux sont soumis à des règles différentes de celles qui s'appliquent aux tribunaux de canton. Le Tribunal fédéral (Cour suprême), le Tribunal pénal fédéral et le Tribunal administratif fédéral ne conservent que les archives des procès directement liés à leurs activités (article 3 de l'Ordonnance du Tribunal fédéral relative à la Loi fédérale sur l'archivage et article 3 par. 1 du Règlement sur l'archivage au Tribunal administratif fédéral – à savoir les mémoires écrits, sentences, correspondances, protocoles etc.). Cette conservation est assurée durablement (article 3 par. 1 de l'Ordonnance sur le Tribunal fédéral et article 3 par.1 du Règlement sur l'archivage au Tribunal administratif fédéral). En revanche, en principe, ces instances ne conservent pas d'autres documents comme les moyens de preuve, etc., qui sont retournés à leur expéditeur (article 3 par. 2 de l'Ordonnance du Tribunal fédéral relative à la Loi fédérale sur l'archivage et article 3 par. 2 du Règlement sur l'archivage au Tribunal administratif fédéral). Conformément aux dispositions de l'article 39 par. 1 de la Loi fédérale sur l'Organisation des autorités de poursuites, le Code suisse de procédure pénale s'applique au Tribunal pénal fédéral ainsi qu'aux tribunaux de cantons. Son article 103 prévoit la conservation des actes d'une affaire pénale. L'article 3 par. 1. du Règlement sur l'archivage au Tribunal pénal fédéral fait obligation à ce dernier de conserver les actes de procédure de façon permanente. Les originaux doivent être rendus aux personnes fondées à les recevoir dès que le procès pénal a donné lieu au prononcé d'une sentence définitive (article 103 par. 2 du Code suisse de procédure pénale).

	Tribunaux cantonaux Les tribunaux cantonaux doivent respecter les lois fédérales pour ce qui est du stockage et de la conservation des données et dossiers. L'article 103 du Code suisse de procédure pénale s'applique donc aussi aux tribunaux (pénaux) cantonaux (voir ci-dessus), mais il n'y a pas d'autres dispositions au niveau fédéral prévoyant une obligation de stockage et de conservation de documents (y compris les preuves électroniques) qui s'appliquerait aux tribunaux cantonaux. En outre, la Loi fédérale sur la protection des données n'est pas applicable aux tribunaux cantonaux (article 2 par. 2 pour les cas où elle ne s'applique pas). Plusieurs lois cantonales prévoient la conservation d'actes de procédures. On citera ainsi le Règlement du Canton d'Argovie créé par l'instance judiciaire suprême, qui régit la période de conservation (différentes périodes sont prévues en fonction de l'affaire en l'espèce ; § 22 du Règlement) ainsi que les normes de sécurité (§ 5). La Loi cantonale sur la protection des données ne s'applique pas aux tribunaux cantonaux (§ 2 par. 2 de la Loi du Canton d'Argovie sur la protection des données). Pour Berne, il y a une disposition prévoyant que les documents électroniques seront traités comme des documents papier (article 7 par. 1 de la Loi sur l'archivage du Canton de Berne). L'article 12 de cette loi dispose que la Cour d'appel (procédures pénales et civiles) et le Tribunal administratif sont chargés de réglementer le stockage et la conservation de données et dossiers. Il existe donc deux Règlements : l'un concernant la conservation des données par les tribunaux pénaux et civils, l'autre concernant la conservation des données par les tribunaux administratifs. Le premier réglemente la période de conservation (il y a des périodes différentes en fonction de l'affaire en l'espèce – articles 11 à 13) ainsi que les normes de sécurité (article 7 par. 1). Le Règlement applicable aux tribunaux administratifs est similaire au Règlement fédéral. Certains actes seulement seront conservés, les autres seront pour l'essentiel retournés à leur expéditeur (article 4). De plus, la Loi du Canton de Berne sur la protection des données s'applique aux tribunaux ainsi qu'à d'autres autorités (article 4 para. 1 de la Loi du Canton de Berne sur la protection des données). La protection et la sécurité des données incombent aux tribunaux (article 8 par. 1 et article 17).
Turquie	Les preuves communiquées durant une procédure judiciaire sont conservées dans les archives des tribunaux conformément à la législation applicable.
Ukraine	La Loi ukrainienne du 7 juillet 2010 n° 2453-VI sur la justice et le statut des juges a complété le Code ukrainien de procédure commerciale en lui ajoutant son article 2 « Système automatisé de flux de documents des tribunaux » qui a introduit la répartition des affaires entre les juges sur une base aléatoire, et qui prévoit l'archivage numérique des affaires, l'enregistrement de la correspondance entrante et sortante du tribunal au moyen d'ordinateurs et la conservation centralisée sous forme électronique des textes liés aux décisions judiciaires.
Royaume-Uni (Angleterre & Pays-de-Galles)	**Avocats** Les preuves doivent être conservées aussi longtemps que le procès est en cours et jusqu'à ce que les possibilités d'appel soient épuisées. **Tribunaux** Les actes de procédures doivent être conservés pour l'année en cours plus une période allant de 7 à 12 ans, en fonction de la juridiction. Cependant, les pièces sont en général retournées avant, ou conservées en fonction de la nature de la preuve et de la possibilité d'une poursuite de l'action judiciaire.

