aec²

THE ADMISSIBILITY OF
ELECTRONIC EVIDENCE IN COURT
CYBEX INITIATIVE

LA ADMISIBILIDAD DE LAS PRUEBAS ELECTRÓNICAS ANTE LOS TRIBUNALES:
LUCHANDO CONTRA LOS DELITOS TECNOLÓGICOS

THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COURT:
FIGHTING AGAINST HIGH-TECH CRIME

L'ADMISSIBILITÉ DE LA PREUVE ÉLECTRONIQUE DEVANT LES TRIBUNAUX :
LUTTE CONTRE LES DÉLITS TECHNOLOGIQUES

AGIS 2005
With financial support from the AGIS Programme
European Commission -Directorate- General Justice,
Freedom and Security

cybex
Intelligence on e-evidence

INVESTIGADOR PRINCIPAL / MAIN INVESTIGATOR
INVESTIGATEUR PRINCIPAL

FREDESVINDA INSA
CYBEX

COORDINACIÓN / COORDINATION

CARMEN LÁZARO
CYBEX

EQUIPO INVESTIGADOR / RESEARCH TEAM
ÉQUIPE D'INVESTIGATION

BURKHARD SCHAFER
UNIVERSITY OF EDINBURGH
CYBEX
DAN MINZALA
NATIONAL INSTITUT OF CRIMINOLOGY OF ROMANIA
DIEGO TORRENTE
UNIVERSIDAD DE BARCELONA
FERNANDO FERNÁNDEZ
POLICÍA NACIONAL DE ESPAÑA
FRANCISCO MÁLAGA
UNIVERSIDAD POMPEU FABRA
FREDESVINDA MÉRIDA
UNIVERSIDAD DE BARCELONA
JOHN KINGSTON
UNIVERSITY OF EDINBURGH
PATRICK BURKE
QINETIQ
SHARA MONTELEONE
ASSOCIAZIONE NAUTILUS

COLABORACIÓN / COLLABORATION

FLORENCIA RODRÍGUEZ -CYBEX-
NURIA GARCÍA -CYBEX-

PRIMERA EDICIÓN, 2006
FIRST EDITION, 2006
PREMIÈRE ÉDITION, 2006

L'ADMISSIBILITÉ DE LA PREUVE ÉLECTRONIQUE DEVANT LES TRIBUNAUX:
LUTTE CONTRE LES DÉLITS TECHNOLOGIQUES

THE ADMISSI
ELECTRONIC
CYBEX INITIATIV

INTRODUCTION

Les nouvelles technologies et l'évolution des systèmes de communication ont transformé substantiellement les processus d'échange d'information et de production, dans toutes les sphères de la vie: le monde de l'entreprise, la vie civile et militaire, augmentant ainsi de manière exponentielle la création de documents électroniques au sein des organisations. Plus de trois trillions de courriers électroniques sont envoyés chaque année dans le monde et plus de 90% des documents créés au sein des organisations sont électroniques, parmi lesquels seuls 30% sont imprimés.

L'utilisation massive des environnements numériques et de l'environnement virtuel n'est pas exempte de conflits, ni d'usages frauduleux ou criminels. Les typologies traditionnelles de fraudes et de délits se sont modifiées suite à l'utilisation de nouveaux canaux de communication et à l'incorporation de nouvelles catégories délictuelles. Les délinquants et les bandes organisées ont trouvé dans les nouveaux moyens technologiques un allié solide pour commettre de nouveaux crimes, tels que la pornographie infantile sur Internet, le *phishing*, le *pharming,* l'abus des moyens corporatifs et la concurrence déloyale, entre autres.

Face à ces nouveaux types de délits et aux nouvelles voies pour les commettre, un nouvel outil, qui permet de prouver que ces fraudes ont été commises, fait son apparition: la *preuve électronique*. Il s'agit d'un instrument qui peu à peu, commence à faire partie de notre vie quotidienne et qui acquiert également une plus grande importance au sein des processus judiciaires. On peut affirmer que les preuves traditionnelles sont en train de migrer du support papier vers un environnement virtuel, et leurs processus de gestion ainsi que les critères d'admissibilité changent par rapport à la preuve traditionnelle.

Nous assumons que la *preuve électronique* est le moyen approprié pour prouver la commission des délits commis par l'intermédiaire des nouvelles technologies et nous la définissons de la manière suivante: *toute information obtenue à partir d'un dispositif électronique ou d'un environnement numérique et qui sert à acquérir la conviction de la certitude d'un fait.*

Du fait de l'importance de ce nouvel outil procédural, nous considérons qu'il était fondamental d'approfondir les connaissances de l'admissibilité des *preuves électroniques* devant les tribunaux, en tant que moyen pour lutter contre les délits technologiques. Pour ce faire, le projet avait pour objectif de répondre aux questions fondamentales suivantes: qu'est-ce que la *preuve électronique*?, la *preuve électronique* fait-elle l'objet d'une réglementation en Europe ? , quels sont les problèmes auxquels sont confrontés les agents sociaux européens impliqués dans l'obtention, l'analyse et la présentation de *preuves électroniques* et comment agissent-ils en réalité ? Les réponses à ces questions permettront de connaître la réalité législative et pratique à ce sujet. Grâce à ces objectifs, la Direction Générale Justice, Liberté et Sécurité de la Commission européenne, dans le cadre du Programme cadre AGIS, a approuvé notre projet, du fait de la valeur ajoutée qu'il représente. C'est également la première fois que l'on étudie, au niveau européen, un instrument juridique qui touche de plus en plus les citoyens européens. De plus, avec cette étude on développe et renforce le *networking* entre les états membres de l'UE et les pays candidats. Elle permet d'échanger des informations et des expériences au niveau européen et favorise en même temps la coopération entre les autorités judiciaires, les avocats, les polices et les experts privés. C'est une façon de contribuer au développement et à la consolidation de l'Espace Judiciaire Européen, en luttant ensemble contre les délits technologiques.

Un projet ambitieux et nouveau qui a été réalisé dans seize pays, les quinze pays de l'Union européenne[31] et la Roumanie, en tant qu'état candidat à l'Union européenne. Une équipe de chercheurs européens multidisciplinaires (policiers, juristes, sociologues, techniciens, entrepreneurs, académiciens, avocats et experts en informatique légale), qui a assumé ce projet comme un défi professionnel et qui s'est engagée à le réaliser en un an.

Pour réaliser l'analyse légale de la *preuve électronique* et son admissibilité devant les tribunaux et afin de connaître le degré de développement et d'homogénéité législative existant européen, nous avons passé en revue les législations en vigueur. Le champ d'observation est composé de normes qui, d'une manière ou d'une autre, traitent de ces quatre éléments ou ont des conséquences sur ces éléments: "preuve", "*preuve électronique*", "admissibilité de la preuve" et "admissibilité de la *preuve électronique*". D'après ce critère, nous comptabilisons soixante dix-huit normes analysées.

Pour connaître les problèmes auxquels sont confrontés les agents sociaux qui interviennent lors d'une analyse légale des moyens électroniques et pour savoir comment ils agissent, nous avons réalisé cent vingt-cinq entretiens en profondeur auprès des catégories professionnelles suivantes: avocats, juges civils, pénaux, commerciaux et du travail, procureurs, notaires, représentants du Conseil Général du Pouvoir Judiciaire, policiers, experts en informatique légale et entrepreneurs, et nous avons recueilli systématiquement les informations qu'ils nous ont transmises. Finalement, avec toutes les informations légales et pratiques obtenues, nous avons réalisé un guide d'amélioration.

[31] Allemagne, Autriche, Belgique, Danemark, Espagne, Finlande, France, Grèce, Hollande, Irlande, Italie, Luxembourg, Portugal, Royaume-Uni, Roumanie et Suède.

Il s'agit d'une étude comparative du droit de la procédure, et concrètement des dispositions relatives à l'admissibilité des *preuves électroniques* devant les tribunaux. L'étude a pour objectif de connaître les lacunes existantes et d'identifier les meilleures méthodes pour parvenir à une plus grande protection des intérêts des victimes lors des procédures, en faisant de la *preuve électronique* un outil utile pour lutter contre les délits technologiques.

Avant de présenter les résultats obtenus, nous devons d'abord commenter les limites identifiées au cours de cette étude. Cette étude s'en tient aux paramètres qui sont propres à l'analyse de contenu des lois européennes qui abordent le thème de la *preuve électronique*, mais elle n'en étudie pas les effets sociaux. Nous n'avons pas non plus analysé l'éventuel impact social engendré par les structures de relations juridiques qui sont créées par l'intermédiaire des lois ni leurs éléments les plus significatifs. La pluralité linguistique européenne est une des difficultés à laquelle nous avons été confrontés. Nous avons décidé, d'un commun accord, de travailler en anglais, vu que de nombreuses lois avaient déjà été traduites dans cette langue. Cependant, il y a beaucoup de lois qui n'existent que dans la langue du pays où elles ont été publiées. Finalement, nous devons souligner la difficulté principale intrinsèque de toute étude de droit comparée: toutes les figures et/ou éléments juridiques n'ont pas toutes/tous la même équivalence ou une équivalence identique dans chaque système juridique. Après avoir résolu certaines limites et en tenant compte des difficultés rencontrées, nous avons obtenu des résultats qui nous ont permis de développer une proposition de "guide d'amélioration", qui, à notre avis, constituera une référence dont les professionnels européens devront tenir compte.

DONNÉES ET MÉTHODE

Le Droit de la Procédure Comparé ainsi que la Sociologie du Droit constituent les cadres théoriques choisis pour cette étude. Afin de connaître la réalité juridique et pratique de la *preuve électronique* en Europe, nous avons analysé le contenu des lois et les relations cognitives qui se créent entre les éléments significatifs qui composent ces normes. Etant donné que l'organisation cognitive de l'ensemble des éléments est différente pour chaque réglementation et pays, nous avons choisi différents matériels et différentes méthodes d'analyse.

Pour effectuer l'analyse de la législation, nous avons élaboré un questionnaire, en systématisant la collecte d'informations provenant de données secondaires. Les *données secondaires* sont constituées par les législations de seize pays européens qui réglementent la preuve, la *preuve électronique, l'admissibilité de la preuve ou l'admissibilité de la preuve électronique*.

Pour réaliser l'étude de la réalité, nous avons recueilli les *données primaires suivantes:*

a) Des données provenant d'une enquête présentée à un échantillon de professionnels ayant une relation avec l'analyse légale des moyens électroniques et leur admissibilité, en tant qu'approximation initiale à la notion de *preuve électronique*. Il s'agit d'un échantillon non représentatif d'un point de vue statistique. Il s'agit d'une approximation prospective et les personnes ont été choisies dans des environnements proches à l'utilisation de ce genre de preuve. Toutes les personnes qui ont participé à cette étude ont été choisies en fonction des conditions requises parmi les trois profils adoptés par les chercheurs d'un commun accord. Cependant, le champ d'observation est composé des acteurs sociaux impliqués: avocats, procureurs, juges (civil, pénal, commercial, du travail) représentants du pouvoir judiciaire, notaires, policiers, experts en informatique légal et entrepreneurs. L'objectif est de se rapprocher de manière prospective aux descripteurs de base de la *preuve électronique*.

b) Des données obtenues, suite aux *entretiens en profondeur* réalisés au moins auprès d'un représentant de chaque groupe professionnel, dans chacun des seize pays étudiés. Il s'agit d'un échantillon qualitatif, choisi directement par chaque chercheur. L'objectif est de réunir, pour chaque pays, un éventail divers et hétérogène de participants, qui peuvent exprimer des opinions qui diffèrent de leur manière d'agir sur le terrain et qui peuvent parler des avantages, des inconvénients et des perspectives d'avenir lorsqu'ils traitent des *preuves électroniques*. Pour cette partie concernant le travail de terrain, nous avons utilisé trois protocoles différents, un pour les juristes, un autre pour les experts en informatique légale et enfin un troisième pour les entrepreneurs.

Au total, l'échantillon du champ d'observation est composé de cent vingt-cinq questionnaires et soixante dix-huit lois.

