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

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

INTRODUCTION

New technology and the evolution of communications systems have substantially transformed the process of exchanging information and products in all spheres of life: business, civil and military, exponentially increasing the creation of electronic documents in organisations. Annually, over three trillion electronic mail messages are sent worldwide and more than 90% of the documents created in organisations are electronic, less than 30% of which are printed.

The massive use of digital media and the virtual environment are not exempt from conflicts or from fraudulent or criminal practices. Traditional types of fraud and crimes have been modified to use new channels of communication and incorporate new criminal categories. Delinquents and organised gangs have found a strong ally in the new technological medium for committing crimes, such as child pornography through the Internet, *phishing*, *pharming,* abuse of corporate resources and unfair competition, among many others.

With these new ways of perpetration and new types of crimes, a new tool has appeared that would make it possible to prove said fraud: *electronic evidence*. This is an instrument that, little by little, is starting to become a part of our daily life and is acquiring increasing importance in lawsuits. It can be affirmed that traditional evidence is migrating from paper supporting documents towards a virtual environment and its management processes and criteria for admissibility are changing with respect to traditional evidence.

We assume that *electronic evidence* is the proper medium to prove the perpetration of crimes committed with new technology, and we define it *as any information obtained from an electronic device or digital medium which serves to convince the truth of a deed.*

Due to the importance of this new procedural tool, we consider it fundamental to examine in depth the knowledge of the admissibility of *electronic evidence* in court as a mean of combating technological crimes. For this purpose, the objective of the project was to answer the following fundamental questions: what is *electronic evidence*? Is *electronic evidence* regulated in Europe? What problems do the European social agents involved have in collecting, analysing and presenting *electronic evidence* and how are they really working? The answers to these questions will lead us to know the truth, legislative as well as practical, of this matter. These objectives moved the Directorate General for Justice, Freedom and Security of the European Commission, within the AGIS framework programme, to approve our project due to the added value that it represents, and for the first time, we are studying at the European level a legal instrument which, more and more each day, affects European citizens. Furthermore, this investigation develops and reinforces the networking between the EU states and candidate states. It permits the exchange of information and experiences at the European level and cooperation between legal authorities, lawyers, police and private experts. It is a way of developing the European Judicial Space, fighting together against technological crimes.

It is a novel and ambitious project that has been carried out in sixteen countries: the fifteen countries of the European Union[16] and Romania, as a candidate state to the European Union. As a team of multidisciplinary European investigators (policemen, lawyers, sociologists, technicians, businessmen, academics, solicitors and Computer Forensic experts), we assumed this professional challenge and promised to develop it in one year.

In order to carry out the legal analysis of *electronic evidence* and its admissibility in courts and to know the degree of development and legislative homogeneity achieved in Europe, we began by reviewing the legislation now in force. The field of observation is formed by the regulations which in some way treat and affect any of these four elements: "evidence", "*electronic evidence*", "admissibility of evidence" and "admissibility of *electronic evidence*". The number of regulations analysed by following this criteria was seventy-eight.

In order to understand the problems confronting the social agents who intervene in a forensic analysis of electronic media and how they are dealing with it, one hundred and twenty-five in-depth interviews were held with the following profiles: lawyers, civil, criminal, commercial and labour judges, public prosecutors, notaries, representatives of the General Judiciary Council, police, Computer Forensic experts and businessmen, systematically gathering information that was transmitted to us. Finally, with all the legal and practical information obtained we drew up an improvement guide.

The investigation is a comparative study of procedural law, specifically in the provisions relative to the admissibility of *electronic evidence* in court. The objective is to find the existing gaps and identify the best practices to achieve better protection in the interest of victims of the prosecution, developing *electronic evidence* as a useful tool to combat technological crime.

Before proceeding to the presentation of the results obtained, we must comment on the limitations we identified in this investigation. This study is circumscribed by the

[16] Germany, Austria, Belgium, Denmark, Spain, Finland, France, Greece, Holland, Ireland, Italy, Luxemburg, Portugal, United Kingdom, Romania and Sweden.

particular parameters of the analysis contained in European laws which contemplate *electronic evidence*, but its social effects are not reviewed. Nor have we analysed the social impact that might have been generated by the structures of legal relations that are created through laws and their most significant elements. One of the difficulties we had to overcome refers to the plurality of European languages. We agreed to work in English since many of the laws were already translated into this language. However, many more only exist in the language of the country in which they were published. Finally, we must point out the main intrinsic difficulty of a comparative legal study being that not all of the legal figures and/or elements have the same/identical equivalence in every piece of legislation. Overcoming some of these limitations and taking into account the difficulties found, we have achieved results that have allowed us to develop a proposal for an "improvement guide" which we understand will be a reference to be considered by European professionals.

DATA AND METHODS

Comparative Procedural Law together with the Sociology of Law are the theoretical frameworks chosen in this investigation. In order to know the legal and practical reality of *electronic evidence* in Europe we have analysed the contents of the laws and the cognitive relationships that are created between the significant elements that compose these regulations. Taking into account that the cognitive organisation of the combined elements is different in every regulation and country, we have chosen distinct materials and methods of analysis.

For the analysis of legislation we have created a questionnaire to this end systemizing the collection of information coming from secondary data. *Secondary data* is made up of the legislation from sixteen European countries that regulates evidence, *electronic evidence, the admissibility of evidence or the admissibility of electronic evidence*.

For the study of reality we chose the following *primary data*:

a) Data coming from a survey presented to a sample of professionals related to the forensic analysis of electronic media and their admissibility, as an initial approximation to the notion of *electronic evidence*. This is a statistically non-representative sample. It is a prospective approximation and the people are chosen in milieus close to the use of this type of evidence. All those participating were chosen because they fulfilled the requirements in the three profiles agreed upon by the investigators. However, the field of observation is formed by the social actors involved: lawyers, prosecutors, judges (civil, criminal, commercial, labour) judiciary representatives, notaries, police, Computer Forensic experts and businessmen. The objective is the prospective approach to the basic descriptors of *electronic evidence*.

b) Data coming from *in-depth interviews:* at the very least one representative was chosen from every professional group in each of the sixteen countries studied. This is a qualitative sample that was directly selected by each investigator. The objective is to combine, in each country, a diverse and heterogeneous range of participants who can express different opinions with respect to how they are working in practice, advantages, inconveniences and future perspectives when dealing with *electronic evidence*. For this part of the field-work, we used three different protocols: one for lawyers, another for Computer Forensic experts and another for businessmen.

   The total sample of field observations is made up of one hundred twenty-five questionnaires and seventy-eight laws.

The structures are formed by the relationships that make up the legal elements contained in laws regulating *electronic*

evidence in Europe. They are created "through" and "in" written laws, which was one of the objectives in the collection of secondary data. We are looking for the universal semantics of the legal conceptualisation of *electronic evidence* by means of the association of words or terms used to define the concept and use of this evidence.