Observations en guise de conclusions

73. Les Termes de référence demandaient :

(i) une analyse des dispositions légales nationales en vigueur qui ont été adoptées ou adaptés concernant l'impact de la preuve électronique sur les règles et modes de preuve, dans le périmètre des procédures en droit civil, droit administratif et droit commercial ;

(ii) l'identification des problèmes que rencontrent les différents systèmes juridiques des Etats membres dans ce domaine, et pour lesquels ils ont besoin de recours ou solutions ou en ont mis en place ;

(iii) l'élaboration de propositions de solutions sur la base des approches et meilleures pratiques déjà adoptées dans les Etats membres et autres en vue de résoudre ou du moins d'atténuer la charge de travail des tribunaux lorsqu'ils ont affaire à des preuves électroniques dans des procédures civiles et administratives.

74. Il ressort des réponses reçues que, dans le contexte du droit civil, du droit administratif et du droit commercial, un certain nombre de dispositions légales nationales en vigueur ont été largement adaptées pour refléter la réalité de la preuve électronique sur les règles et modes de preuve.

Partie A

75. Dans la Partie A, les types de preuves qui pourraient devoir être obtenues dans des procédures judiciaires ont été examinés, et des questions ont été posées sur la manière dont les preuves électroniques pourraient être recueillies ou saisies, en tenant compte de la nécessité de garantir l'authenticité, quels étaient les droits éventuels des parties à obtenir des preuves avant qu'une procédure ne soit entamée, et s'il existe des règles spéciales concernant la présentation de la preuve, en particulier concernant les signatures électroniques.

76. La question 1 avait pour but d'établir si, lorsqu'il est présenté des preuves provenant de site web sur Internet librement accessibles, il est nécessaire de recueillir la preuve selon des modalités spécifiques pour en garantir l'authenticité, par exemple par le recours à un huissier ou à un spécialiste de la preuve numérique mandaté par le tribunal. Bien que cinq Etats membres (Andorre, Croatie, France, Lituanie et Turquie) aient répondu « oui » à la question, les réponses plus détaillées les concernant ont montré que le recueil des données selon une manière spécifique n'était nécessaire que dans certaines circonstances, essentiellement lorsque l'authenticité risquait d'être remise en question. Les autres Etats membres ayant répondu au questionnaire ont révélé qu'il n'y avait pas de conditions pour que la preuve électronique soit recueillie selon une manière spécifique. Il est conclu que la méthode de collecte de la preuve sur Internet est en général libre de toutes obligations techniques spécifiques, et que le juge des faits apprécie l'authenticité et donc la valeur probante de la preuve en fonction de la totalité des preuves.

77. La question 2 avait pour but d'établir s'il est possible d'obtenir des preuves électroniques avant qu'une action judiciaire ait été entamée sur le fond. À l'exception de trois Etats membres (Andorre, Arménie et Serbie), il est en général possible qu'une partie obtienne copie de données électroniques dans ces circonstances, même si des règles différentes pourraient trouver à s'appliquer en fonction (i) de la possibilité ou non qu'une partie soit partie à l'action ; (ii) lorsque la partie n'a pas de possibilité d'être partie à l'action, et (iii) lorsqu'une personne est compromise dans des actes condamnables. Dans la plupart

des cas, les règles pertinentes de la procédure civile s'appliqueront. Les types de preuves importent peu lorsqu'une partie a de bonnes raisons d'obtenir les preuves avant qu'une action judiciaire n'ait été entamée sur le fond. Ceci vaut particulièrement pour ce qui est des preuves électroniques, étant donné que les preuves pertinentes ont plus de chances d'être trouvées sous forme électronique que sous toute autre forme.