Les structures sont constituées par les relations formées par les éléments juridiques contenus dans les lois qui réglementent la *preuve électronique* en Europe. Elles sont créées "à travers" et "dans" les lois écrites, ce qui constituait un des objectifs de la collecte de données secondaires. Nous cherchons l'univers sémantique de la conceptualisation juridique de la *preuve électronique* par l'association de mots ou de termes utilisés pour définir le concept et l'usage de ces preuves.

Pendant le processus de recherche, nous avons utilisé l'analyse de contenu traditionnel et l'analyse structurale, ou analyse des réseaux sémantiques ou cognitifs. Cette dernière, est une méthodologie apparue récemment qui concentre son attention sur l'interaction entre les éléments observés[32], quel que soit leur niveau d'agrégation (signifiants, individus, groupes, ou organisations). Les processus juridiques et les comportements des professionnels en Europe sont expliqués par l'intermédiaire des structures relationnelles. Les éléments importants se mettent en rapport, entrent en relation[33]. Il s'agit d'une approximation méthodologique qui s'éloigne des processus intuitifs. Expliquer les processus et les comportements sociaux par rapport au réseau de relations qui se mettent en rapport avec les éléments juridiques et les acteurs, constitue une nouvelle approximation théorique de la connaissance scientifique. Les réseaux cognitifs se construisent à partir des éléments juridiques qui sont partagés dans les lois qui réglementent la *preuve électronique*. Cela permet d'acquérir une vision d'ensemble de l'importance que les législateurs et les professionnels européens confèrent à chaque élément. Une forme innovatrice et suggestive de présentation et d'élaboration de l'information a été développée au cours de cette étude. Elle peut nous orienter vers des aspects et des dimensions d'intérêt, dans le cadre général de l'analyse de la réglementation de la *preuve électronique*. Elle permet également d'identifier rapidement et visuellement, parmi une grande quantité d'informations, une ou plusieurs représentations de la notion étudiée. Elle peut également les comparer entre elles, ou entre plusieurs notions parmi les différents documents où est appliquée l'analyse.

A) AU SUJET DE LA PREUVE ÉLECTRONIQUE

L'utilisation de *preuves électroniques* est devenue un élément nécessaire pour essayer de tirer au clair les délits commis avec ou par l'intermédiaire de dispositifs électroniques. Par conséquent, nous avons approfondi le thème de la réglementation de la *preuve électronique* à travers les références trouvées dans les textes légaux européens et roumains en ce qui concerne la preuve en général ou la preuve traditionnelle, aux moyens de preuve, au document électronique et à la signature électronique.

Les références légales peuvent être appliquées à la *preuve électronique* grâce au principe interprétatif de l'application analogique des normes, présente dans les systèmes juridiques, qui permet d'utiliser les dispositions légales pour réglementer une situation spécifique ou une lacune législative. Le principe d'application analogique des normes acquiert une importance très spéciale dans le cas de l'analyse de la législation en Europe en matière de *preuve électronique,* vu qu'il n'existe pas de normes spécifiques pour ce type de preuve. Les découvertes faites dans les normes ont été corroborées par les réponses obtenues sur le terrain: la plupart des juges avec qui nous avons parlé, se basent sur ce concept interprétatif pour essayer de trouver une solution juridique pour les cas où figurent ce genre de preuve.

Définition de *preuve électronique*

Suite à l'examen législatif réalisé, aucune référence directe ni explicite n'a été trouvée concernant la *preuve électronique*, ni aucune définition *per se,* spécifique et exclusive. Cependant, dans tous les pays, il existe des normes qui contiennent des préceptes qui, d'une certaine manière, font référence à la *preuve électronique*.

Dans le cas de l'Allemagne, le *Code de Procédure Pénale* contient des articles applicables à la *preuve électronique*, concrètement, des dispositions relatives à la protection de données lors d'une enquête. Les articles détaillent les conditions de destruction des données sans intérêt spécifique pour les cas. Ce texte comprend également des préceptes sur les mesures à suivre pour garder des données personnelles obtenues lors d'enquêtes dans les bases de données de la police.

Le *Code de Procédure Pénale* en vigueur en Autriche comprend une série de normes, de conditions et de formalités qui doivent être respectées pour prendre des mesures d'*observation des télécommunications*.

[32] Rodríguez, 2005, Mérida, 2004.

[33] Wasserman, 1994; Borgatti, Everett y Freeman 1996; Freeman, Borgatti y White,1991; Burt 1997, 1992, 1982.

En Belgique, la *Loi sur les Délits Informatiques* énonce que les normes concernant la collecte de preuves qui dépendent de cette Loi sont applicables à toutes sortes de preuves et par conséquent, également aux *preuves électroniques*.

La *Législation Procédurale Civile* hollandaise, dispose que *la preuve peut être introduite par tous les moyens, sauf dans les cas explicitement interdits par la Loi.*

En Espagne, le *Code de Procédure Pénal* comprend, parmi les moyens de preuve, *les moyens de reproduction des mots, du son et de l'image, ainsi que les instruments qui permettent d'archiver, de connaître ou de reproduire des mots, des données, des chiffres et des opérations mathématiques réalisées à des fins comptables ou à d'autres fins, importantes pour la procédure*. De plus, dans le *Code Pénal*, l'énumération des différents supports qui peuvent être considérés comme un "document" comprend *n'importe quel support qui contient des données*. Et enfin, pour l'Espagne, la *Loi de Procédure du Travail* permet d'utiliser toutes sortes de preuves, y compris les *moyens mécaniques de reproduction de mots, d'images et de sons.*

Lorsque le *Code de Procédure Judiciaire finlandais* mentionne la charge de la preuve, il la définit comme *les faits qui soutiennent l'action,* entendant par "fait" le numérique tout comme le traditionnel. De plus, la réglementation finlandaise comprend une définition de message électronique, qu'elle définit comme *une information qui a été envoyée par des moyens de transmission électroniques.*

Le *Code Civil* français définit que la preuve par écrit résulte d'une *suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et les modalités de transmission*.

Dans le cas de la Grèce, le *Code de Procédure civile* définit les objets de la preuve, en disposant qu'il peut s'agir seulement de *faits réels avec une influence essentielle pour la décision judiciaire.*

En Irlande, la *Loi de Preuve Pénale* comprend dans la définition de la preuve par écrit les *cartes, les plans, les graphiques, les dessins ou les photographies, ou bien encore la reproduction de manière lisible réalisée en permanence par un ordinateur ou par l'intermédiaire d'autres moyens d'information enregistrée de manière non lisible (…)*.

En Italie, le *Code Pénal* a été mis à jour conformément aux réglementations européennes et comprend un texte qui définit le document électronique comme *n'importe quel outil informatique qui contient des informations ayant une valeur probatoire ou n'importe quel software désigné pour traiter ces informations*. De plus, le *Code de Gouvernement Electronique* de ce pays, donne une définition de document électronique, d'authentification électronique et d'autres concepts comme la carte d'identité électronique ou la certification des fournisseurs de services. En particulier, conformément à ce qui est disposé dans ce texte, un document électronique serait la *représentation électronique d'actes, de faits ou de données ayant une importance juridique* et, d'autre part, la signature électronique est définie comme *un ensemble de données sous forme électronique, unies ou associées de manière logique à d'autres données électroniques, utilisée comme une méthode d'authentification*.

Au Luxembourg, le *Code Civil* a été mis à jour et comprend une définition pour la signature électronique qui est interprétée comme *l'ensemble de données qui sont liées à un document légal de manière indissociable et qui garantissent leur intégrité*.

Dans le cas du Portugal, le *Code de Procédure Pénal* définit la preuve par écrit comme *n'importe quel type de déclaration, symbole ou note présentée sous forme écrite ou sous n'importe quel autre moyen technique conformément aux lois pénales du pays*, comprenant ainsi le document électronique. Le *Code Civil portugais* définit également la preuve par écrit, et englobe les "reproductions mécaniques ou électroniques des documents". Et enfin, au Portugal, nous avons trouvé une définition de document électronique dans la *Loi sur documents et signature électronique* qui dispose que le document électronique est celui qui a été élaboré *par l'intermédiaire du traitement électronique de données.*

Nous avons trouvé une référence plus directe dans le *Code sur la Police et la Preuve Pénale* au Royaume-Uni qui définit la preuve comme *toute information contenue dans un ordinateur*. De plus, le *Code sur les Abus Informatiques* dans ce pays cite plusieurs définitions d'actions technologiques, telles que l'exécution d'un programme constitue "l'utilisation" d'un ordinateur, et les fichiers "log" confirment que le programme a été exécuté.

Dans le *Code de Procédure Pénale* roumain, nous avons trouvé la définition suivante pour la preuve: *tout élément basé sur les faits qui sert à déterminer ou non, l'existence d'une offense criminelle, pour identifier l'acteur et pour connaître les circonstances nécessaires pour adopter une décision juste*.

Aucun système juridique européen ne dispose d'une définition concrète de la *preuve électronique*. Nous avons trouvé des références plus ou moins spécifiques concernant la preuve traditionnelle, qui comprennent pour certains la *preuve électronique*.

Equivalence de la preuve traditionnelle avec la *preuve électronique*

L'analyse du contenu des législations montre que la *preuve électronique* est équivalente à la preuve traditionnelle dans tous les pays analysés. De plus, nous avons trouvé trois types d'équivalences. La première et la plus courante, fait

référence à l'équivalence du document électronique avec le document sur support papier. Certaines lois spécifient le type de document et comparent également le reçu électronique au reçu sur support papier. Le contrat électronique est également comparé au contrat sur support papier et même les notifications réalisées de manière électronique (fax) sont comparées aux notifications traditionnelles.

Le deuxième type d'équivalence est celui qui parle de l'équivalence de la signature électronique avec la signature manuscrite et les actes électroniques notariés avec les actes notariés traditionnels. Pour finir, la troisième catégorie d'équivalence, compare le courrier électronique et le courrier postal. Il faut mentionner ici le cas du Portugal qui compare le courrier électronique à une conversation téléphonique.

Il y a plusieurs Etats[34] qui assimilent expressément les documents électroniques aux documents sur support papier et leur attribuent la validité de la preuve documentaire lors d'un jugement. De plus, il y a un groupe de pays[35] qui compare la signature électronique à la signature traditionnelle, et qui concède aux deux la même valeur devant un tribunal de justice.

Du point de vue de la pratique juridique, la plupart des juges européens considèrent que la *preuve électronique est* équivalente à la preuve traditionnelle. De plus, les représentants du pouvoir judiciaire en Europe considèrent, pour la plupart, qu'elle est équivalente à la preuve par écrit. Il faut mentionner ici quelques opinions dissidentes[36] qui ont déclaré qu'ils la considéraient comme un support différent et non pas comme un moyen de preuve.

La réglementation de la preuve par écrit en Europe joue un rôle important pour envisager la réglementation de la *preuve électronique*.

Avantages et inconvénients de la *preuve électronique*

Les acteurs que nous avons rencontrés interprètent de manière hétérogène les avantages et les inconvénients qui découlent de l'utilisation de la *preuve électronique*. C'est le cas relatif à la "fiabilité". Tandis que certains juges considèrent que son objectivité et son exactitude la rendent plus fiable et par conséquent, sont favorables à son utilisation. D'autres pensent que le manque de connaissances pour vérifier son authenticité la rend plus vulnérable et par conséquent, moins fiable qu'une preuve traditionnelle, constituant donc un inconvénient pour son utilisation et son admissibilité.

Parmi les avantages mentionnés par les juristes et les techniciens, la *preuve électronique* offre une information exacte, complète, claire, précise, véridique, objective et neutre. Etant donné qu'elle provient d'un élément électronique, où la subjectivité n'existe pas, si on la compare, par exemple, aux déclarations de témoins qui peuvent être contradictoires. De plus, ils pensent qu'elle nous permet de disposer d'informations que l'on ne pouvait pas obtenir jusqu'à présent, comme toutes celles contenues dans les dispositifs électroniques.