In the process of investigation we used the analysis of traditional content and structural analysis, or of semantic or cognitive networks. The latter is a new generation method that centres its attention on the interaction between the elements observed[17], whatever their level of aggregation (significant, individual, groups, or organizations) may be. Through structural relationships, legal processes and professional behaviours in Europe are explained. The relative elements are connected and put into relationships[18]. It is a methodological approach that moves away from intuitive processes. Explaining social processes and behaviours in relation to the network of relationships that connect legal elements and actors is a new theoretical approach to scientific knowledge. Cognitive networks are built from the legal elements that are shared in the laws regulating *electronic evidence*. They enable us to acquire an overall vision of the relevance European legislators and professionals confer to each element. This study develops an innovative and suggestive means of presentation and elaboration of information that may point towards aspects and dimensions of interest in the general framework of analysis of regulating *electronic evidence*. It also allows us to identify in a quick and graphic way, from a large amount of information, one or several representations of the notion that is being investigated and to compare them, or between various notions, the distinct documents to which the analysis is being applied.

A) ON ELECTRONIC EVIDENCE

The use of electronic evidence has become a necessary element to deal with in order to solve crimes committed with or through electronic devices. Consequently, we have delved into the regulation of *electronic evidence* through references found in European and Romanian legal texts with respect to evidence in general or traditional evidence, to the media of evidence, to electronic documents and the electronic signature.

Legal references result from the application of *electronic evidence* thanks to the interpretative principle of the analogical application of regulations, present in legal systems, that allow us to use legal provisions in order to regulate a specific situation or legislative gap. The principle of analogical application of these regulations acquires a very special relevancy in the analysis of legislation in Europe on *electronic evidence* material due to the fact that specific norms for this type of evidence do not exist. The findings encountered in the regulations have been corroborated by the answers obtained in practice: the majority of judges interviewed base their judgements on this interpretative concept to try to find a legal solution to the cases in which this type of evidence is presented.

Definition of *electronic evidence*

The legislative review carried out shows that neither direct and explicit references were found to *electronic evidence*, nor was a specific and exclusive definition *per se*. However, in all countries there are regulations containing precepts which, in some way, refer to *electronic evidence*.

In the case of Germany, *The Criminal Procedure Code* contains articles applicable to *electronic evidence*, specifically provisions related to data protection during an investigation. They detail the conditions for destroying data with no specific interest to the case. This text also includes precepts on the measures to follow when saving personal data obtained in investigations from police databases.

The *Criminal Procedure Code* in force in Austria includes a series of regulations, conditions and requirements that must be met in order to decide on measures of *observations of telecommunications*.

In Belgium, the *Law related to Computer Crimes* states that the regulations referring to collecting evidence under this Law are applicable to all types of evidence and therefore also to the electronic type.

[17] Rodríguez, 2005, Mérida, 2004.

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

In the case of the Dutch *Civil Procedural Legislation*, it is established that *evidence may be introduced by whatever means except where explicitly prohibited by Law.*

In Spain, the *Criminal Procedure Law* includes among the modes of evidence *the means of reproducing words, sounds and images as well as instruments permitting the filing and knowing or reproducing words, data, figures and mathematical operations carried out for accounting purposes or other ends, relevant to the trial.* Furthermore, in the enumeration of the different formats that can be considered a "document" under the *Criminal Code any format containing data* is included. Finally, in Spain, the *Labour Proceedings Law* allows the use of any type of evidence, including those *mechanical means of reproducing words, images and sounds*.

In the Finnish *Legal Proceedings Code*, when it speaks of the burden of proof it refers to this as *the deeds that support the action*, understanding by "deed" the digital as well as the traditional. Furthermore, the regulations in Finland contain a definition of electronic messages, referred to as *that information which was sent by means of electronic transmissions*.

The French *Civil Code* describes documentary evidence as the result of *a succession of letters, characters, figures or any other sign or symbol endowed with an intelligible meaning, whatever its supports and mode of transmission may be*.

In the case of Greece, the *Civil Proceedings Code* defines the objects of the evidence, establishing that they can only be *real deeds with essential influence for resolving a trial*.

In Ireland, the *Criminal Evidence Act* includes in its documentary evidence *maps, plans, graphics, drawings or photographs, or the reproduction in legible permanent form made by a computer or through other means of other types of registered information in a non-legible form (…)*.

In Italy, the *Criminal Code* has been updated in accordance with European regulations and contains a text defining the electronic document as *any computer tool that contains information with evidentiary value or any software indicated for the processing of this information.* Furthermore, this country's *Code of Electronic Government* includes the precise meaning of an electronic document, electronic authentication and other concepts such as an electronic identity document or the certification of service suppliers. Particularly, in accordance with what is established in the text, an electronic document would be the *electronic representation of acts, deeds or data with legal relevance* and, on the other hand, the electronic signature is defined as *data in electronic form united or associated in a logical manner to other electronic data used as a method of authentication*.

In Luxemburg, the *Civil Code* has been updated and contains a definition of an electronic signature interpreting it as the *set of data that are connected to a legal document in an inseparable way guaranteeing the integrity of the same*.

In the case of Portugal, the *Criminal Procedural Code* defines documentary evidence as *any type of declaration, symbol or note presented in written form or by any other technical means in accordance with the criminal laws of the country,* thus including the electronic document. The *Portuguese Civil Code* also defines documentary evidence, encompassing "mechanical or electronic reproductions of documents". Lastly, in Portugal we found a definition of electronic documents in the *Law on electronic documents and signatures* which states that it is what has been elaborated *through electronic data processing*.

A more direct reference was found in the *Police and Criminal Evidence Code* of the United Kingdom that refers to evidence as *all information contained in a computer.* Furthermore, the *Code on Computer Abuse* in this country quotes diverse definitions of technological actions, such as that the execution of a program constitutes "use" of a computer and the "log" files confirm that the program has been executed.

In the Romanian *Criminal Procedures Code* we find a definition of evidence as *any factual element used to determine, or not, the existence of a criminal offence in order to identify the actor and to ascertain the necessary circumstances for the just resolution of the trial*.

In Europe, none of the countries stipulate in their legal codes a specific definition of what *electronic evidence* is. In all of them we have found some references that are more or less specific for traditional evidence, encompassing some of those pertaining to *electronic evidence*.

Equivalence of traditional evidence to *electronic evidence*

The analysis of the contents of legislation shows that *electronic evidence* is equivalent to traditional evidence in all of the countries analysed. Furthermore, we found three types of equivalences. The first, and most common, refers to the equivalence of the electronic document to the paper support document. In some laws, the type of document is specified and it also compares the electronic receipt to the supporting paper receipt. It also compares the electronic contract with the supporting paper contract including notifications made electronically (fax) with traditional notifications.

The second type of equivalence is that referred to as the equivalence of the electronic signature with the handwritten

signature and electronic notarial deeds with traditional notarial deeds. Lastly, and as a third category, electronic mail is compared to postal mail. We highlight here the case of Portugal where electronic mail is compared to a telephone conversation.

There is a group of states[19] that expressly assimilate electronic documents with paper support documents and give them value as documentary evidence in a trial. There is also a group[20] that compares the electronic signature with the traditional signature, conferring on both the same value before a court of law.

From the point of view of legal practice, the great majority of European judges consider *electronic evidence* as equivalent to traditional evidence. Moreover, the representatives of the judiciary in Europe, in their majority, deem it to be equivalent to documentary evidence. It should be emphasized here that some dissident opinions[21] have declared it a different type of support and not a means of evidence.

The regulation of documentary evidence in Europe plays a relevant role when it comes to considering the regulation of *electronic evidence*.

Advantages and inconveniences of electronic evidence

The actors interviewed interpret the advantages and inconveniences derived from the use of *electronic evidence* in a heterogeneous way. This is the case concerning "reliability". While some judges believe that their objectivity and precision make it more reliable and therefore they favour its use, others think that the lack of means to verify its authenticity make it more vulnerable and therefore less reliable than traditional evidence, considering it an inconvenience for its use and admissibility.