78. Étant donné qu'une partie peut avoir à demander des preuves électroniques avant qu'une action judiciaire n'ait été entamée sur le fond, il a été jugé nécessaire de poser la question 3, à savoir lorsqu'une partie n'est pas résidente dans la juridiction, peut-elle demander la même ordonnance judiciaire que celle objet de la question 2 ? Ceci est important car les preuves sous format électronique peuvent être hébergées sur des serveurs qui se trouvent n'importent où dans le monde. À l'exception d'Andorre et de la Serbie, il est possible pour une partie d'autres Etats membres qui n'est pas résidente dans la juridiction de saisir le tribunal pour obtenir la même ordonnance que celles mentionnées dans la question 2 explicitée ci-dessus.

79. La question 4 est une variante de la question 1 ; elle se réfère là encore, pour l'essentiel, au fait de savoir si, en cas de saisie de preuves électroniques à la suite d'une ordonnance de justice, la partie recherchant les preuves est obligée de suivre un ensemble spécifique de dispositions légales ou de lignes directrices. Ce type de lignes directrices existe pour les procédures pénales, et lorsqu'il en existe, les lignes directrices pour les procédures pénales ne s'appliquent pas spécifiquement aux procédures civiles. Toutefois, la pratique dans certaines juridictions consiste pour les avocats dans des procédures civiles à suggérer à leurs clients d'obtenir les preuves électroniques en suivant les lignes directrices pour les procédures pénales, ce qui permet plus facilement d'établir que des procédures correctes ont été utilisées pour saisir et stocker les preuves de telle manière que cela n'affecte pas leur intégrité et l'authenticité des données.

80. La réponse quasi unanime a été qu'il n'y avait pas de lignes directrices applicables à la saisie de preuves électroniques dans les procédures civiles. Il convient donc de conclure que cette absence reflète la différence dans la norme de preuves entre les procédures pénales et civiles.Toutefois, du fait de l'augmentation de la destruction et de la falsification délibérées des preuves électroniques, il semble judicieux d'indiquer aux avocats, lorsqu'ils sont dans le cadre d'une procédure civile, de songer à suivre un ensemble de lignes directrices lorsque la preuve électronique est complexe, par exemple dans des affaires bancaires.

81. Le rapport inclut les procédures administratives, et la question 5 cherchait à faire émerger l'existence ou non de règles spéciales concernant la présentation de la preuve dans les procédures administratives, en particulier pour ce qui est des signatures électroniques. Sur les réponses à cette question, 15 Etats membres ont indiqué qu'il n'y avait pas d'exigences spécifiques. Un certain nombre d'Etats membres (Croatie, Estonie, Grèce, Lettonie et Serbie) exigent une signature électronique avancée telle que définie dans le cadre de la Directive de l'Union européenne et, en Allemagne, les documents électroniques doivent être signés avec une signature électronique qualifiée lorsque la loi exige une forme écrite. Étant donné que les procédures administratives sont largement internes d'une juridiction et n'affectent pas un grand nombre de parties étrangères, il n'est pas considéré que cette conclusion spécifique mérite davantage de commentaires.

Partie B

82. Dans la partie B, l'attention était portée sur l'obtention de l'aide d'un tribunal pour établir l'identité d'une personne, lorsque une partie prétend, par exemple, qu'un message électronique lui a porté préjudice (diffamation, secrets commerciaux etc.) mais que l'identité de l'expéditeur ne peut pas être établie avec certitude.

83. La question 6 avait pour but de savoir s'il est possible qu'une partie s'adresse à un tribunal pour identifier l'utilisateur d'un service électronique fourni par une société dans la juridiction, par exemple l'utilisateur d'un compte de messagerie électronique, d'un service d'accès à Internet, ou d'un compte VoIP, afin de voir jusqu'à quel point il est facile ou difficile pour une partie d'obtenir des informations importantes qui ne sont pas nécessairement accessibles facilement. Parmi tous les Etats membres qui ont répondu, à l'exception de la Croatie, de la Finlande, de la Géorgie, de la Serbie, de la République slovaque et de de l'Ukraine, tous ont indiqué qu'une partie peut s'adresser à un tribunal pour identifier l'utilisateur un service électronique fourni par une société dans la juridiction concernée.

84. La question 7 est une extension de la question 6 qui a été posée poursavoir si une partie qui n'est pas résidente dans le pays concerné pourrait s'adresser au tribunal pour obtenir la même ordonnance. À l'exception de la Belgique, de la Croatie, de la Finlande, de la Géorgie, de la Fédération de Russie, de la Serbie, de la République slovaque et de l'Ukraine, tous les répondants ont indiqué qu'une partie qui ne réside pas dans la juridiction peut s'adresser à un tribunal pour identifier l'utilisateur d'un service électronique fourni par une société dans la juridiction, et qu'il est possible d'intenter une action en justice sur le fond.