D'autres informateurs ont mentionné l'avantage de la solidité de ces preuves, leur fiabilité et leur viabilité grâce à l'information qu'elles contiennent. A plusieurs occasions, la *preuve électronique* a été considérée essentielle pour éclaircir certains délits, pour lesquels ce type de preuve constitue le seul moyen probatoire existant. Les *preuves électroniques* s'avèrent donc très utiles dans ces cas là. La facilité et la rapidité d'obtention et d'utilisation de ce type de preuve est un autre avantage mentionné par les juges, ainsi que leur conservation et leur stockage (avantage cité par les notaires européens). Tous les professionnels qui pensent que l'utilisation de documents et de signatures électroniques favorise le développement du commerce électronique et baisse les coûts du courrier coïncident grandement.

Les professionnels du droit perçoivent la difficulté d'établir la valeur juridique de ce type de preuves, à cause d'un manque de connaissances des procédures de traitement de données et de l'interprétation des lois de procédure à ce sujet. Cette difficulté est due à l'absence de réglementation spécifique et systématique, ainsi qu'à l'absence de jurisprudence homogène. De plus, ces professionnels craignent la vulnérabilité et la facilité avec laquelle ces preuves peuvent être manipulées, du fait de leur degré élevé de volatilité, constituant donc un des principaux inconvénients lorsqu'il s'agit de prouver leur authenticité. Certains pensent qu'il s'agit de preuves très techniques, méconnues des juges et des procureurs et difficiles à expliquer, d'où leur rejet à les admettre lors d'un jugement. Les difficultés pour préserver les preuves électroniques et le manque d'information au sujet du stockage correct de ces preuves en vue d'une conservation future, sont d'autres inconvénients qui ont été cités.

Les inconvénients cités par les experts informatiques, du secteur public comme du secteur privé, font référence au

[34] Allemagne, Belgique, Espagne, Finlande, France, Irlande, Italie, Luxembourg, Portugal et Roumanie.

[35] Belgique, Espagne, Finlande, France, Hollande, Italie, Luxembourg, Portugal et Roumanie.

[36] Procureurs au Portugal et en Espagne. Roumanie: ce n'est pas un moyen de preuve parce qu'il n'est pas prévu par la loi.

manque de support légal et de modèles de certification. Ils déclarent qu'elles sont plus difficilement acceptées dans les tribunaux, car les juges demandent plus de garanties qu'ils ne le font pour les preuves traditionnelles. Pour les experts, l'incompréhension montrée par certains organes judiciaires en Europe concernant les tâches qu'ils réalisent constitue un inconvénient. De plus, ces experts considèrent que le processus d'obtention et d'interprétation des informations fournies par un dispositif électronique pour les transformer en *preuve électronique*, nécessite beaucoup de temps, et représente par conséquent un coût élevé, rendant plus difficile son utilisation.

Les avantages offerts par la *preuve électronique* en Europe, consistent principalement à obtenir des informations complètes, véridiques et jusqu'à présent impossible à obtenir. Le degré élevé de spécialisation des connaissances techniques nécessaires pour pouvoir présenter la *preuve électronique* devant les tribunaux, ainsi que le coût en temps et en argent que représente son obtention, constituent les principaux inconvénients.

AVANTAGES:

INFORMATION: EXACTE, COMPLÈTE, CLAIRE, PRÉCISE, VÉRIDIQUE, OBJECTIVE, NOUVELLE ET NEUTRE.

PREUVE: SOLIDE, UTILE, FIABLE, VIABLE, ESSENTIELLE POUR PROUVER CERTAINS DÉLITS QU'IL ÉTAIT IMPOSSIBLE DE PROUVER AUPARAVANT.

FACILE: OBTENTION, UTILISATION, CONSERVATION ET STOCKAGE.

LES DOCUMENTS ÉLECTRONIQUES AINSI QUE LA SIGNATURE ÉLECTRONIQUE FACILITENT LE COMMERCE ÉLECTRONIQUE QUI EST PLUS RAPIDE ET PLUS SÛR.

INCONVENIÉNTS:

- PEU/MANQUE DE RÉGLEMENTATION SPÉCIFIQUE ET SYSTÉMATIQUE.
- JURISPRUDENCE LIMITÉE.
- MATIÈRE MÉCONNUE ET TRÈS TECHNIQUE. PEU D'EXPERTS.
- EXIGE DES CONNAISSANCES SPÉCIFIQUES.
- DIFFICILE DE PRÉSENTER AU TRIBUNAL DE MANIÈRE COMPRÉHENSIBLE.
- PLUS DIFFICILES À ÊTRE ACCEPTÉES DEVANT LES TRIBUNAUX: LES JUGES DEMANDENT PLUS DE GARANTIES QUE POUR LES AUTRES PREUVES.
- MANQUE D'INFRASTRUCTURE TECHNIQUE DANS LES DÉPENDANCES JUDICIAIRES.
- COÛT ÉLEVÉ POUR EXAMINER ET INTERPRÉTER L'INFORMATION.
- DIFFICILE DE SAVOIR COMMENT SONT TRAITÉES LES DONNÉES ET COMMENT SONT INTERPRÉTÉES LES LOIS SPÉCIFIQUES DE PROCÉDURE.
- DIFFICILE DE PROUVER L'AUTHENTICITÉ, L'INTÉGRITÉ, LA FIABILITÉ ET L'ORIGINE DES DONNÉES.
- VOLATILITÉ DES DONNÉES ET MANIPULATION FACILE.
- IDENTIFICATION DIFFICILE DE L'AUTEUR DU DÉLIT.
- DIFFICILE À CONSERVER, PRÉSERVER ET STOCKER.
- DIFFICILE D'ÉTABLIR LA VALEUR JURIDIQUE DE LA PREUVE.
- MANQUE DE SUPPORT LÉGAL ET DE MODÈLES DE CERTIFICATION.

B) AU SUJET DE LA LOI ET DE LA JURISPRUDENCE

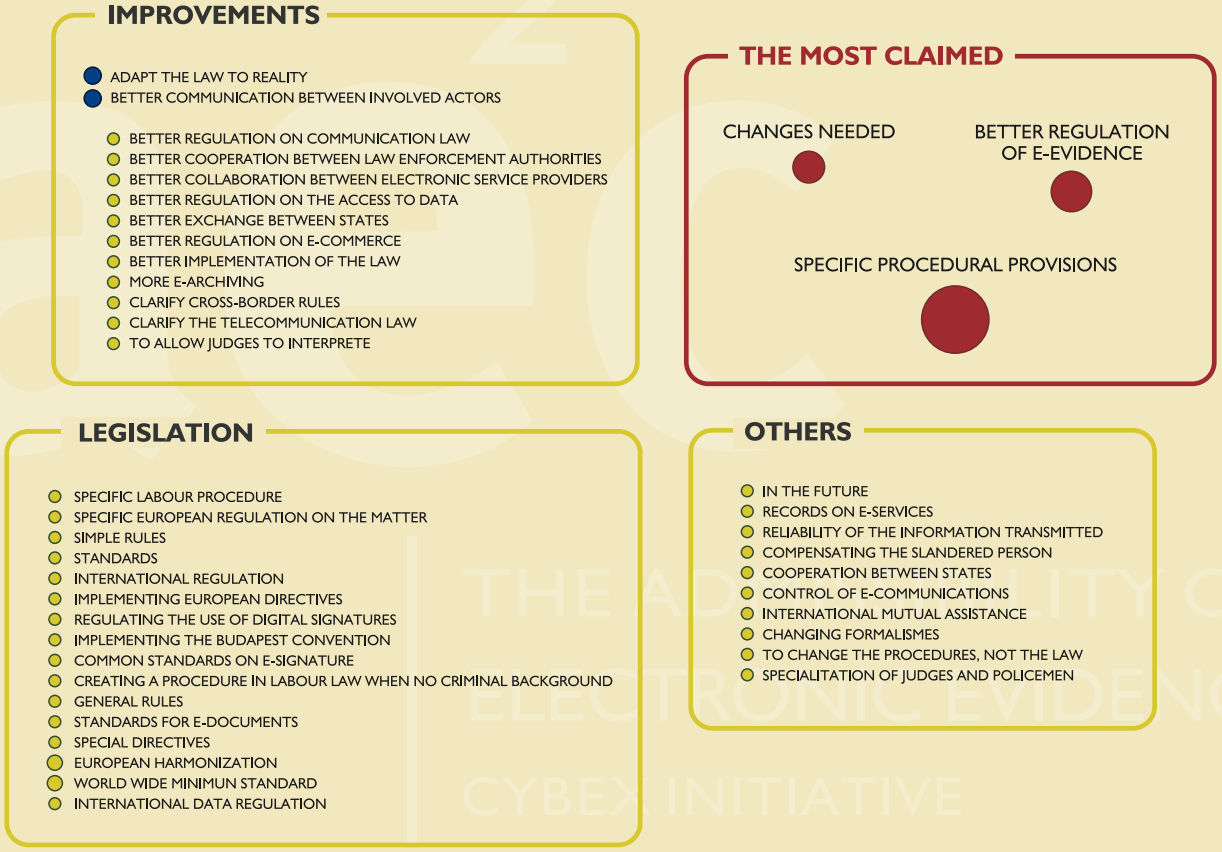
Le cadre légal qui réglemente la *preuve électronique* en Europe est composé fondamentalement d'une série de règles de procédure, de textes de droit civil, pénal et commercial, et de dispositions concernant le commerce électronique ou la signature électronique, parmi lesquelles nous n'avons pas trouvé de réglementation spécifique pour la *preuve électronique*.

L'interprétation analogique des dispositions qui figurent dans ces textes pour la preuve traditionnelle, réglemente également les *preuves électroniques* en Europe.

Nous avons trouvé essentiellement la réglementation de la *preuve électronique* dans les juridictions suivantes: la réglementation du droit civil et du droit pénal, suivis de la réglementation de la preuve dans le droit du travail et de sa réglementation dans d'autres matières légales[37].

La perception subjective des juristes au sujet de la réglementation de la *preuve électronique* (Graphique 1) est hétérogène et présente également de multiples contradictions. Il existe une tendance principale parmi les avocats, les procureurs et les notaires à penser que la *preuve électronique* est actuellement bien réglementée. Cependant,

GRAPHIQUE 1: CHANGEMENTS PRÉFÉRÉS PAR LES JURISTES



Source des données et élaboration propres.

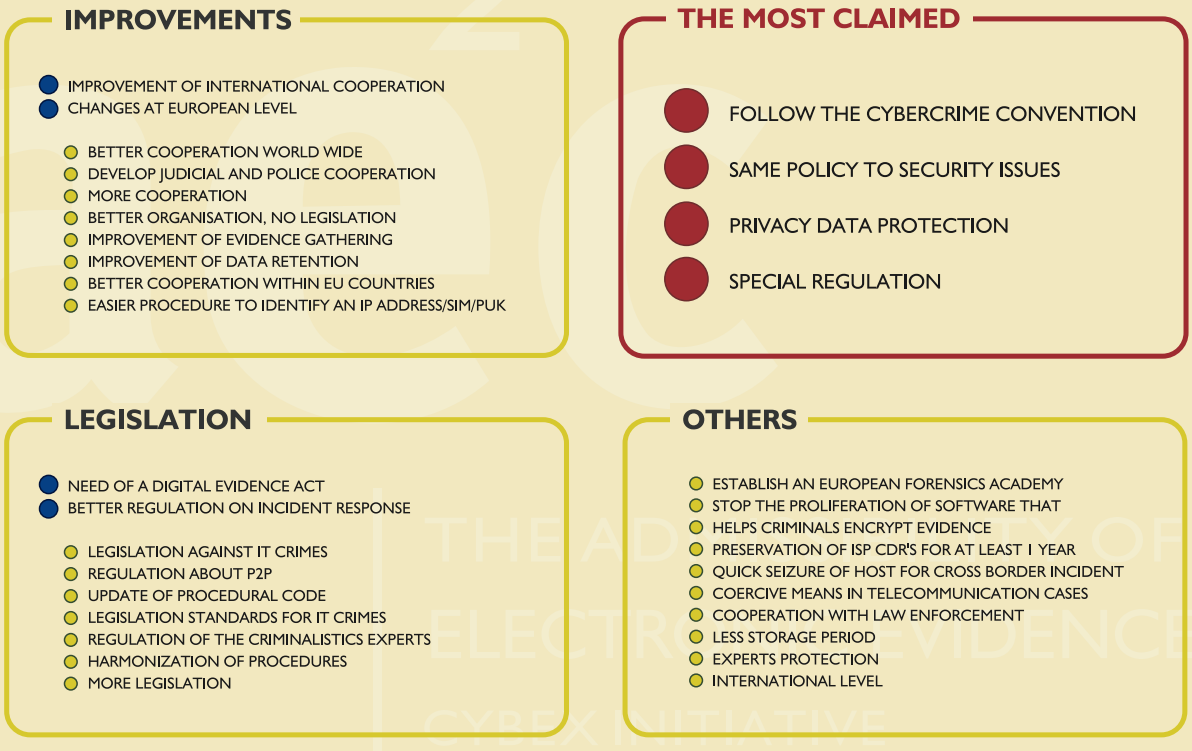
[37] Réglementation administrative, commerciale, lois sur l'organisation judiciaire et règles constitutionnelles.

les juges, qui doivent interpréter la loi à cause de la lacune légale, ont des opinions divisées en fonction de leur spécialité. Mais ils pensent, pour la plupart, que la situation légale actuelle n'est pas appropriée et que des changements sont nécessaires pour adapter les lois à la réalité technologique.