Among the advantages that and technicians cited is their consideration that *electronic evidence* offers information that is exact, complete, clear, precise, true, objective and neutral, given that it comes from an electronic element, in which there is no subjectivity whatsoever, when comparing it to, for example, the declarations made by witnesses that can always be contradicted. Moreover, they believe that it gives them access to information which until now was impossible to obtain, such as everything that is contained in electronic devices.

Other informants cited as an advantage the soundness of the same, its reliability and viability due to the information it contains. On several occasions, *electronic evidence* was considered as essential to solving certain crimes, because this evidence was the only existing proof, therefore turning out to be very useful. Another advantage in which the judges coincide is the ease and rapidity in collecting and using it as well as its conservation and storage (an advantage cited by European notaries). We found great agreement among all the professionals who claim that the use of electronic documents and signatures favours the development of electronic commerce and also lowers mailing costs.

Law professionals perceive the establishment of legal value on this type of evidence as a difficulty due to the existing ignorance about data processing procedures and of the interpretation of prosecutorial law in this respect. This difficulty is generated by the lack of suitable and systematic regulation as well as the lack of homogenous jurisprudence. Furthermore, these professionals express a fear of the vulnerability and ease with which this evidence can be manipulated, given its high degree of volatility, which is one of the inconveniences when proving its authenticity. Some are of the opinion that it is very technical evidence that is not understood by judges and prosecutors and is hard to explain and out of this feeling comes the rejection of using it in court. As an inconvenience, they also cite the difficulty to preserve electronic evidence and the scant information on how to store it correctly for safekeeping.

Inconveniences cited by computer experts, in the public as well as the private sector, refer to the lack of legal support and certification models. They feel that it is harder to accept in court due to the fact that judges ask for more guarantees for it than for traditional evidence. Experts interpret the lack of understanding shown by some judicial agencies in Europe as an inconvenience for the tasks they are developing. Furthermore, these experts consider the process of obtaining and interpreting the information supplied by an electronic device in order to convert it into *electronic evidence* as time-consuming, which entails heavy costs and impedes its use.

[19] Germany, Belgium, Spain, Finland, France, Ireland, Italy, Luxemburg, Portugal and Romania.

[20] Belgium, Finland, France, Holland, Italy, Luxemburg, Portugal, Romania and Spain.

[21] Prosecutors from Portugal and Spain. Romania: is not considered a different means of evidence because there is no legislation to provide it.

The advantages that *electronic evidence* offers in Europe consist mainly of securing information that is complete, true and, up until now, impossible to obtain. The disadvantages are that they require highly specialised technical knowledge in order to present it at court, and the cost in time and money entailed in securing it.

ADVANTAGES:

INFORMATION: EXACT, COMPLETE, CLEAR, PRECISE, TRUE, OBJECTIVE, NOVEL AND NEUTRAL.

PROOF: SOLID, USEFUL, RELIABLE, VIABLE, ESSENTIAL TO PROVE CERTAIN CRIMES THAT PREVIOUSLY COULDN'T BE PROVEN.

EASY: COLLECTION, USE, SAFEKEEPING AND STORAGE.

ELECTRONIC DOCUMENTS, TOGETHER WITH ELECTRONIC SIGNATURES, FACILITATE ELECTRONIC COMMERCE MAKING IT FASTER AND MORE SECURE.

INCONVENIENCES:

- SCANT/LACK OF SUITABLE AND SYSTEMATIC REGULATION.
- SCANT JURISPRUDENCE.
- UNKNOWN AND VERY TECHNICAL MATERIAL. FEW EXPERTS.
- DEMANDS SPECIFIC KNOWLEDGE.
- DIFFICULT TO PRESENT AT COURT IN AN UNDERSTANDABLE MANNER.
- HARDER TO BE ACCEPTED AT COURT: JUDGES ASK FOR MORE GUARANTEES THAN WITH OTHER EVIDENCE.
- LACK OF TECHNICAL INFRASTRUCTURE IN JUDICIAL DEPARTMENTS.
- HIGH COST OF EXAMINING AND INTERPRETING THE INFORMATION.
- HARD TO KNOW HOW TO PROCESS THE DATA AND HOW TO INTERPRET SPECIFIC PROCESSING LAWS.
- DIFFICULT TO PROVE AUTHENTICITY, RELIABILITY AND ORIGIN OF DATA.
- VOLATILITY OF DATA AND EASE OF MANIPULATION.
- HARD TO IDENTIFY PERPETRATOR OF THE CRIME.
- DIFFICULT TO CONSERVE, PRESERVE AND STORE.
- HARD TO ESTABLISH LEGAL VALUE OF EVIDENCE.
- LACK OF LEGAL SUPPORT AND CERTIFICATION MODELS.

B) ON LAWS AND JURISPRUDENCE

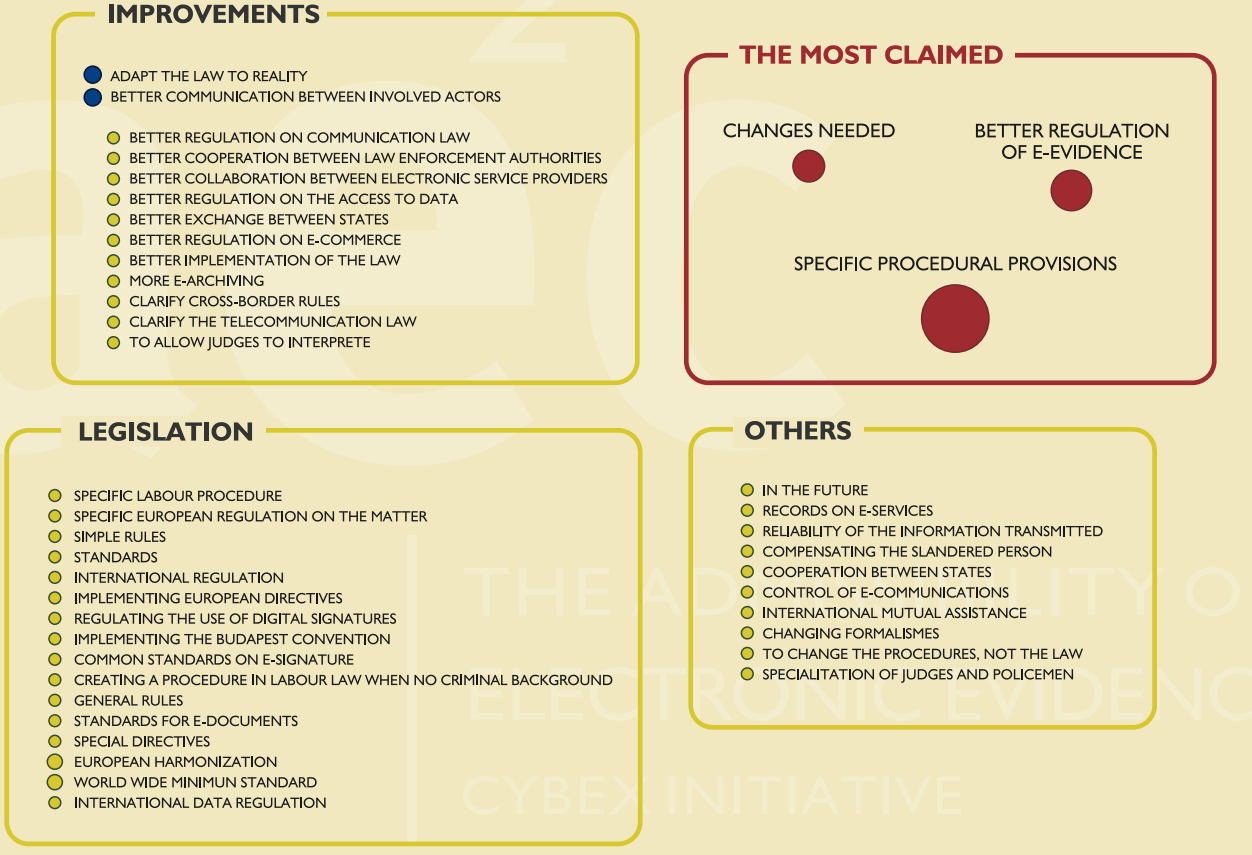
The legal framework regulating *electronic evidence* in Europe is fundamentally composed of a series of procedural regulations, civil, criminal and commercial law texts, provisions on electronic commerce or on electronic signatures, among which we have not been able to find any specific regulations on *electronic evidence*.