85. La question de la défaillance de certains Etats membres de permettre à leurs propres citoyens ou aux ressortissants d'autres pays d'obtenir des informations pertinentes concernant une partie potentielle à des procédures civiles est quelque peu préoccupante. Vu la facilité avec laquelle l'auteur d'un délit peut se dissimuler derrière l'anonymat, ou utiliser des services dans une juridiction qui ne permet pas à une partie potentiellement lésée d'intenter une action en justice, on peut estimer qu'il est somme toute injuste d'empêcher une partie lésée d'obtenir des informations pertinentes en vue de décider si elle va intenter ou non une action en justice.

Partie C

86. Dans la partie C, couvrant des questions de droit matériel liées à la preuve électronique, l'objectif était d'établir comment un État membre a classé la preuve électronique (si une telle classification a été faite), et s'il y a présomption de fiabilité.

87. La question 8 permettait aux Etats membres d'indiquer comment la preuve électronique avait été catégorisée, le cas échéant. Pour les explications détaillées concernant chaque juridiction, le lecteur est renvoyé à la réponse individuelle de l'État membre et aux informations fournies dans le tableau récapitulatif des réponses à cette question, mais de manière générale, la preuve est présumée fiable à moins que la partie adverse ne la conteste. Si l'on va un peu plus loin, la question 9 cherchait à établir s'il y a une présomption concernant la « fiabilité » des preuves électroniques, si celles-ci sont présumées être « correctes », « précises », « convenablement représentées ou calibrées » ou « fonctionnent convenablement ». La seule juridiction pour laquelle il existe une présomption explicite concernant la fiabilité des ordinateurs est celle de l'Angleterre et du

Pays-de-Galles, ce qui a fait l'objet de critiques[20]. Dans les procédures civiles en Angleterre et au Pays-de-Galles, il y a présomption d'authenticité de toutes les formes de preuves ; il revient à la partie adverse de soulever la question de l'authenticité dans le cadre des règles de la procédure civile (*Civil Procedure Rules* - CPR 32.19)). L'Estonie a adopté une position similaire, où toute preuve est présumée fiable à moins que la partie adverse ne le conteste, auquel cas la preuve doit être authentifiée. Au Monténégro, la position n'est pas certaine. En Fédération de Russie, cette présomption existe lorsque les données électroniques ont été obtenues de la manière prescrite par la loi. En Espagne, une présomption s'appliquera, selon que les données en format numérique sont « signées » par une signature électronique avancée. Pour les autres juridictions qui ont répondu au questionnaire, une telle présomption n'existe pas.

88. D'un point de vue pratique, compte tenu du niveau de preuves moins élevé dans les procédures civiles, une présomption de l'authenticité de toute forme de preuve est utile puisqu'elle permet aux parties de se dispenser de prouver chaque pièce à conviction – en particulier lorsque les deux parties pourraient ne pas contester les preuves. Lorsqu'une partie conteste néanmoins ces dernières, alors il incombera à la partie qui les a présentées d'en démontrer l'authenticité. De plus, lorsque certaines procédures sont utilisées telles que les signatures électroniques avancées, ou lorsque des services indépendants extérieurs officiellement reconnus tels que des huissiers obtiennent des preuves indépendamment des parties, il n'est pas nécessaire de tester des règles strictes relatives à l'authenticité de la preuve, à moins bien entendu que l'une des parties ne le conteste. Toutefois, la présomption en Angleterre et au Pays-de-Galles que les ordinateurs sont fiables est dangereuse, outre que c'est une présomption qui n'est étayée par rien.

Partie D

89. Dans la partie D, concernant l'admissibilité de la preuve électronique, le but était établir s'il était nécessaire d'utiliser une procédure spécifique pour obtenir la preuve électronique (comme dans les procédures pénales) et, si tel n'était pas le cas, si le tribunal analyserait comment les preuves ont été obtenues pour décider de leur admissibilité ou non. Tel était l'objet de la question 10. Les réponses indiquent qu'aucun État membre n'a prévu de disposition légale visant à ce que la preuve électronique soit obtenue selon une procédure spécifique, même si des règles de procédure civile pourraient trouver à s'appliquer pour ce qui concerne l'obtention et l'admission des preuves. La question 11 couvrait le fait de savoir si, au cas où la preuve électronique n'avait pas obtenue conformément à une norme ou à des procédures spéciales, le tribunal en tiendrait compte pour décider de l'admissibilité de cette dernière. De manière générale, la réponse a été qu'un tribunal évaluerait la preuve qui lui est présentée dans le cours normal des procédures judiciaires, en tenant compte de l'intégralité des preuves techniques à sa disposition. Dans certaines juridictions, le juge décidera quel élément de preuve est accepté et quel élément de preuve il fera tester pour ce qui est de l'authenticité.