Ceux qui souhaitent changer la situation légale actuelle, préfèrent principalement les changements qui apporteraient une réglementation spécifique des différentes dimensions de la *preuve électronique* et des préceptes spécifiques de procédure au niveau national. D'un autre côté, au niveau européen, les juristes préfèrent l'harmonisation (de la matière), mais ils apostillent qu'elle doit avoir lieu par l'intermédiaire de règles générales qui permettront à chaque pays de les mettre en place en fonction de leur tradition juridique. Et pour finir, il y a ceux qui pensent qu'il devrait y avoir une norme avec des minimums requis au niveau international.

La perception subjective des experts en informatique légale au sujet de la situation légale et jurisprudentielle (Graphique 2), est assez équilibrée. Cependant, la plupart de ces experts[38] pensent que la situation peut être améliorée. Les changements les plus significatifs qu'ils introduiraient consisteraient à: établir une politique de sécurité commune, suivre la réglementation de la Convention sur le Cybercrime du Conseil de l'Europe, établir une réglementation spécifique pour la *preuve électronique* et améliorer la protection des données personnelles.

GRAPHIQUE 2: CHANGEMENTS PRÉFÉRÉS PAR LES EXPERTS EN INFORMATIQUE LÉGALE



Source des données et élaboration propres.

[38] Des experts autrichiens, allemands, irlandais, britanniques et français considèrent que la situation légale et jurisprudentielle est appropriée. La situation pourrait être améliorée pour les experts belges, grecs, espagnols, danois, portugais et roumains. En Italie et en Hollande, les opinions sont contradictoires dans le même pays. L'expert du Luxembourg ne se prononce pas.

Les interprétations des experts légaux et des experts en informatique légale concernant la situation actuelle de l'admissibilité de la *preuve électronique* devant les tribunaux, coïncident sur la nécessité de développer des préceptes spécifiques qui contribueraient à apporter une sécurité juridique. Ils sont également d'accord sur le besoin de développer des normes européennes qui garantiraient une homogénéité minimum pour le traitement de la *preuve électronique*, ainsi que sur le besoin d'établir des règles internationales qui aideraient à améliorer la coopération internationale.

Pertinence d'un cadre européen pour réglementer la *preuve électronique*

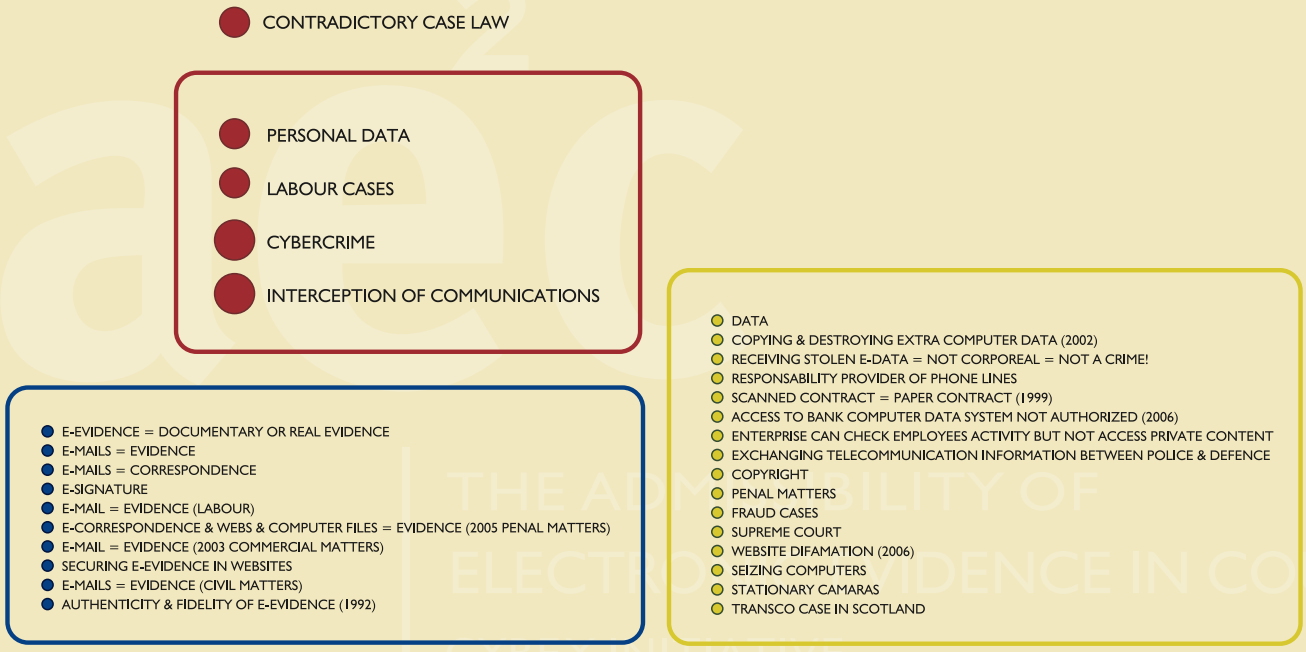
La plupart des juristes européens juge pertinente la possibilité d'établir un type de réglementation pour les différentes dimensions de la *preuve électronique* en Europe. Les arguments sont multiples. Nous avons trouvé des opinions partagées: certains pensent que le cadre européen est nécessaire à cause de la dimension transnationale des délits que les *preuves électroniques* tentent de prouver, et qu'il faciliterait également la coopération internationale. Il permettrait également d'uniformiser, de manière plus importante, le développement de la *preuve électronique*, en réalisant, par exemple, les actions nécessaires suivantes: harmonisation de la protection des données et des procédures de collecte de *preuves électroniques*. Un autre groupe moins nombreux de juristes pense que la réglementation de la *preuve électronique* doit continuer à dépendre exclusivement des États. Les représentants de l'Autriche, du Danemark et de la Finlande pensent que la réglementation nationale est suffisante, étant donné qu'elle couvre tous les aspects de la preuve, y compris la *preuve électronique*. D'un autre côté, il faut signaler les opinions des représentants judiciaires grecs, qui considèrent que sans norme européenne commune, l'adaptation de la législation actuelle à la réalité technologique ne sera pas possible dans leur pays.

Un cadre réglementaire européen qui réglementerait la *preuve électronique* est perçu comme un élément positif pour l'évolution législative de la matière.

Jurisprudence existante

Les cas de jurisprudence actuels les plus importants font référence au cybercrime, à l'interception des communications,

GRAPHIQUE 3: CAS LES PLUS FRÉQUENTS CONCERNANT LA *PREUVE ÉLECTRONIQU*



Source des données et élaboration propres.

aux cas du droit du travail et à la violation de la protection des données (Graphique 3).

Certains juristes ont signalé l'existence de cas de jurisprudence contradictoire qui révèlent un manque d'homogénéité des critères d'admissibilité des *preuves électroniques*. Dans des cas très semblables, les *preuves électroniques* ont parfois été admises et parfois refusées.

Les experts en informatique légale du secteur public travaillent principalement sur des cas de cybercrime, de cyberterrorisme, de pornographie infantile et de délits économiques commis par l'intermédiaire des environnements électroniques. Les experts du secteur privé travaillent plus fréquemment sur des cas d'abus des environnements corporatifs, sur l'étude des appareils technologiques (GSM et SIM *forensics*, récupération de données GPS), sur des incidents de sécurité, des délits économiques et de propriété intellectuelle. Les entrepreneurs sont confrontés à des problèmes dans le monde du travail qui sont habituellement des cas d'utilisation incorrecte et d'abus des ressources corporatives électroniques, ainsi que des problèmes de sécurité des données et des ordinateurs. Ils citent également les fraudes bancaires et les délits commis contre la propriété intellectuelle, en plus des délits qui découlent du commerce électronique. Cependant, la plupart de ces entrepreneurs ne dispose pas de protocole pour réglementer l'utilisation du matériel informatique qui est mis à disposition de leurs employés. Ils ne disposent pas non plus d'une infrastructure qui les conseille pour se protéger contre ce type de délits.

C) AU SUJET DE LA PROCÉDURE POUR L'OBTENTION, LA CONSERVATION ET LA PRÉSENTATION DE LA *PREUVE ÉLECTRONIQUE* DEVANT LES TRIBUNAUX ET SON ADMISSIBILITÉ

Les règles de procédure ne recueillent aucune procédure spécifique qui réglemente l'obtention, la conservation et la présentation de la *preuve électronique* devant les tribunaux de justice. En général, les pays appliquent par "analogie" la réglementation de la procédure générale de la preuve traditionnelle.

Presque la moitié des règles analysées (48%) envisagent des procédures qui sont appliquées de manière analogue à la *preuve électronique*. Les règles qui ressemblent le plus à une procédure en matière de *preuve électronique,* nous les avons trouvées au Royaume-Uni et en Belgique. Le *Code sur la Police et la Preuve Pénale*[39] en vigueur au Royaume-Uni réglemente, de manière spécifique, l'obtention de "preuves d'ordinateurs", et, dans la *Loi belge relative aux Délits Informatiques,* des préceptes sur la collecte des preuves sont inclus et ils sont applicables aux *preuves électroniques*.

Les autres procédures qui peuvent être utilisées par analogie à la *preuve électronique* sont celles envisagées par les lois de procédure en Europe, développées pour l'interception des communications ou des télécommunications, ainsi que les règles de procédure à suivre quand il existe la possibilité d'enfreindre les droits fondamentaux de la personne.

La perception des juristes sur l'existence ou non d'une procédure dépend de l'interprétation que l'on fait du concept "procédure". Certains considèrent que l'application analogique permet d'appliquer les règles de procédure qui existent pour la preuve traditionnelle à la *preuve électronique* et, par conséquent, selon eux, il existe une seule procédure pour toutes les preuves. D'autres ont interprété le concept "procédure" d'une manière plus restreinte et considèrent qu'il n'existe pas de procédure concrète pour la *preuve électronique,* ou qu'il existe seulement des préceptes qui réglementent certains aspects de l'obtention, la conservation et la présentation de ce type de preuves. Par exemple, c'est le cas de la procédure à suivre en matière pénale pour contrôler les communications par l'intermédiaire d'un moniteur et pour les intercepter. Procédure qui consiste à demander au juge un ordre judiciaire. Cet ordre judiciaire est également nécessaire pour réaliser une enquête, ou pour obtenir des preuves ou des *preuves électroniques* dans les cas où il peut y avoir violation des droits fondamentaux.

Les notaires, à l'unanime, pensent qu'ils ne disposent pas de procédure spécifique pour garder les *preuves électroniques* et

[39] Police and Criminal Evidence Act, PACE.

les procédures auxquelles ils se réfèrent sont celles utilisées pour la création des signatures électroniques. En Italie, les notaires peuvent utiliser des procédures informelles pour archiver les documents électroniques, dont l'exécution n'est pas obligatoire.