The analogical interpretation of the provisions contained in these texts for traditional evidence also regulates *electronic evidence* in Europe.

The regulation of *electronic evidence* was found mainly in the following jurisdictions: the regulation of civil law and the regulation of criminal law followed by the regulation of evidence in labour law and in the regulations that are similarly made on other legal matters[22].

The subjective perspectives from jurists on the regulation of *electronic evidence* (Graph 1) are heterogeneous and also present multiple contradictions. The main tendency in *electronics* is actually found to be well-regulated. However, judges, who are the ones that have to interpret the law because of a legal gap, are divided in their opinions

GRAPH 1: CHANGES PREFERRED BY JURISTS



Our own source of data and elaboration.

[22] Administrative and business regulations, legal organisation laws and Constitutional rules.

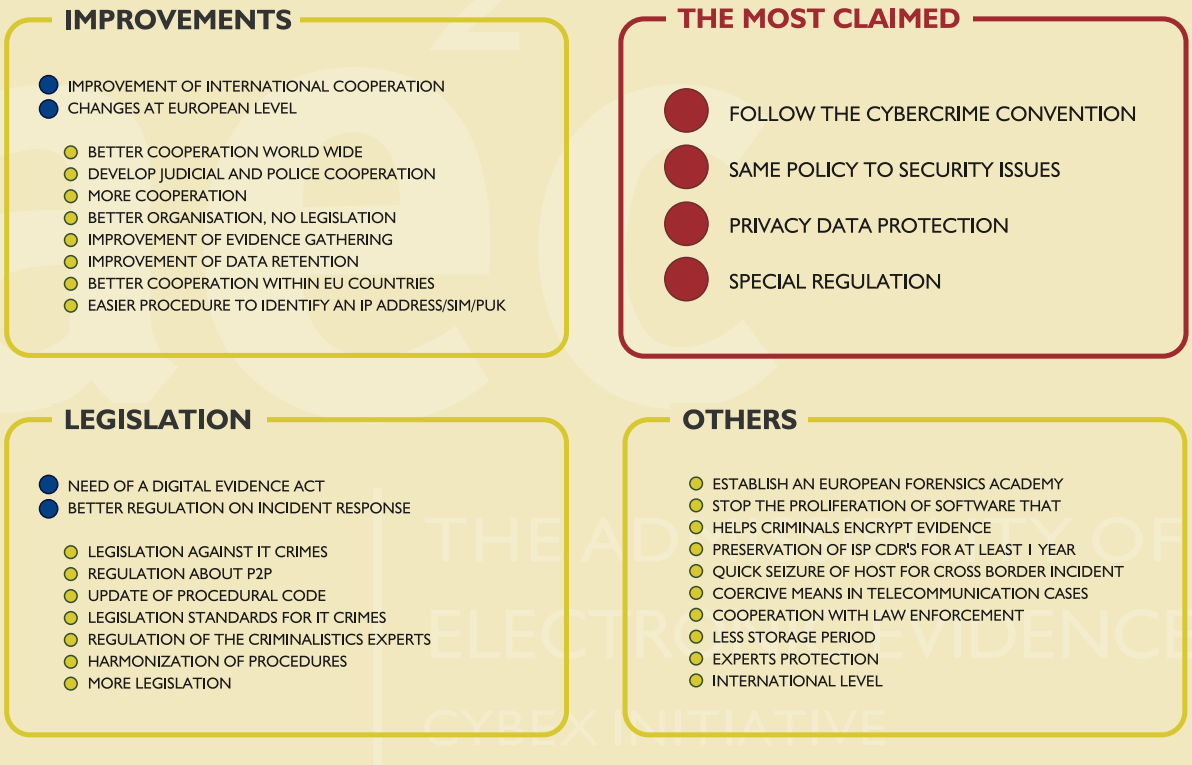
according to their speciality, but the majority opinion favours those whose tend to think that the current legal situation is not the ideal one and needs changes to adapt the laws to technological reality.

Those who favour introducing changes in the current legal situation mainly lean towards changes that would add specific regulations for the distinct dimensions of *electronic evidence* and precepts for specific procedures at a national level. On the other hand, at the European level, jurists prefer harmonization (of the matter) but note that it must be done through general rules that permit each country its own implementation according to its legal tradition. Finally, there are those who think that, at an international level, there should be a rule of minimums.

The subjective perception held by experts in forensic computer science on the legal situation (Graph 2) is quite balanced. However, the majority of these experts think[23] that the situation can be improved. The most significant changes they would introduce consist of establishing a policy of common security, following the regulations of the Cybercrime Convention of the Council of Europe, establishing specific regulations for *electronic evidence* and improving protection of personal data.

Interpretations by legal experts and Computer Forensic experts on the current situation of the admissibility of

GRAPH 2: CHANGES PREFERRED BY COMPUTER FORENSIC EXPERTS



Our own source of data and elaboration.

[23] Experts from Austria, Germany, Ireland, UK and France consider the legal situation to be adequate. The situation can be approved according to the experts from Belgium, Greece, Spain, Denmark, Portugal and Romania. In Italy and Holland opinions are contradictory within the same country. The expert from Luxemburg states no opinion.

electronic evidence in court coincide in that there is a need to develop specific precepts that contribute to legal security. They also share the need to develop some European rules that guarantee a minimum homogeneity in the treatment of *electronic evidence* as well as establishing international regulations that would help to improve international cooperation.