90. La question 12 est une variante de ce thème, qui interroge sur la publication de lignes directrices techniques ou de bonnes pratiques décrivant comment on peut obtenir des preuves électroniques tout en préservant leur intégrité. Aucune ligne directrice n'a été produite par les Etats membres hormis la Pologne - et ces lignes directrices pourraient ne pas couvrir les procédures civiles - et l'Angleterre et le Pays-de-Galles pour ce qui concerne les affaires pénales et non les affaires civiles). En Allemagne, il y a une présomption limitée concernant l'intégrité lorsqu'un individu s'est enregistré de manière sécurisée pour un compte « De-Mail» et au Monténégro, la loi sur la signature électronique prévoit la création

[20] Pour une critique détaillée, voir Stephen Mason, éd. gén., *Digital Evidence* (3e éd., LexisNexis Butterworths, 2012), chapitre 5.

d'un ensemble de règles liées aux signatures électroniques avancées qui, si elles sont suivies, assurent une présomption de fiabilité.

91. Lors de la formulation de la question 13, il s'agissait de savoir si les règles sur l'admissibilité de la preuve électronique variaient en fonction de la complexité ou de la simplicité de la preuve. La quasi-totalité des réponses a été que les règles sur la recevabilité des preuves électroniques tendent à ne pas varier. Le volume des preuves pour démontrer l'authenticité de données numériques peut changer, en fonction de la complexité de la preuve.

Partie E

92. Dans la partie E, l'intention était d'établir quelles règles étaient éventuellement en place concernant l'obligation et les exigences relatives au stockage et à la conservation des preuves électroniques pour les avocats et les tribunaux, et quelles étaient les conditions éventuelles de garanties de la sécurité de la preuve après un procès.

93. La situation concernant l'archivage et la sécurité des données électroniques par les avocats et les tribunaux semble plutôt confuse. Lorsqu'un État membre est également membre de l'Union européenne, la directive applicable est la Directive sur la protection des données[21] – en particulier, les dispositions de son article 17 sur « la sécurité du traitement ». Les lignes directrices du Conseil des barreaux européens (CCBE) et les lignes directrices professionnelles au niveau national (lorsqu'elles existent) sont également susceptibles de couvrir ce point. Un certain nombre de réponses des Etats membres indiquent que les obligations des tribunaux et des avocats en matière de sécurité des données de leurs clients ne sont pas bien comprises. Dans l'Union européenne, la situation au regard de la législation est claire. Signe de l'importance que revêt cette question, le Crown Prosecution Service (services du ministère public) pour l'Angleterre et le Pays-de-Galles s'est vu notifier, le 2 novembre 2015, une sanction pécuniaire de 200 000 livres par l'Office of the Information Commissioner (Commissariat à l'information) après que des ordinateurs portables qui contenaient les enregistrements vidéo d'auditions réalisées par la police eurent été dérobés dans un studio cinématographique privé. Ces auditions de 43 victimes et témoins concernaient 31 enquêtes, presque toutes en cours, relatives à des actes de violence ou à des faits à caractère sexuel.[22]

94. Les Etats membres doivent analyser cet aspect de la preuve électronique de manière approfondie, et à partir d'un certain nombre de perspectives, notamment la préservation sécurisée, l'effacement réel (autrement dit expurger des données), et les exceptions en matière d'affaires historiques. Les avocats ont une obligation professionnelle à l'égard de leurs clients, et le fait que leur correspondance se fasse à la fois sur papier et par voie électronique ne les exonère pas de leur obligation d'assurer la bonne sécurité des documents électroniques.

[21] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, OJ L 281, 23.11.1995, pp. 31-50.

[22] https://ico.org.uk/media/action-weve-taken/mpns/1560074/crown-prosecution-service-monetary-penalty-notice.pdf.