La police et les experts privés en informatique légale ne disposent pas d'une procédure spécifique pour l'obtention, la conservation et la présentation de la *preuve électronique* devant les tribunaux, à l'exception de l'Autriche et de la Roumanie. Dans ces pays, il existe bien une procédure pour l'obtention[40]. Au Royaume-Uni[41] et en Roumanie[42] la procédure consiste à suivre les règles internes de la police. Au Luxembourg, la police travaille actuellement sur une procédure interne d'obtention et d'analyse de *preuves électroniques*. En Finlande, ils sont en train d'élaborer une stratégie d'enquête criminelle de IT, qui peut devenir par la suite un manuel de procédure.

Du point de vue de la pratique légale, les juristes sont d'accord sur le fait qu'en Europe, il existe des règles de procédure générale qui réglementent l'obtention de la preuve en matière pénale et commerciale dans certains cas (Finlande), qui peuvent être appliquées aux *preuves électroniques* par analogie, mais pas dans le reste des juridictions. Ils mentionnent également qu'aucune procédure n'a été établie pour la conservation ou la préservation de la *preuve électronique* et que la présentation de celle-ci, devant les tribunaux, se fera dans chaque pays en fonction de l'interprétation analogique des préceptes définis pour la preuve traditionnelle, c'est à dire, en tant que preuve par écrit et en tant que preuve par témoins dans la plupart des cas.

Dans le système réglementaire procédural en vigueur en Europe, il n'existe pas de procédures spécifiques qui réglementent l'obtention de la *preuve électronique*, à l'exception des préceptes législatifs de deux pays, le Royaume-Uni et la Belgique. Préceptes qui sont relatifs à l'obtention de preuves d'ordinateurs. Dans aucun pays européen nous n'avons trouvé de procédure pour la préservation et la présentation de la preuve électronique devant les tribunaux.

D) AU SUJET DE L'ADMISSIBILITÉ DE LA *PREUVE ÉLECTRONIQUE*

Autorité compétente pour l'admissibilité des *preuves électroniques*, motivation de l'exclusion et garde des *preuves électroniques*

La figure du juge ou du tribunal s'est révélée être l'autorité compétente maximum pour décider de l'admissibilité ou non d'une *preuve électronique* en Europe, en suivant le résultat de l'analyse des législations comme celui des questions posées aux juristes. Dans certains pays comme la Grèce ou le Luxembourg, en plus des mentions faites au juge, nous avons trouvé des références particulières à la figure du procureur général en tant qu'autorité compétente.

L'admissibilité est très liée à la possibilité, ou non, d'exclusion de la *preuve électronique* sans motivation préalable. Nous pouvons affirmer qu'aucune des règles analysées ne permet, ni aucune des personnes interrogées n'accepte, la possibilité d'exclure une *preuve électronique* sans la motivation pertinente de l'organe judiciaire. Cependant, les juges commerciaux danois précisent que dans certains cas, la motivation de l'exclusion de la preuve et de la *preuve électronique* peut se faire très brièvement et verbalement pendant l'audience.

Pendant l'enquête, ce sont les agents de la police et les procureurs qui sont chargés de garder la *preuve électronique* au cours des procédures pénales. Pendant la phase du jugement, c'est l'organe judiciaire qui est chargé de garder ces preuves (concrètement, la figure du secrétaire-greffier dans la plupart des pays). En matière civile, ce sont principalement les parties qui gardent les preuves qui seront présentées devant le juge ou le tribunal, quand celui-ci en formule la demande, pendant la phase préalable au jugement comme pendant celui-ci. Dans certains pays, les notaires et les experts sont chargés de garder et de faire parvenir au tribunal, le cas échéant, les *preuves électroniques*.

Conditions requises que doit respecter la *preuve électronique* pour être admise devant les tribunaux

En Europe, conformément aux textes légaux, deux modèles de pays coexistent en ce qui concerne les conditions requises que doivent remplir les preuves pour être admises lors d'un procès. Un groupe de pays a en commun une tradition juridique qui établit des critères très vastes d'admissibilité de la preuve. Ils se basent sur la libre considération du juge au moment d'admettre ou non la *preuve électronique* (Autriche, Danemark, Suède,

[40] En Roumanie, le "G8 Proposed Principles for the Procedures Relating to Digital Evidence" ce n'est pas obligatoire ou de compliment recommandé.

[41] Association of Chef Police Officers.

[42] Guidelines: Operational procedure to be followed for search of computers.

Finlande). L'autre groupe de pays a en commun des législations qui réglementent de manière plus restrictive, l'admissibilité de la preuve en fonction d'un ensemble de conditions requises, de la preuve ou des moyens de preuves, établies par la loi.

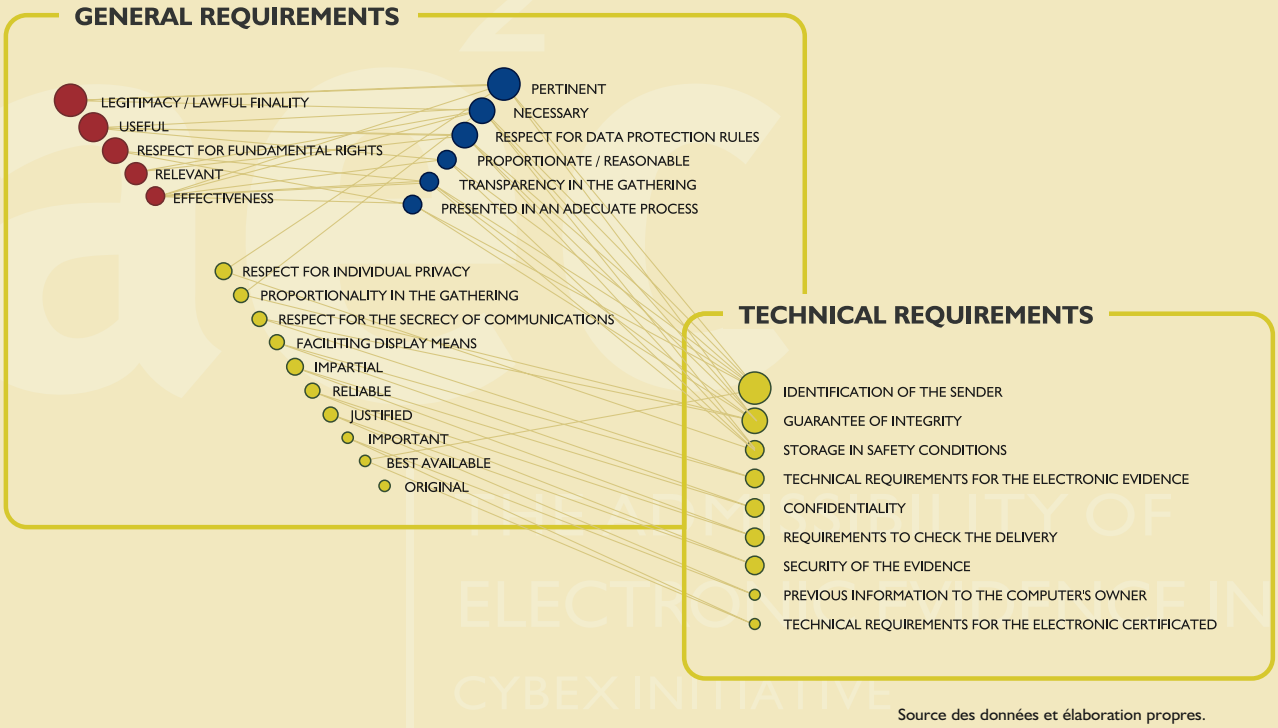
La légalité de la preuve[43] est la condition requise la plus fréquemment citée par les lois (Graphique 4). Dans certains pays, comme l'Allemagne, l'Irlande et le Royaume-Uni, la doctrine du fruit de l'arbre empoisonné[44] n'est pas appliquée, de ce fait la condition de la légalité n'est pas toujours appliquée.

Une autre condition requise envisagée par les lois est le respect des droits fondamentaux[45], parmi ces droits, il est fréquent de trouver des mentions concernant les règles sur la protection des données personnelles et les droits des travailleurs. La fiabilité de la preuve, ainsi que sa pertinence, et le fait qu'elle constitue la meilleure preuve disponible à un moment précis, sont d'autres conditions requises fondamentales que le juge examinera pour décider de l'admissibilité d'une preuve en particulier.

Les autres conditions requises recueillies tout au long des législations et dont le respect marquera l'admissibilité ou la non admissibilité de la *preuve électronique* sont: l'utilité, la proportionnalité et le caractère effectif de la preuve. Entendant par caractère effectif la capacité de prouver la déclaration.

Pour finir, certaines lois demandent que la preuve soit originale dans la mesure du possible, et qu'il ne s'agisse pas d'une copie.

GRAPHIQUE 4: CONDITIONS LÉGALES DE LA *PREUVE ÉLECTRONIQUE* POUR QU'ELLE SOIT ADMISE DANS UN JUGEMENT



Source des données et élaboration propres.

[43] Code civil italien. Code de procédure pénale allemand, belge, irlandais, portugais, roumain. Lois de procédure civile en Espagne, France, Grèce, Hollande, Luxembourg, entre autres exemples.

[44] Cette doctrine définit le caractère illicite des preuves obtenues à partir d'une procédure corrompue, elles sont donc contaminées par l'illégalité de la procédure.

[45] Loi de procédure danoise. Loi de procédure civile en Espagne, au Luxembourg. Code de procédure pénale allemand ou portugais entre autres exemples.

En plus de l'originalité, la preuve doit être directe et ne pas être fondée sur les ouï-dire ni indirecte, (connue sous le terme de *hearsay*). Il s'agit de règles d'exclusion qui régissent l'admissibilité de la *preuve électronique* au Royaume-Uni et en Irlande.

Si les conditions requises citées auparavant apparaissent dans les textes légaux, dans la pratique judiciaire, elles ne sont pas toujours respectées par toutes les parties. Nous avons voulu savoir quelles sont les conditions requises qui sont le moins souvent respectées dans le cadre juridique européen. L'opinion subjective des juristes démontre qu'il s'agit du respect des droits fondamentaux, et tout particulièrement du droit à la protection des données et les droits des travailleurs ceux qui sont le moins respectés lors de la présentation de la *preuve électronique* devant les tribunaux. Ce qui fait que ces preuves sont souvent rejetées. Les conditions techniques formelles qui sont le moins souvent respectées en Europe sont celles relatives à l'application des mesures nécessaires pour vérifier l'authenticité et l'inaltérabilité du document électronique, du courrier électronique envoyé, ainsi que l'absence de signature électronique dans les documents qui n'ont plus de force probante au moment où ils sont présentés devant les tribunaux. De plus, dans de nombreux cas, la chaîne de garde a été transgressée, générant ainsi une insécurité juridique de la *preuve électronique* présentée.