Advisability of a European framework regulating *electronic evidence*

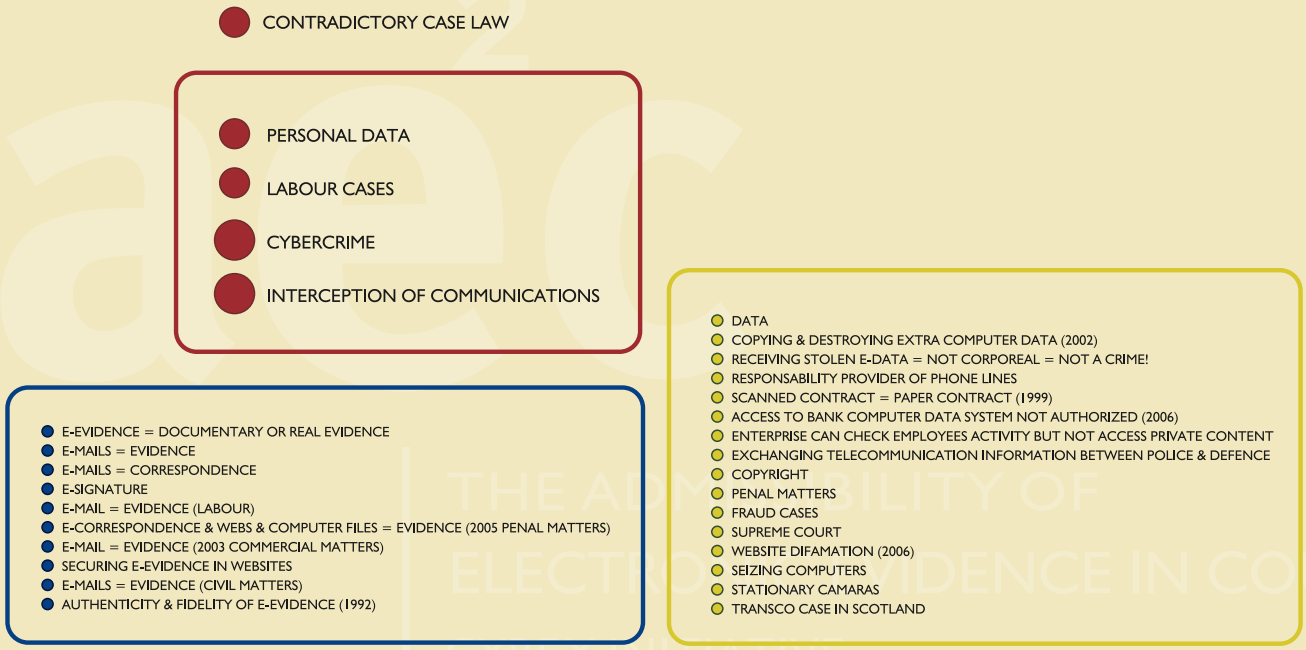
The great majority of European lawyers consider the possibility of having some type of regulation for the different dimensions of *electronic evidence* from Europe advisable. The arguments are varied. We found divided opinions, such as that the European framework is necessary due to the trans-national dimension of the crimes the *electronic evidence* is trying to prove, as well as facilitating international cooperation. It would also facilitate more uniformity in the development of *electronic evidence*, citing as examples of necessary actions the harmonisation of data protection and procedures for collecting *electronic evidence*. Another, less numerous, group of jurists feels that regulations on *electronic evidence* should continue to be exclusive in each state. The representatives from Austria, Denmark and Finland feel that national regulations are sufficient since they cover all aspects of evidence, including the electronic type. On the other hand, we must point out the opinions of the Greek jurists, who feel that without common European regulations, the adaptation of the current legislation to technological reality will not be possible in their country.

A regulatory European framework that controls *electronic evidence* is seen as a positive element for the legislative evolution of the matter.

Existing jurisprudence

The cases of the most relevant current jurisprudence refer to cybercrime, interception of communications, cases of labour law and the infringement of data protection (Graph 3).

GRAPH 3: MOST FREQUENT CASES CONCERNING *ELECTRONIC EVIDENCE*



Our own source of data and elaboration.

Some jurists emphasized the existence of cases with contradictory rulings that reveal a lack of homogeneity in the criteria for admitting *electronic evidence*. In very similar cases, in some cases *electronic evidence* was admitted and in others it was rejected.

Computer Forensic experts in the public sector work mainly on cases of cybercrime, cyberterrorism, child pornography and economic crimes committed through electronic means. Experts in the private sector work ever more frequently on cases of abuse of corporate means, investigation of technological devices (GSM and SIM *forensics*, GPS data recuperation), security incidents, economic crimes and intellectual property. Businessmen confront problems in the labour environment usually referred to as cases of incorrect use and abuse of corporate electronic resources as well as data and computer security problems. Furthermore, they list bank fraud and crimes of intellectual property as well as those derived from electronic commerce. However, the majority of these businessmen do not have a protocol that controls the use of computer material at the disposal of their workers. Nor do they have access to an infrastructure that advises them on how to protect themselves from this type of crime.

C) ON THE PROCEDURE FOR OBTAINING, CONSERVING AND PRESENTING ELECTRONIC EVIDENCE BEFORE THE COURT AND ITS ADMISSIBILITY

Procedural standards do not include any specific procedure that regulates collection, conservation or presentation of *electronic evidence* in court. Generally speaking, countries apply by "analogy" the regulations in the general procedures for traditional evidence.

Almost half of the rules analysed (48%) contemplate procedural processes that can be analogically applied to *electronic evidence*. The most similar rules to those that could be a procedure for *electronic evidence* were found in the United Kingdom and Belgium. The *Police and Criminal Evidence Code*[24] in force in the United Kingdom regulates in a specific way the collection of "computer evidence", and in the Belgian *Law on Computer Crimes* precepts are included on gathering evidence that are applicable to *electronic evidence*.

Other procedures that can be used by analogy for *electronic evidence* are those contemplated in European trial laws developed for the interception of communications or telecommunications and of the trial rules to follow when the possibility exists of infringing the fundamental rights of the person.

The perception by jurists of the existence, or lack, of a procedure is biased due to how the concept of "procedure" is interpreted. Some feel that the analogical application makes it so the procedural standards for traditional evidence are applied to *electronic evidence* and therefore, in their opinion, there is only one procedure for all evidence. Others have interpreted the concept of "procedure" in a more restricted manner and think that a specific procedure for *electronic evidence* does not exist or that there are only precepts that regulate some aspects of securing, conservation and presentation of this type of evidence. For example, this is the case for the procedure to follow in criminal material for monitoring and intercepting communications, consisting of the demand for a court order. A court order is also necessary to carry out an investigation or to collect evidence or *electronic evidence* the possibility of a violation of fundamental rights exists.

Notaries are unanimous in their opinion that there is no specific procedure for safekeeping *electronic evidence* and the procedures to which they refer are those for the creation of electronic signatures. In Italy, notaries may use informal procedures to file electronic documents, compliance to which is not obligatory.

[24] Police and Criminal Evidence Act, PACE.

The police and private experts in forensic computer science do not have a specific procedure for obtaining, conserving or presenting *electronic evidence* in court, except in Austria and Romania. In these countries there is a procedure for collecting it[25]. In the United Kingdom[26] and Romania[27] they follow the internal police procedure rules. In Luxemburg, the police are working on an internal procedure to obtain and analyse *electronic evidence*. In Finland, they are drawing up a strategy for the criminal investigation of IT that can be made into a procedural manual.

From the point of view of legal practice, jurists agree that in Europe there are general standards of procedure that regulate the securing of evidence in criminal and commercial material in some cases (Finland), that can be extended to *electronic evidence* by analogy, but not in the rest of the jurisdictions. They also refer to the fact that there is no procedure established for the conservation or preservation of *electronic evidence* and that the preservation of the same, in court, will be done in each country as a result of the analogical interpretation of the precepts established for traditional evidence, that is, as documentary evidence and as testimonial evidence in the majority of cases.

In the system of legal standards now in force in Europe there are no specific procedures regulating the collection of *electronic evidence* except the legislative precepts of two countries, the United Kingdom and Belgium, which refer to obtaining computer evidence. We did not find any procedures for the preservation and presentation of *electronic evidence* in court in any of the European countries.