Recommandations existantes du Comité des Ministres

95. Il a également été demandé au CDCJ de passer en revue les recommandations ci-après du Comité des Ministres afin de voir si elles devraient faire l'objet d'une révision et, dans l'affirmative, de formuler des propositions en ce sens :

> Recommandation n° R (86) 12 relative à certaines mesures visant à prévenir et à réduire la surcharge de travail dans les tribunaux;
>
> Recommandation n° R (95) 11 relative à la sélection, au traitement, à la présentation et à l'archivage des décisions de justice dans les systèmes de documentation juridique automatisés ;
>
> Recommandation Rec(2001)2 concernant la conception et la reconception rentables des systèmes judiciaires et des systèmes d'information juridique ;
>
> Recommandation Rec(2001)3 sur les services des tribunaux et d'autres institutions juridiques fournis aux citoyens par de nouvelles technologies ;
>
> Recommandation(2003)14 sur l'interopérabilité des systèmes d'information de la justice ;
>
> Recommandation(2003)15 relative à l'archivage de documents électroniques dans le secteur juridique.

96. Il n'apparaît pas nécessaire de refondre la Recommandation n° R (86) 12, en ce qu'elle traite de la charge de travail des tribunaux.

97. Il pourrait s'avérer utile de rappeler aux tribunaux les dispositions de la Recommandation n° R (95) 11, puisque les décisions de justice sont aujourd'hui de plus en plus souvent publiées en ligne, ainsi que celles de la Recommandation Rec(2003)15.

98. Il conviendrait de réviser les Recommandations Rec(2001)2, Rec(2001)3 et Rec(2003)14, en tenant compte de la diversité des tâches qui sont réalisées – surtout au sein de l'Union européenne –, telle qu'elles ressortent en partie des dispositions desdites recommandations.

Annexe A

Mandat

pour une étude comparative sur l'impact d'internet et des nouvelles technologies

sur les règles et les modes de preuve

Les consultants devront :

1. Réaliser une étude comparative et une analyse des lois nationales existantes qui ont été adoptées ou adaptées à l'impact de la preuve électronique (qui, par nature, inclut l'Internet et les nouvelles technologies) sur les règles de preuve et les modes de preuve, axée sur les procédures en matière civile, administrative et commerciale.

2. Identifier les problèmes auxquels les différents systèmes juridiques des Etats membres sont confrontés à cet égard et pour lesquels ils aimeraient bien trouver une solution ou ont trouvé des solutions.

3. Enoncer des propositions de solution sur la base d'approches et de meilleures pratiques déjà adoptées dans certains Etats membres et non membres, dans le but de réduire ou du moins d'alléger l'engorgement des tribunaux civils et administratifs confrontés à des preuves électroniques.

L'étude devrait aborder, mais pas uniquement, les questions de la recevabilité des preuves électroniques, du poids des preuves électroniques, du rôle du juge, de la recherche des preuves avant le procès, et du rôle des experts judiciaires ou des experts indépendants.

L'étude comparative prendra en considération les informations fournies par les membres du Comité européen de coopération juridique (CDCJ) sur la base d'un questionnaire qui sera préparé par les consultants.

A la lumière de l'analyse susmentionnée, les consultants devront également examiner dans quelle mesure il est nécessaire de réviser les recommandations[23] du Comité des Ministres pertinentes pour l'utilisation par les tribunaux des technologies de l'information et de la communication.

[23] Recommandation n° R (86) 12 relative à certaines mesures visant à prévenir et à réduire la surcharge de travail dans les tribunaux;

Recommandation n° R (95) 11 relative à la sélection, au traitement, à la présentation et à l'archivage des décisions de justice dans les systèmes de documentation juridique automatisés ;

Recommandation Rec(2001)2 concernant la conception et la reconception rentables des systèmes judiciaires et des systèmes d'information juridique ;

Recommandation Rec(2001)3 sur les services des tribunaux et d'autres institutions juridiques fournis aux citoyens par de nouvelles technologies ;

Recommandation Rec(2003)14 sur l'interopérabilité des systèmes d'information de la justice ;

Recommandation Rec(2003)15 relative à l'archivage de documents électroniques dans le secteur juridique.

Annexe B

Questionnaire

sur l'utilisation des preuves électroniques

dans les procédures civiles et administratives

et son impact sur les règles et modes de preuve

A. Obtention de la preuve électronique

Préambule

Il existe trois types d'éléments de preuve qui pourraient être obtenus lors d'une procédure judiciaire:

(i) Les preuves en provenance de sites internet accessibles au public, tels que (cette liste n'est qu'indicative) les blogues et les images publiées sur les réseaux sociaux.

(ii) Les preuves substantielles (ou probante), comme l'e-mail ou des documents en format numérique qui ne sont pas rendus publics et détenus sur un serveur.