Influence du respect des garanties de légalité

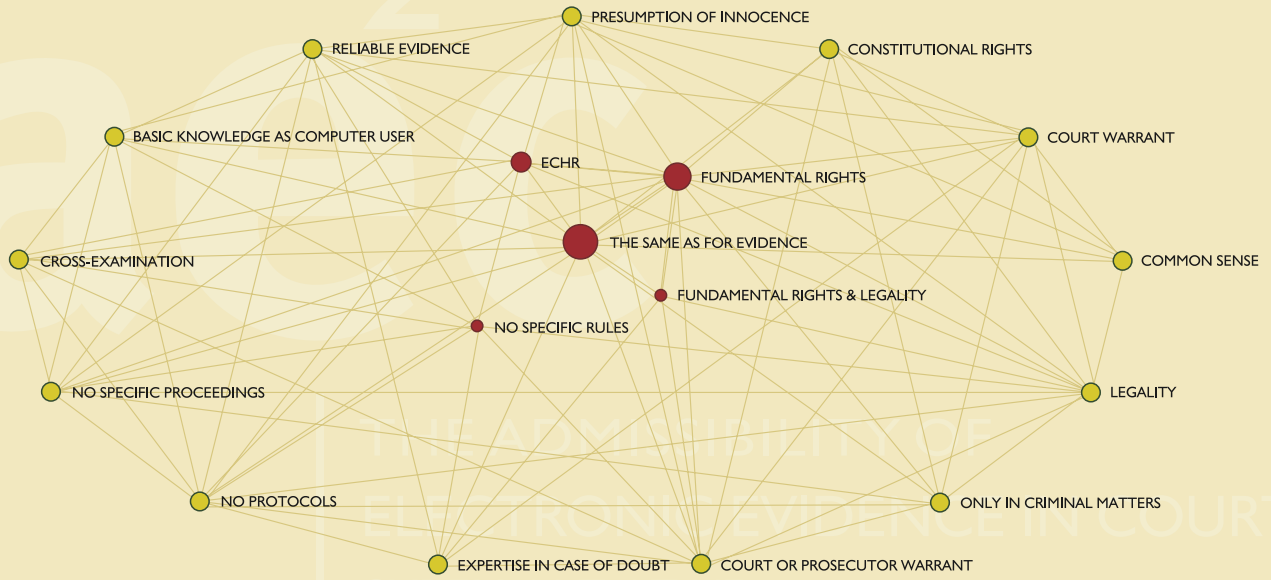
a) Sur l'admissibilité de la *preuve électronique*

Le respect des garanties de légalité est l'une des conditions exigées par la plupart des législations. Dans la pratique, l'ensemble des magistrats pense que le respect de ces garanties de légalité a une influence positive sur l'admissibilité de la *preuve électronique*. D'autres professionnels de la justice signalent qu'il est fondamental que le jugement soit juste ou que la vérité matérielle soit obtenue (Danemark et Finlande). Au Danemark, ils précisent également que ces garanties auront seulement une influence si l'une des parties objecte au sujet du respect des garanties de légalité.

b) Sur le processus d'obtention, d'analyse et de présentation de la *preuve électronique* lors d'un procès

En ce qui concerne les garanties de légalité qui doivent être prises en compte au cours du processus d'obtention, d'analyse et de présentation de la *preuve électronique* lors d'un procès, une bonne partie des opinions exprimées par

GRAPHIQUE 5: PERCEPTION DES GARANTIES DE LÉGALITÉ QUI SELON LES JURISTES DOIVENT ÊTRE RESPECTÉES



Source des données et élaboration propres.

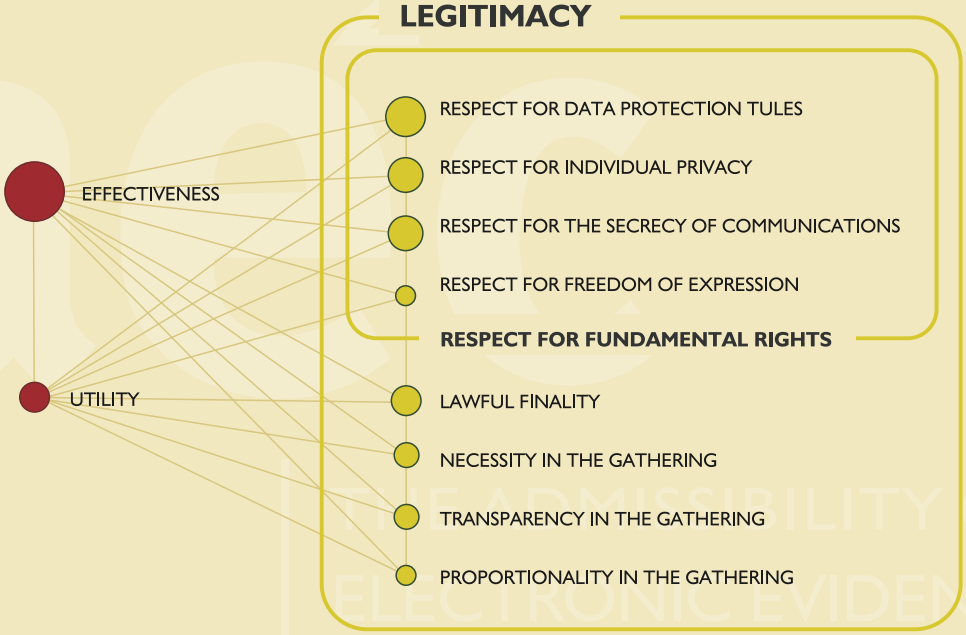
les juristes européens signalent le manque de règles spécifiques à ce sujet (Graphique 5). Ils affirment donc être en faveur du même type de mesures qui doivent être respectées pour tout autre type de preuve. Les mentions positives insistent sur le respect des droits fondamentaux et sur la jurisprudence provenant de la Cour européenne des Droits de l'Homme, ainsi que sur le respect de la légalité.

Principes qui affectent l'admissibilité de la *preuve électronique*

Les principes relatifs à l'efficacité, à l'utilité et à la légitimité de la *preuve électronique* occupent un rôle important au sein des différentes législations européennes. La nécessité de l'obtention de la preuve, la transparence pendant l'obtention et le respect de la liberté d'expression sont des principes qui sont exprimés dans les règles, mais qui occupent une position secondaire en ce qui concerne l'admissibilité de la preuve. Les principes qui concernent de manière concrète la *preuve électronique* et qui sont donc plus importants, sont: le respect des règles de protection des données, le respect du secret des communications et le respect du droit de la liberté d'expression (Graphique 6).

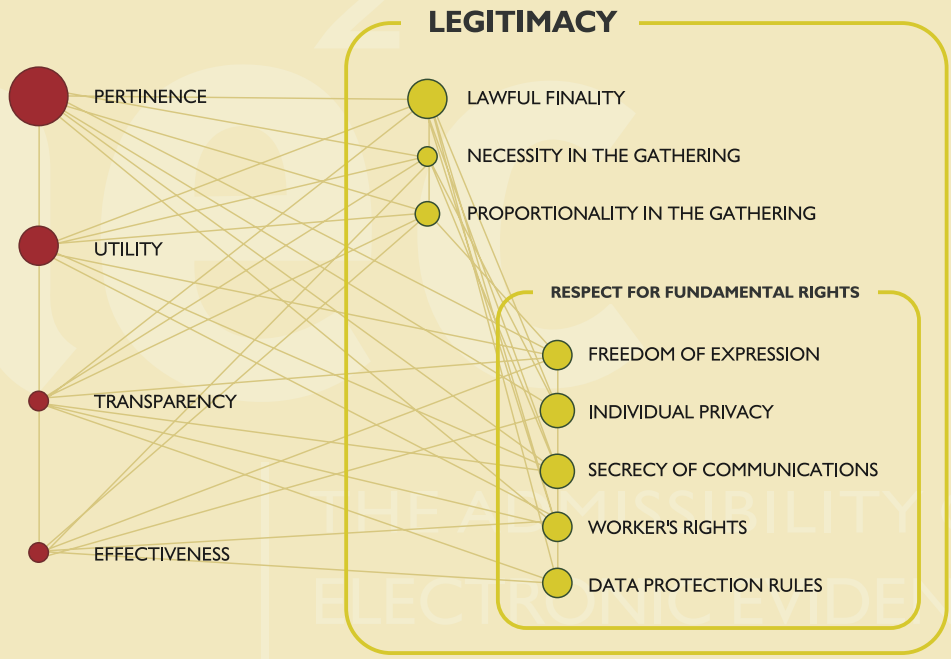
Dans la pratique, tandis que les juristes européens considèrent que ce sont les principes de légitimité (soulignant la position privilégiée en tant que partie intégrante de ce principe) du respect des droits fondamentaux, de la pertinence de la preuve et de son utilité qui ont le plus d'influence. Les techniciens experts en informatique légale soulignent qu'ils agissent en tenant compte du respect des droits individuels. De plus, ils mentionnent le respect des règles de protection des données (Allemagne et Grèce), le maintien de la confidentialité (France, Luxembourg et Irlande), le développement de leurs fonctions en utilisant un matériel crypté comme principes de bases (Italie et Royaume-uni). De plus, ils expliquent qu'ils disposent du support légal d'un notaire (Espagne), et de la présence de témoins (Espagne et Roumanie) (Graphique 7).

GRAPHIQUE 6: PRINCIPES LÉGAUX TROUVÉS DANS LES LÉGISLATIONS QUI CONDITIONNENT L'ADMISSION DE LA PREUVE



Source des données et élaboration propres.

GRAPHIQUE 7: PERCEPTION DES JURISTES DES PRINCIPES QUI CONCERNENT L'ADMISSIBILITÉ DES *PREUVES ÉLECTRONIQUES*



Source des données et élaboration propres.

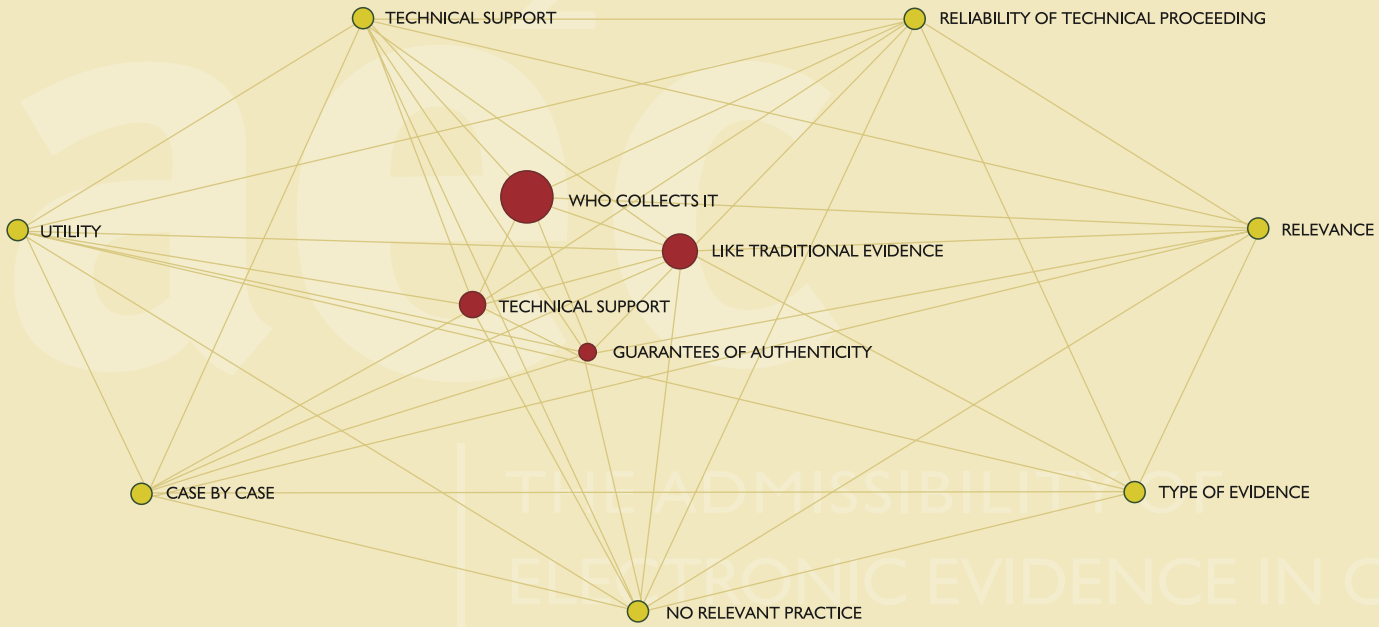
Facteurs qui ont une influence sur la valeur probatoire de la *preuve électronique*

Le respect de la légalité pour l'obtention de la preuve a un rôle fondamental lorsqu'il s'agit d'évaluer son admissibilité. Pour cette raison, nous avons voulu connaître les responsables chargés d'obtenir la preuve, qu'elle soit traditionnelle ou électronique, conformément aux lois. D'un côté, l'organe judiciaire, avec les figures du juge ou du tribunal et du procureur en collaboration avec la police, a un rôle fondamental pour obtenir les preuves en Europe. D'un autre côté, la législation concède aux parties la responsabilité de l'obtention de la preuve en matière civile. La figure de l'expert, est également citée en tant qu'agent responsable de l'obtention de la *preuve électronique,* en matière civile tout comme en matière pénale.