D) ON THE ADMISSIBILITY OF *ELECTRONIC EVIDENCE*

Competent authority for the admissibility of *electronic evidence*, motives for its exclusion and custody of the same.

The figure of the judge or the court has been revealed as the maximum competent authority to decide on the admissibility of any *electronic evidence* in Europe, following the results of the analysis of legislation and the questions formulated by lawyers. In some countries, such as Greece and Luxemburg, in addition to mentioning judges, we found particular references to the figure of the public prosecutor as a competent authority.

Admissibility is very much related to the possibility, or not, of excluding *electronic evidence* without prior motive. We can affirm that none of the standards analysed allow, nor anyone interviewed accepts, the possibility of excluding *electronic evidence* without due motive on the part of a judicial body. However, Danish commercial judges point out that motivation in some cases for excluding evidence and *electronic evidence* can be done in a very brief manner and verbally during the hearing.

During the investigation it is the police and the prosecutors who are responsible for guarding *electronic evidence* in criminal proceedings. During the trial stage, it is the judicial body that is in charge of guarding this evidence (specifically, the figure of the judicial secretary in most countries). In civil matters, it is mainly the parties who keep the evidence that will be presented before the judge or in court when the latter so requires, both in the pre-trial phase and during the same. In some countries, notaries and experts are the ones in charge of safekeeping *electronic evidence* and getting it to court, as the case may be.

Requirements that *electronic evidence* must fulfil to be admitted in court

In Europe, in accordance with legal texts, two models of countries exist with respect to the requirements that must be met for evidence to be admitted in a trial. One group of countries has in common that their legal tradition establishes some very broad criteria for admitting evidence. They base it on the free consideration of the judge at the time of admitting *electronic evidence* or not (Austria, Denmark, Sweden, Finland). The other group of countries coincide in

[25] In Romania, the "G8 Proposed Principles for the Procedures Relating to Digital Evidence" is not compulsory or recommended.

[26] Association of Chief Police Officers.

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

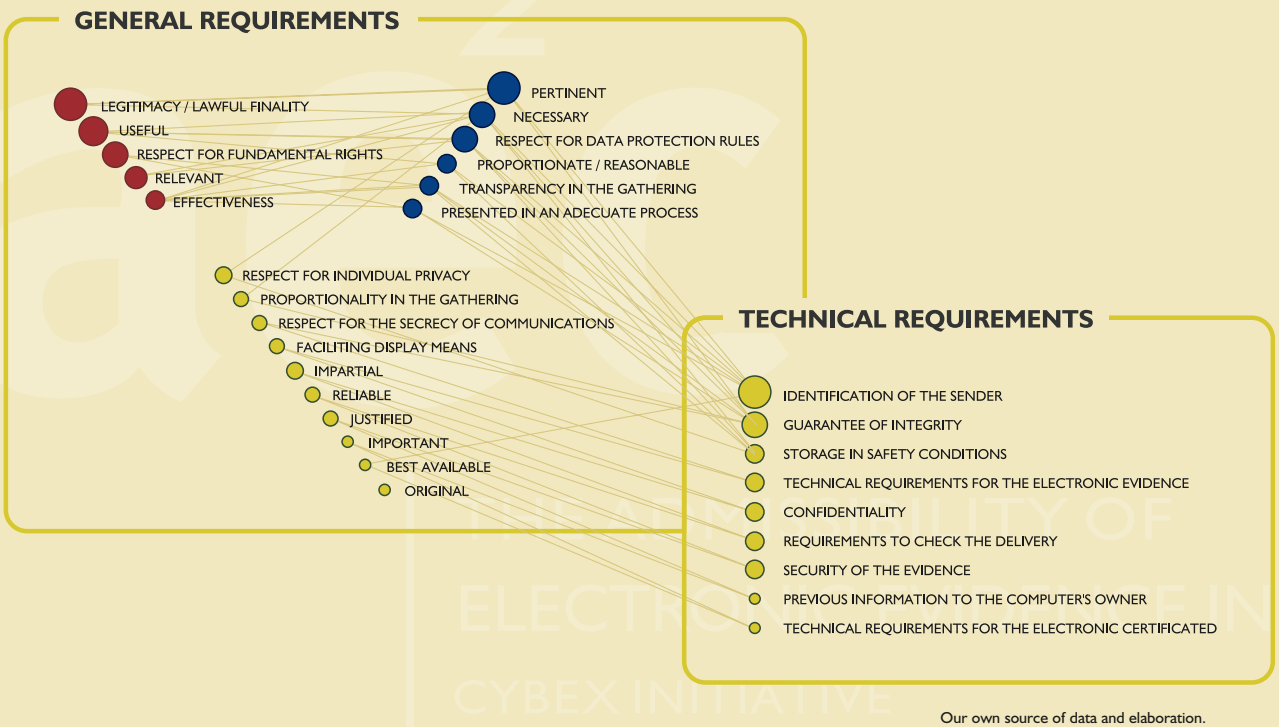
that their legislation regulates in a more restrictive manner the admissibility of evidence in accordance with a series of requirements for the evidence or the means of evidence established by law.

The legality of evidence[28] is the requirement most frequently cited in the laws (Graph 4). In some countries, such as Germany, Ireland and the United Kingdom, they do not apply the doctrine of the fruit of the poisoned tree[29], which is why the requirement for legality is not always applied.

Another requirement considered in the laws is respect for fundamental rights[30], among which one can frequently find references to respect for the norms of protecting personal data and workers' rights. The reliability of the evidence, together with its pertinence and that it be the best available at a certain moment in time are other fundamental requirements that the judge will examine in order to decide on the admissibility of particular evidence.

Other requirements gathered from the legislation that will mark the admissibility or not of *electronic evidence* are the use, proportionality and effectiveness of the same. Effectiveness is understood as the capacity to prove the allegation.

GRAPH 4: LEGAL REQUIREMENTS FOR ELECTRONIC EVIDENCE TO BE ADMITTED AT TRIAL



Our own source of data and elaboration.

[28] Italian Civil Code. Criminal procedure Laws of Germany, Belgium, Ireland, Portugal, Romania. Civil Procedure Laws in France, Greece, Holland, Spain and Luxembourg among others.

[29] This doctrine establishes the illicit character of evidence obtained by a procedure that is shown to be marred, making them contaminated by the illegality of the procedure.

[30] Danish Procedure Law. Civil Procedure Law in Luxembourg, Spain. Criminal Procedure laws in Germany, Portugal among others.

Finally, they comment that the laws establish as a requirement that the evidence be original whenever possible and not a copy. As well as being original, the evidence must be direct and not hearsay or indirect. These are rules of exclusion that govern the admissibility of *electronic evidence* in the United Kingdom and Ireland.

Although the aforementioned requirements appear in legal texts, in judicial practice they are not always complied with everywhere. We wanted to know which requirements are the ones not fulfilled most frequently in the European legal field. The subjective opinion of jurists shows that it is respect for fundamental rights, especially those pertaining to the right of data protection and the rights of workers that are breached most frequently at the time of presenting *electronic evidence* in court. This makes it so that evidence is often rejected. The formal technical requirements that are most usually breached in Europe are those pertaining to the compliance of measures necessary for checking the authenticity and inalterability of the electronic document, the electronic mail sent as well as the lack of electronic signature on documents that end up without evidential strength at the time they are presented at court. Furthermore, on many occasions, the chain of custody is violated generating legal insecurity in the *electronic evidence* presented.