(iii) L'identité présumée d'un utilisateur et des données de trafic («métadonnées») qui sont utilisées pour aider à identifier une personne en découvrant la source de la communication, mais pas le contenu.

Par exemple, un problème de compétence se pose si une entreprise française estime qu'un employé a volé des secrets d'affaires et qu'il a conservé les données sur un serveur privé dématérialisé britannique.

Questions

1. Si une partie souhaite produire des preuves à partir de sites Internet accessibles au public, un tribunal peut-il exiger la production de copies des sites sous un format spécifique afin de garantir l'authenticité notamment par la désignation d'un huissier ou d'un expert auprès du tribunal spécialisé en preuves numériques?

   Oui ☐
   Non ☐

   Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

2. Est-il possible pour une partie de demander à un tribunal l'obtention d'une copie numérique des données collectées (tels que les fichiers informatiques conservés sur un ordinateur d'un tiers localisé dans le ressort de la juridiction) avant qu'une action en justice soit initiée sur le fond?

   Oui ☐
   Non ☐

   Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

3. Est-il possible pour une partie qui ne réside pas dans votre pays d'avoir accès au même recours auprès d'un tribunal comme mentionné dans le point 2 ci-dessus, et est-il également possible, même si c'est peu probable que l'action en justice sur le fond soit plaidée devant une juridiction nationale ?

   Oui ☐
   Non ☐

   Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

4. Lorsqu'en vertu d'une ordonnance d'un tribunal, une saisie de preuves électroniques est réalisée, faut-il que la partie qui demande la preuve suive un ensemble particulier de dispositions juridiques ou de lignes directrices pour la saisie de ces preuves électroniques?

   Oui ☐
   Non ☐

   Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

5. En ce qui concerne la procédure administrative, veuillez indiquer s'il existe des règles spécifiques concernant la production d'éléments de preuve, notamment en matière de signatures électroniques, et si un format particulier de signature électronique est requis lors de la production de preuves par voie électronique.

B. Obtention de l'identité présumée d'un utilisateur

Préambule

Le problème se pose quand une partie prétend qu'un courriel a causé un dommage (diffamation, secrets commerciaux, etc.), mais que l'identité de l'expéditeur ne peut être établie. La partie qui a subi ce mauvais usage souhaiterait utiliser les informations d'identification détenues par le fournisseur d'accès (métadonnées) pour prouver le lien entre un compte de message électronique et une personne physique, qui est l'utilisateur du courriel.

Questions

6. Est-il possible pour une partie de faire une requête auprès d'un tribunal pour identifier l'utilisateur d'un service électronique fourni par une entreprise dans votre juridiction, comme l'utilisateur d'un compte de messagerie électronique, service d'accès à Internet, ou un compte VoIP[24]?

   Oui ☐
   Non ☐

   Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

[24] VOIP (voice-over internet protocol) : Il s'agit d'une technologie permettant de communiquer via la voix au travers d'internet ou n'importe quel réseau basé sur le protocole TCP/IP.

7. Est-il possible pour une partie qui ne réside pas dans votre pays d'avoir recours à la même ordonnance d'un tribunal, et est-il également possible même si c'est peu probable que l'action en justice sur le fond soit plaidée devant une juridiction nationale?

   Oui ☐
   Non ☐

   Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

C. Les questions de fond relatives à la nature de la preuve électronique

Préambule

Dans une certaine mesure, la preuve électronique est encore un concept relativement nouveau. Notre objectif, dans cette section, est de soulever des questions qui permettent d'évaluer comment les différentes juridictions appréhendent les preuves électroniques dans les procédures judiciaires. L'article 9 de la directive européenne 2000/31 sur le commerce électronique impose aux États membres d'intégrer dans leurs systèmes juridiques les contrats électroniques de sorte que cela ne crée pas d'obstacles pour leur validité; voir aussi l'article 4-2 de la directive européenne 1999/93 sur les signatures électroniques.

Questions

8. Veuillez définir les classifications des preuves, le cas échéant, comment la preuve électronique s'inscrit dans cette classification. Par exemple, existe-t-il certains types de preuves électroniques qui sont présumés authentiques et fiables et existe-t-il d'autres formes de preuve dites imparfaites?

9. Existe-t-il dans votre juridiction une présomption en vertu de laquelle les preuves électroniques sont considérées comme « fiables », « recevables », « précises », « convenablement définies ou calibrées » ou « fonctionnant convenablement » ?