L'affirmation précédente acquiert une importance particulière en sachant que, selon les opinions des juristes, la personne chargée de l'obtention de la *preuve électronique* est le facteur qui a le plus d'influence sur la valeur probatoire qui peut lui être attribuée. Ce qui indique que, étant donné que c'est la police qui est chargée d'obtenir la *preuve électronique,* comme elle dispose du soutien de l'organe judiciaire, son évaluation est importante lorsqu'il s'agit d'admettre ou non une preuve. Le soutien technique d'un côté et les garanties d'authenticité de l'autre, complètent l'ensemble des facteurs qui ont le plus d'influence sur les organes européens chargés de juger, lorsqu'il s'agit de concéder une valeur probatoire plus ou moins importante à une preuve en particulier. Un autre groupe de magistrats ne considère pas qu'il existe un facteur important, mais qu'il faut tenir compte des mêmes facteurs que pour la preuve traditionnelle.

Ces affirmations démontrent le degré d'intérêt et de préoccupation pour l'authenticité et l'intégrité de ce type de preuves, que partage le collectif judiciaire européen.

GRAPHIQUE 8: PERCEPTION DES JURISTES DES FACTEURS QUI DONNENT PLUS DE VALEUR PROBATOIRE À LA *PREUVE ÉLECTRONIQUE*



Source des données et élaboration propres.

E) AU SUJET DES EXPERTS EN INFORMATIQUE LÉGALE

Formation et conditions requises pour travailler en tant qu'expert en informatique légale en Europe

En Europe, il n'existe pas de normes qui déterminent les caractéristiques que doit posséder un expert en informatique légale. En l'absence de préceptes légaux, les juristes tout comme les experts tiennent compte avant tout de l'expérience spécifique.

La maîtrise est, selon les experts, la formation minimum de base pour qu'ils se considèrent eux-mêmes experts en informatique légale. Il est préférable de posséder une maîtrise en informatique, en ingénierie ou en mathématiques. De plus, ils considèrent qu'une formation continue et spécialisée est essentielle et constitue le seul moyen d'actualiser les connaissances. Nous savons également que la police spécialisée reçoit une formation interne de la part d'organismes publics, nationaux et internationaux et également de sociétés privées. Cependant, nous n'avons pas trouvé de formation universitaire réglementée en matière d'analyse légale des environnements numériques, tandis qu'il existe bien des formations de troisième cycle en informatique légale (France) et en enquête sur les cybercrimes (Irlande). En Europe, les experts privés d'informatique légale coexistent avec ceux des forces et des corps de sécurité de l'Etat. Seul en Roumanie, pour exercer comme expert, il faut être muni d'un certificat émis par les autorités publiques de l'Etat.

La plupart des professionnels du droit considèrent que les lois ne précisent pas les conditions spéciales qu'il faut remplir pour exercer en tant qu'expert en informatique légale devant un tribunal. Pour eux, la condition formelle d'être inscrit sur la liste des experts que possèdent les tribunaux en Europe est fondamentale. Ceux qui pensent que la condition à remplir est d'être "expert en informatique"sont moins nombreux.

Perceptions des experts en informatique légale vus par les juristes européens et par les experts consultés

Les juristes européens pensent principalement que ce sont les policiers ou les procureurs qui devraient être experts en informatique légale. De plus, ils pensent que ces professionnels devraient posséder un certificat d'analyse légale délivré par le secteur privé. L'opinion des experts est très divisée. Les experts préfèrent, du fait de l'absence de diplôme spécifique, avoir au moins cinq ans d'expérience professionnelle. En ce qui concerne les professions qu'ils considèrent les mieux appropriées pour être experts, on trouve les avocats et les policiers.

GUIDE D'AMÉLIORATION

Les sources qui ont inspiré ce guide d'amélioration sont basées sur les perceptions et les visions subjectives des professionnels suivants: juristes, techniciens et entrepreneurs européens.

- En ce qui concerne la **réglementation** de la *preuve électronique*, **les juristes** considèrent qu'il faut réaliser des changements, sur le plan national, au sein du corps législatif actuel, changements qui contribueront à diminuer le degré d'insécurité législative. Ils plaident en faveur d'une meilleure réglementation nationale de la *preuve électronique*, et concrètement de la procédure, ce qui permettra d'obtenir, de préserver et de présenter ces preuves en respectant toutes les garanties légales spécifiques/propres, pour qu'elles soient admises, lors des jugements, comme une typologie supplémentaire de preuve. Au niveau européen et international, ils expriment le besoin de développer un ensemble de directives de minimums en matière de procédure, afin d'assurer une bonne coopération entre les Etats pour l'obtention et la préservation. La coopération internationale est essentielle pour obtenir une plus grande efficacité dans la lutte individuelle de chaque pays contre les délits commis par l'intermédiaire des/ou dans les environnements numériques qui, de par leur nature, sont dans de nombreuses occasions transnationaux.

  Pour **les experts en informatique légale**, du secteur public comme du secteur privé, il faut tout d'abord que la *preuve électronique* dispose d'une réglementation spécifique au niveau national. D'autres recommandent sa réglementation en mettant en place des protocoles qui développeraient la protection des droits fondamentaux durant les phases d'obtention, de préservation et de présentation de la *preuve électronique*, pour pouvoir ainsi améliorer le respect des garanties d'admissibilité de ce type de preuves. Comme les juristes, ils pensent qu'il faut réaliser des changements au niveau européen, en établissant des règles minimums de procédure. Ils pensent tout particulièrement qu'il est très important que les pays respectent les dispositions contenues dans la Convention du Conseil de l'Europe sur les Cybercrimes adoptée à Budapest. De plus, ils pensent qu'il faudrait agir au niveau international pour améliorer la coopération entre les États en matière d'obtention et de préservation.

AU SUJET DE LA RÉGLEMENTATION DE LA *PREUVE ÉLECTRONIQUE*:

- RÉGLEMENTATION SPÉCIFIQUE AU NIVEAU NATIONAL TOUT COMME AU NIVEAU EUROPÉEN AFIN D'APPORTER UNE SÉCURITÉ JURIDIQUE.
- RÉGLEMENTATION EUROPÉENNE POUR GARANTIR L'HOMOGÉNÉITÉ DU TRAITEMENT DES PREUVES.
- RÈGLES INTERNATIONALES QUI CONTRIBUERONT À AMÉLIORER LA COOPÉRATION INTERNATIONALE.

- En ce qui concerne **la profession de l'informatique légale**, **les juristes tout comme les experts** sont d'accord sur le fait que pour exercer cette profession, l'expérience constitue un élément clé et ils lui confèrent une grande valeur pour le présent comme pour le futur. Ils pensent également qu'un professionnel en informatique légal devrait posséder une maîtrise en informatique, en ingénierie ou en mathématiques. De plus, les experts considèrent qu'ils devraient disposer d'un certificat d'analyse légale des environnements numériques délivré par une autorité publique, et avoir au moins deux d'expérience en cas de diplôme universitaire. Pour ceux qui n'ont pas de formation universitaire, ils pensent qu'ils devraient avoir au moins cinq ans d'expérience spécifique. Ils mettent également l'accent sur la nécessité de la formation continue. Pour leur part, les juristes pensent qu'un professionnel doit être membre de la police et disposer d'un certificat privé d'analyse légale des environnements numériques.

- **Les entrepreneurs et les organisations professionnelles** européens parlent principalement de trois grands thèmes: prévention, formation et législation. En ce qui concerne la prévention, ils défendent la nécessité de créer des protocoles informatiques standards pour que les entrepreneurs puissent les utiliser dans leur travail. En ce qui concerne la formation, ils pensent qu'il faudrait mettre en place des initiatives de conseil. Des mesures qui leur permettraient de savoir comment procéder pour recueillir et stocker des *preuves électroniques* afin de ne pas amoindrir leur valeur probatoire devant les tribunaux. Ils plaident également pour l'utilité de l'échange de bons usages entre pays. Sur le thème de la législation, ils expriment le besoin de réformer et d'éclaircir la législation existante en matière de *preuve électronique*. Ils proposent tout particulièrement d'augmenter la sécurité des communications électroniques, la mise en place effective de la signature électronique et la réduction du temps de stockage des documents. Cependant d'autres entrepreneurs, provenant d'autres pays européens, où le principe de la libre admissibilité de la *preuve électronique* est en vigueur, pensent que la situation légale et jurisprudentielle est appropriée et qu'il n'est pas nécessaire de modifier la législation.

ACTIONS DE CHANGEMENT SUGGÉRÉES PAR LES ENTREPRENEURS EUROPÉENS:

- PRÉVENTION: PROTOCOLES INFORMATIQUES.
- FORMATION: CONSEILS CONCERNANT LA PROCÉDURE DE COLLECTE ET DE STOCKAGE.
- LÉGISLATION: RÉFORME ET ÉCLAIRCISSEMENT DE LA RÉGLEMENTATION EXISTANTE.

- Certains considèrent que le futur de la *preuve électronique* passe par sa réglementation spécifique au niveau national comme au niveau européen. Ce qui permettra d'assurer le développement progressif de la matière en adaptant, de manière appropriée, la législation aux nouvelles réalités sociales existantes. D'autres pensent au contraire que le principe de liberté de la preuve doit prévaloir dans la réglementation de la *preuve électronique* et que son évolution passe par l'absence de réglementation. Ils considèrent que la situation d'admissibilité actuelle est appropriée et qu'il n'est pas nécessaire de la changer dans l'avenir.

Les juristes pensent qu'il faudrait également améliorer la communication entre les acteurs impliqués dans l'admissibilité de la *preuve électronique*, parmi lesquels nous trouvons les responsables de l'obtention, la préservation et la présentation de celle-ci lors des jugements, et les juges chargés de se prononcer sur son admissibilité. Les techniciens, au contraire, soulignent qu'il est important d'effectuer des changements au niveau de la protection du respect du caractère privé des données personnelles et d'appliquer des politiques homogènes en matière de sécurité.

VISIONS DU FUTUR:

- CONTRADICTOIRES AU SUJET DE LA RÉGLEMENTATION SPÉCIFIQUE
- AMÉLIORATION DE LA COMMUNICATION
- AUGMENTATION DE LA PROTECTION DU RESPECT DU CARACTÈRE PRIVÉ DES DONNÉES PERSONNELLES.