Influence of respect for guarantees of legality

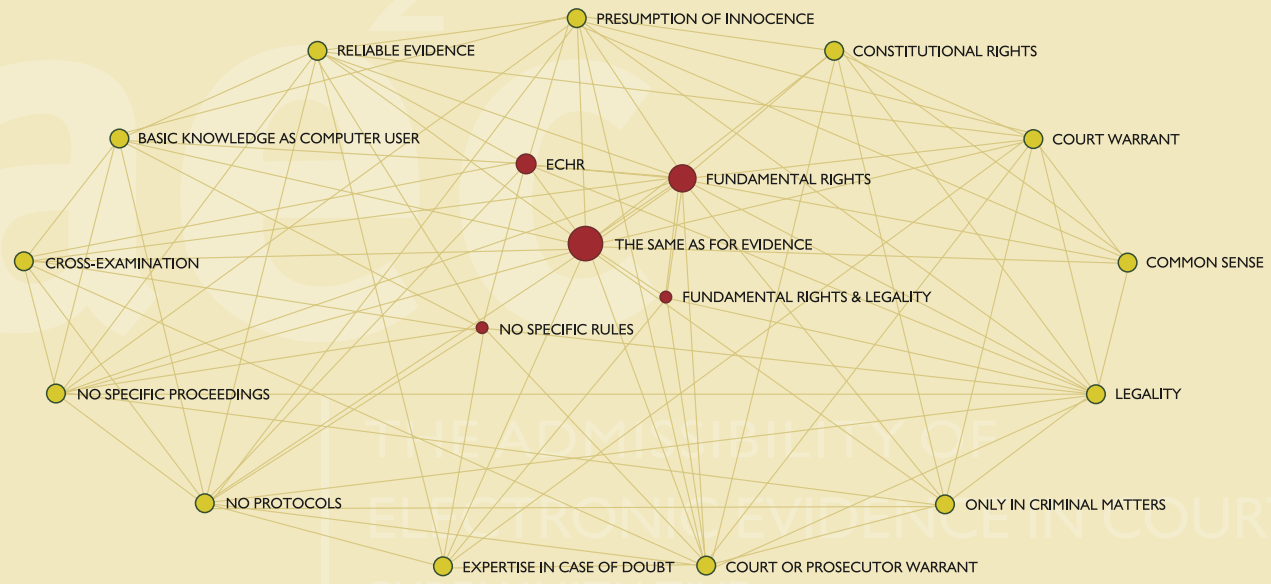
a) On the admissibility of *electronic evidence*

Respect for guarantees of legality is one of the requirements demanded in most legislation. In practice, magistrates as a body coincide in that respecting these guarantees of legality positively influences the admissibility of *electronic evidence*. Other justice professionals indicate that what is relevant is that it be a fair trial or getting the material truth (Denmark and Finland). In Denmark they also point out that said guarantees will only have influence if one of the parties objects to the respect for the guarantees of legality.

b) On the process of gathering, analysing and presenting *electronic evidence* at trial

With respect to the guarantees of legality that must be taken into account in the process of gathering, analysing and presenting *electronic evidence* at trial, a good part of the opinions voiced by European jurists points to the lack of specific relative standards (Graph 5), which is why they are in favour of the same type of measures that must be respected

GRAPH 5: PERCEPTION OF GUARANTEES OF LEGALITY THAT LAWYERS CONSIDER MUST BE RESPECTED



Our own source of data and elaboration.

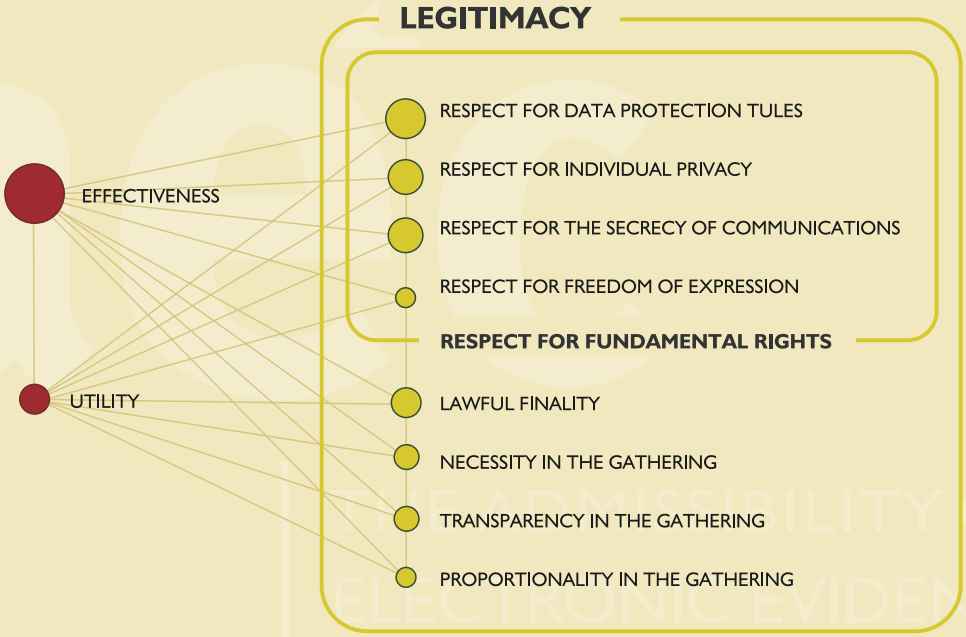
for any other type of evidence. The positive statements insist on respecting fundamental rights and on the jurisprudence originating from the European Court of Human Rights as well as respect for legality.

Principles that affect the admissibility of *electronic evidence*

The principles related to the effectiveness, usefulness and legitimacy of *electronic evidence* play a relevant role in the different European legislations. The need for obtaining the evidence, transparency while gathering it and respect for freedom of expression are principles reflected in the standards but occupy a secondary position as far as admissibility of the evidence is concerned. The principles that affect *electronic evidence* in a specific way, thus having more relevance, are the respect for data protection standards, the respect for the secrecy of communications and the respect for the right to freedom of expression (Graph 6).