   Oui ☐
   Non ☐

   Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

D. L'admissibilité et l'authenticité de la preuve électronique

Préambule

De nombreuses juridictions ont introduits l'admissibilité de la preuve électronique dans leurs procédures juridiques. Cette question a également été abordée à l'échelle régionale, tels que les dispositions de l'article 5 (2) de la Directive de l'Union européenne 1999/93 / CE du Parlement européen et du Conseil du 13 Décembre 1999 sur un cadre communautaire pour les signatures électroniques[25], qui définit que «l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que la signature se présente sous forme électronique». De même, la disposition de l'article 9 (1) de

[25] JO L 13 du 19.1.2000, p.12. La directive est abrogée par le 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 et abrogeant la directive 1999/93/CE, JO L 257, 28.8.2014, pp. 73-114.

la Directive européenne 2000/31 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 »)[26], prévoit que les contrats ne seront pas privés de leur efficacité et de leur validité juridique parce qu'ils ont été conclu par voie électronique. Il est généralement admis que les preuves sous forme électronique sont recevables dans les procédures judiciaires. La règlementation inclurait:

(i) si la preuve doit être obtenue conformément à toute orientation technique, (par exemple, des lignes directrices applicable en procédure pénale, et elles pourraient s'avérer utiles pour les procédures civiles et administratives)[27], et

(ii) la manière dont l'authenticité et la fiabilité de la preuve électronique est déterminée- à savoir, s'il existe des lignes directrices admises pouvant aider un juge à déterminer l'authenticité de la preuve électronique, et s'il y a une présomption quant à la «fiabilité» de la preuve électronique.

Questions

10. Si une partie souhaite soumettre des éléments de preuve électronique dans les procédures civiles ou administratives, est-il nécessaire de recourir à une procédure spécifique, tel que requis par la loi ou autres textes règlementaires?

    Oui ☐
    Non ☐

    Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

11. Si la preuve électronique n'est pas obtenue, conformément à une procédure standard ou spéciale, le tribunal prendra t'il en considération cet élément lorsqu'il jugera de l'opportunité d'admettre la preuve en question?

    Oui ☐
    Non ☐

    Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

[26] JO L 178, 17.7.2000, pp. 0001 – 0016

[27] For example: *Guidelines for Best Practice in the Forensic Examination of Digital Technology*, Version 6 (20 April 2009), European Network of Forensic Science Institutes, Forensic Information Technology Working Group, available at http://www.enfsi.eu/sites/default/files/documents/forensic_it_best_practice_guide_v6_0.pdf; UK Association of Chief Police Officers 'Good Practice Guide for Digital Evidence', Version 5 (October 2011), available at http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf.

12. Si ce n'est pas déjà mentionné ailleurs dans vos réponses, existe-t-il des lignes directrices techniques ou des bonnes pratiques publiées dans votre pays et qui décrivent comment la preuve électronique peut être obtenue tout en conservant son intégrité?

    Oui ☐
    Non ☐

    Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

13. Est-ce que les règles sur la recevabilité de la preuve électronique varient selon la complexité ou la simplicité de la preuve?

    Oui ☐
    Non ☐

    Si la réponse est « oui », pourriez-vous fournir de plus amples informations, en tenant compte des principes juridiques pertinents.

E. L'archivage de la preuve après le procès

Préambule

La preuve électronique doit être traitée différemment des fichiers papier et des pièces à conviction. En imprimant des documents électroniques, les métadonnées pertinentes qui tendent à prouver l'authenticité du document seront perdues. Cela signifie qu'il est nécessaire de conserver les données électroniques sous leur forme originale de la même manière que la conservation d'un dossier physique. Dans une certaine mesure, il est nécessaire pour les avocats et les administrateurs judiciaires d'assurer la confidentialité et la sécurité de ces données électroniques, y compris la conservation des copies de sauvegarde sécurisées dans le cas où il surviendrait un incident sur un autre moyen de stockage.

Le Conseil des barreaux européens (CCBE) a produit un ensemble de directives traitant spécifiquement du «cloud computing», qui est tend à rejoindre cette étude, cependant il n'y a pas d'autres directives produite par le CCBE qui couvre directement ce sujet.[28]

Question

14. Quelles sont les normes ou conduites professionnelles, le cas échéant, relatives à l'obligation et aux exigences à respecter pour le stockage et la préservation de preuves électroniques ?

    En répondant à cette question, veuillez couvrir les domaines suivants:

    - Archivage par les avocats ;
    - Archivage par les greffes du tribunal ;
    - Exigences à mettre en place pour la sécurité des preuves après le procès.

[28] *CCBE guidelines on the use of cloud computing services by lawyers*, available at http://www.ccbe.eu/.