POINTS CLÉS POUR AMÉLIORER LA RÉGLEMENTATION:

- LES JUGES SONT LES ACTEURS PRINCIPAUX DE L'ADMISSIBILITÉ DE LA *PREUVE ÉLECTRONIQUE* ET LES EXPERTS DE LA POLICE OCCUPENT UNE POSITION PRINCIPALE POUR L'OBTENTION DES PREUVES. *AGISSONS SUR CES DEUX TYPOLOGIES D'ACTEURS.*
- LA LÉGISLATION EXERCE UNE INFLUENCE POSITIVE SUR LES PERCEPTIONS DE SÉCURITÉ QUE POSSÈDENT LES DIFFÉRENTS AGENTS SOCIAUX. *ADAPTONS LA LÉGISLATION EXISTANTE.*
- LES EXPERTS EN RELATION AVEC L'OBTENTION, L'ANALYSE ET LA CONSERVATION DE LA *PREUVE ÉLECTRONIQUE* SUSCITENT CONFIANCE. *SUIVONS LES PROCÉDURES TECHNIQUES DES EXPERTS.*
- FORMATION, CONNAISSANCE ET EXPÉRIENCE CONSTITUENT LES ÉLÉMENTS NÉCESSAIRES ET INDISPENSABLES QUE DOIVENT RÉUNIR LES EXPERTS. *AGISSONS SUR LA FORMATION.*
- L'AMÉLIORATION DE LA COMMUNICATION ENTRE LES ACTEURS AYANT UNE RELATION AVEC LA *PREUVE ÉLECTRONIQUE*, AU NIVEAU NATIONAL, EUROPÉEN ET INTERNATIONAL, EST UN BIEN APPRÉCIÉ ET DÉSIRÉ À L'UNANIMITÉ. *AMÉLIORONS L'ENTENTE ENTRE LES JUGES ET LES TECHNICIENS.*

RÉFERENCES

- *Act on Electronic Services and Communication in the Public Sector.* Act n. 13 of 2003 in Finland Statutory Book. Finland.
- *Act on Electronic Signatures.* Act n. 14 of 2003. Finland.
- *Act on Provision of Information Society Services.* Act n. 458/2002 in Finland Statutory Book. Finland.
- BURT, R. S. (1982). *Toward a Structural Theory of Action: Network models of stratification, perception and action.* New York: Academic Press.
- BURT, R. S. (1992). *Structural Holes: The social Structure of Competition*. pp. 260-269. Cambridge, MA: Harvard University Press.
- BURT, R. S. (1997). "*The contingent value of social capital*", pp. 339-365. Administrative Science Quarterly n. 42.
- *Civil code.* DL 47 344 of 25 November 1966. Portugal.
- *Civil code.*1992.Updated at September 2001. Greece.
- *Civil evidence Act.*1995. United Kingdom.
- *Civil procedure code.* A.N. 44/1967 of 16-09-1968. Greece.
- *Civil procedure code*. DL 44-129 28-12-61 (Original code) DL 53/2004 updated version 18 March 2004. Portugal.
- *Code civil*. 8 mars 1803. 2004. Luxembourg.
- *Code civil.*1804. 2005. France.
- *Code de commerce.*15 septembre 1807. 2000. Luxembourg.
- *Code de commerce.* N. 2000/912 du 18 septembre 2000. 2005. France.
- *Code de justice administrative*. N. 2000-387 du 4 de mai. 2005. France.
- *Code de procédure pénale*. 2 mars 1959. 2005. France
- *Code d'instruction criminelle*. N. 447 du 22 septembre 1988. Modifié par Loi n.46/2006. Luxembourg.
- *Code du travail*. 2005. France.
- *Code of civil procedure*. 01/01/2002. Greece.
- *Code of judicial procedure.* N. 4 1734 in Statutory Book/chapter on evidence amended by 571/1948 and other sections by Act 690/1997. Finland.
- *Code of juridical procedure*. Promulgated in 1942, came into force on 1 January 1948. 1999. Sweden.
- *Codice civile*. Regio Decreto,n. 262 16/03/1942. Italy.
- *Codice di procedura civile*. Regio Decreto n. 1443, 28/10/1940. Italy.
- *Codice di procedura penale*. Decreto del Presidente della Repubblica n. 447, 22/09/1988. Italy.
- *Codice penale*. Regio Decreto, n. 1398, 19/10/1930. Italy.
- *Código civil* de 24 de julio de 1889. Actualizado 2000. Spain.
- *Código penal*. Ley n.10/1995 de 23 de noviembre 1995. 2005. Spain.
- *Codul civil*. N. 1655 4/12/1887 as amended by Decree 32/1954. Romania.
- *Codul commercial*. N. 1233 10/05/1887 as amended by Legea 99/1999. Romania.
- *Codul de procedura civila*. N. 11/1865. Amended 2005. Romania.
- Codul de procedura penala. 12/11/1968. Amended 2003. Romania.
- *Computer misuse act*. 1990. United Kingdom.
- *Constitution of Greece*. 11/06/1975 amended 2001. Greece.
- *Criminal code*. N° 39 of 1889 in Finland Statutory Book. Amendment Act 769 of 1990. Finland.
- *Criminal code.* Adopted in 1962, entered into force on 1 January 1965. 1999. Sweden.
- *Criminal evidence act*. N° 12 of 1992. Greece.
- *Criminal procedure act*. N° 689 of 1997 Finland Statutory Book. 1 October 1997. Finland.
- *Criminal procedure code*. 1/1/1951. Greece.
- *Decreto del Presidente della Repubblica* n. 445, 28/12/2000. *In materia di documentazione amministrativa*. Italy.
- *Decreto legislativo* n. 196, 31/12/2003, *Codice in materia di protezione dei dati personali*. Italy.
- *Decreto legislativo* n. 82, 07/03/2005. *Codice dell'Amministrazione digitale*. Italy.
- *Decreto legislativo* n. 373, 15/11/2000 Attuazione della *Direttiva N. 98/84/CE sulla tutela dei servizi ad accesso condizionato e dei servizi di accesso condizionato*. Italy.
- *Decreto legislativo* n. 286. 25/07/1998 *concernenti la disciplina dell'immigrazione e norme sulla condizione dello straniero.* Italy.
- *Electronic commerce act*. N. 27 of 2000.Greece.
- *Electronic documents and signature*. Decree law 290-D/99 of 2 August 1999. Portugal.

- Freeman, L. Borgatti, S. y White, D. (1991). "Centrality in valued graphs: A measure of betweenness based on network flow" pp. 141-154 en Social Networks n. 13.
- *General Principles relating to international co-operation in the Council of Europe Convention on Cybercrime*. CETS 185 article 23.. Signature 23 november 2001. Ratified 12 may 2004. Entered into force 1 September 2004. Romania.
- *Grundgesetz* für die Bundesrepublik Deutschland vom 23.5.1949 (BGBl. I S. 1) zuletzt geändert durch Gesetz vom 28.8.2006 (BGBl. I S. 2034). Germany.
- Legea nr. 161 din 19 aprilie 2003 *privind unele masuri pentru asigurarea transparentei in exercitarea demnitatilor publice, a functiilor publice si in mediul de afaceri, prevenirea si sanctionarea coruptiei*. Romania.
- *Legea* nr. 365 din 7 iunie 2002 *privind comertul electronic*. Romania.
- *Legea* nr. 451 din 1 noiembrie 2004 *privind marca temporala*. Romania.
- *Legea* nr. 455 din 18 iulie 2001 *privind semnatura electronica*. Romania.
- *Legea* nr. 589 din 15 decembrie 2004 *privind regimul juridic al activitatii electronice notariale*. Romania.
- *Legge* n. 155 31/07/2005. *Misure urgenti contro il terrorismo*. Italy.
- *Ley 1/2000 de enjuiciamiento civil* de 7de enero de 2000. Spain.
- *Ley* 30/1992, de 26 de noviembre, de *Régimen jurídico de las administraciones públicas y del procedimiento administrativo común*. Spain.
- *Ley* 34/2002, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico*. Spain.
- Ley 59/2003, de 19 de diciembre, de *firma electrónica*. Spain.
- *Ley de enjuiciamiento penal* de 14 de septiembre 1882. Modificada en 2003. Spain.
- *Ley de procedimiento laboral*. Real Decreto Legislativo n. 2/1995.2000. Spain.
- *Ley Orgánica* 6/1985, de 1 de julio, *del Poder judicial*.2005. Spain.
- *Loi* du 14 août 2000 *relative au commerce électronique*. 2004. Luxembourg.
- *Loi* du 24 mai 1989 *sur le contrat de travail*. 2005. Luxembourg.
- *Loi* du 28 novembre 2000 *relative à la criminalité informatique*. 28 novembre 2000. Belgium.
- *Loi introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire*. 20 Octobre 2000. Belgium.
- *Loi modifiant le Code de la taxe sur la valeur ajoutée*. 5 décembre 2004. Belgium.
- *Loi relative au mandat d'arrêt européen*. 19 Décembre 2003. Belgium.
- *Loi relative aux droits des citoyens dans leurs relations avec les administrations*. Loi n°2000-321 du 12 avril 2000. France.
- *Loi transposant la directive 95/46/CE* du 24 octobre 1995 du Parlement européen et du Conseil *relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données.* 1998-12-11. Belgium.
- Mérida (2004). *Redes cognitivas y sociales: análisis de las estructuras de los textos*. www.e-libro.net.
- *Nouveau code de procédure civile*. Septembre 1998. 2005. Luxembourg.
- *Nouveau code de procédure civile*.1995. 2005. France.
- *Criminal procedure code*. DL 400/82 of 23 September 1982. Portugal.
- *Personal data protection act*. 1st September 2001. Greece.
- *Police and criminal evidence act*.1984. United Kingdom.
- *Polizeigesetz Baden-Württemberg* in der Fassung vom 13.1.1992 (GBl. S. 1, ber. S. 596, 1993 S. 155) zuletzt geändert durch Gesetz vom 1.7.2004 (GBl. S. 469) m.W.v. 1.1.2005. Germany.
- *Regolamento per l'uso della posta elettronica certificata* DPR n.68 dell'11 febbraio 2005. Italy.
- *Retsplejeloven*. N. 90/1916 - 11 April 1916. Denmark.
- Rodríguez, J. A. (2006). *Análisis estructural y de redes*. Cuadernos metodológicos nº 16. Versión actualizada. Madrid. Centro de Investigaciones científicas (CIS). Pp.86.
- *Scope of procedural provisions in Convention on Cybercrime*. CETS 185 article 14 paragraph 2. Signature 23 November 2001. Ratified 12 may 2004. Entered into force 1 July 2004. Romania.
- *Strafprozessordnung* (StPO) vom 7.4.1987 (BGBl. I S. 1074, ber. S. 1319) zuletzt geändert durch Gesetz vom 12.8.2005 (BGBl. I S. 2360). Germany.
- *Strafprozessordnung* 1975 (StPO). BGBl 1975/631as amended by BGBl I 134/2002, 1st October 002 and 2005 (BGB I, 164/2005, BRÂG 2006). Austria.
- UCINET 6 Software. Analytic Technologies. PO Box 920089, Needham, MA 02492 USA.
- Wasserman, S. y Faust, K. (1994). *Social Network Analysis: Methods and Applications*. New York: Cambridge University Press.
- *Zivilprozessordnung* in der Fassung der Bekanntmachung vom 5.12.2005 (BGBl. I S. 3202) geändert durch Gesetz vom 19.4.2006 (BGBl. I S. 866). Germany.

RÉSUMÉ

L'ADMISSIBILITÉ DES *PREUVES ÉLECTRONIQUES* DANS LES TRIBUNAUX EUROPÉENS EST RÉGLEMENTÉE PAR LES DISPOSITIONS GÉNÉRALES DE LA PREUVE TRADITIONNELLE DANS L'ENSEMBLE DES PAYS EUROPÉENS, ET AUCUNE RÉGLEMENTATION NATIONALE SPÉCIFIQUE N'A ÉTÉ MISE EN PLACE EN EUROPE.

LES PERCEPTIONS SUBJECTIVES DES ACTEURS SOCIAUX IMPLIQUÉS DANS LE PROCESSUS D'ADMISSION DE LA *PREUVE ÉLECTRONIQUE*, ET LE VIDE LÉGISLATIF EXISTANT, ONT MIS EN ÉVIDENCE QUE CE TYPE DE PREUVES EN PARTICULIER, CONTRIBUENT À ENGENDRER UN CERTAIN DEGRÉ D'INSÉCURITÉ JURIDIQUE ET PROFESSIONNELLE. PAR CONSÉQUENT, DANS LEURS PERSPECTIVES FUTURES, ILS PERÇOIVENT LES CARENCES ET DEMANDENT UNE FORMATION, UNE QUALIFICATION ET UNE RÉGLEMENTATION SPÉCIFIQUES, AFIN DE CONFÉRER DES STANDARDS ET DES GARANTIES SUFFISANTES POUR PROTÉGER LES VICTIMES DES DÉLITS COMMIS GRÂCE AUX NOUVELLES TECHNOLOGIES.

MOTS CLÉS

PREUVE ÉLECTRONIQUE, DROIT PROCESSUEL, DROIT COMPARÉ, SOCIOLOGIE DU DROIT, ADMISSIBILITÉ, RÉSEAUX JURIDIQUES, RÉSEAUX COGNITIFS ET EUROPE.

aec²

THE ADMISSIBILITY OF
ELECTRONIC EVIDENCE IN COURT
CYBEX INITIATIVE

CON LA COLABORACIÓN DE:

CONSEJO GENERAL
DEL PODER JUDICIAL

"la Caixa"

Grupo Intelligence Bureau: Pl. Cataluña, 20, 9º · 08002 Barcelona · Tel. 93 215 53 23 · Fax. 93 215 50 72
www.cybex.es