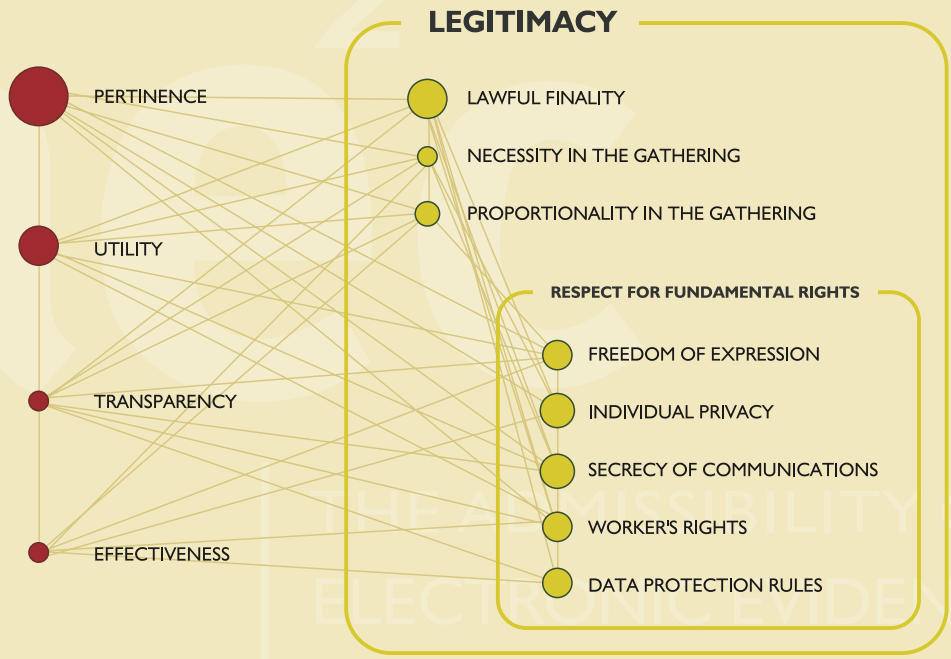
In practice, European jurists think that the principles of legitimacy, (emphasizing the privileged position as an integral part of this principle of respect for fundamental rights) the pertinence of the evidence and the use of the same have greater influence. Technical experts on forensic computer science stress the fact that they act accounting for respect toward individual rights. Moreover, they also cite respect for data protection standards (Germany and Greece), preservation of confidentiality (France, Luxemburg and Ireland), and developing their functions through encrypted material as basic principles (Italy and the United Kingdom). Furthermore, they point out that they count on the legal support of a notary (Spain) as well as the presence of witnesses (Spain, Romania) (Graph 7).

GRAPH 6: LEGAL PRINCIPLES FOUND IN LEGISLATION THAT CONDITION THE ADMITTANCE OF EVIDENCE



Our own source of data and elaboration.

GRAPH 7: JURISTS' PERCEPTIONS OF PRINCIPLES AFFECTING THE ADMISSIBILITY OF *ELECTRONIC EVIDENCE*



Our own source of data and elaboration.

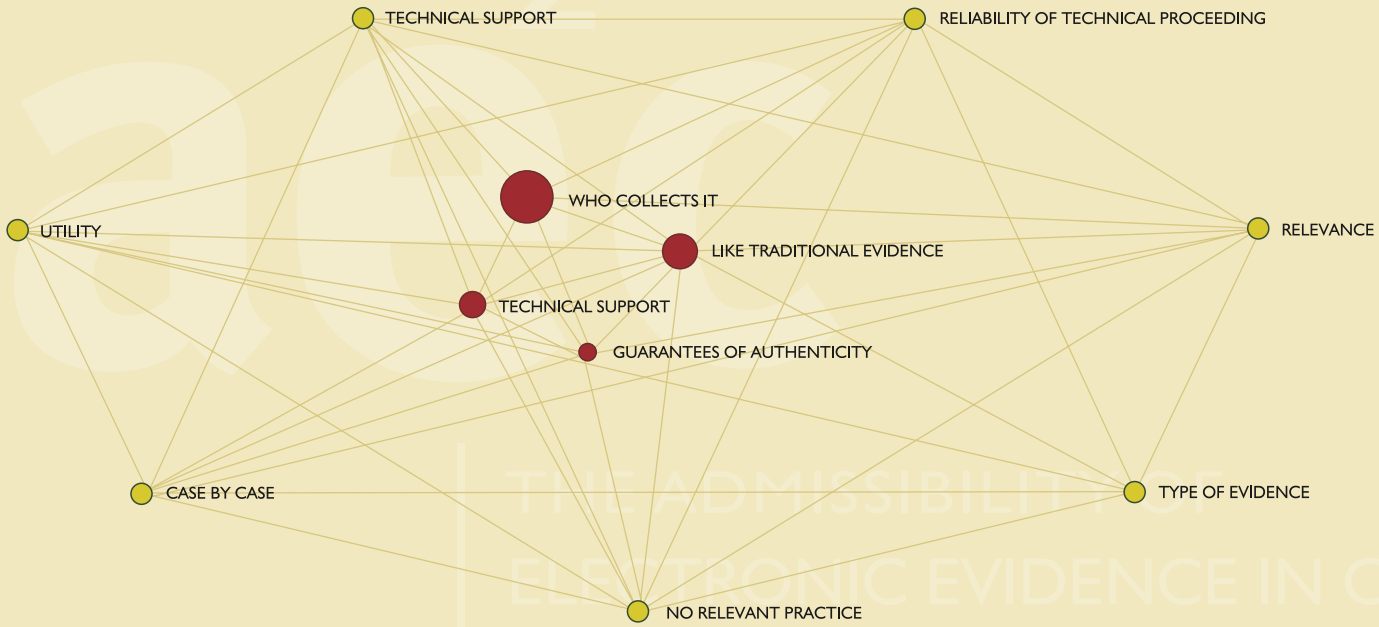
Factors that influence the evidentiary value of *electronic evidence*

Respect for legality in gathering evidence plays a fundamental role when it comes to evaluating the admissibility of the same. This is why we wanted to know who is responsible for gathering traditional and electronic evidence in accordance to the law. On the other hand, the judicial body, in the form of a judge or the court, and the prosecutor, in collaboration with the police, play a fundamental role in gathering evidence in Europe. However, legislation bestows on these parties the responsibility of gathering evidence in civil matters. Experts are also named as agents in gathering *electronic evidence* both in civil matters as well as criminal matters.

This last affirmation is very significant knowing that, concurring with jurists' opinions, the person in charge of gathering *electronic evidence* is the factor that influences most the evidential value attributed to it. This indicates that the fact that it is the police who are in charge of gathering *electronic evidence*, and with support from the judicial body, it is valued in a relevant manner when admitting it as evidence or not. Technical support on one hand, and guarantees of authenticity on the other, complete the list of factors that influence European courts the most when conceding greater or lesser evidential value to specific evidence. Another group of magistrates does not think that a relevant factor exists but rather that it is the same as must be taken into account for traditional evidence.

These affirmations show a degree of interest and concern for the authenticity and integrity of this type of evidence shared by the European judicial body.

GRAPH 8: JURISTS' PERCEPTION OF FACTORS THAT GIVE MORE EVIDENTIAL VALUE TO *ELECTRONIC EVIDENCE*



Our own source of data and elaboration.

E) ON EXPERTS IN FORENSIC COMPUTER SCIENCE

Training and requirements necessary to work as an expert in forensic computer science in Europe

In Europe, there is an absence of standards determining the characteristics that an expert in forensic computer science must satisfy. Lacking legal precepts, what is valued most, both by lawyers and technicians, is specific experience.

Basic training, considered by experts to be necessary to consider themselves as experts in Computer Forensics, should be a degree at the very least, and preferably a degree in computer science, engineering or mathematics. Furthermore, it is considered essential to have continued and specialised training as the only means of staying up to date. We also know that specialised police receive internal training from public, national and international organisations and from private companies. However, we haven't found any regulated university training in forensic analysis of digital media, although there are postgraduate training courses in forensic computer science (France) and in Cybercrime Investigation (Ireland). In Europe, private Computer Forensic experts coexist with those of State security forces. Only in Romania, to be an expert, you have to be authorized or certified by the State.

The vast majority of law professionals think that laws do not specify special requirements to act as a Computer Forensic expert in court. They declare that a fundamental formal requirement is to be registered in the list of experts kept by courts in Europe. Fewer of them think that one requirement to fulfil is to be a "computer expert".

Perceptions on Computer Forensic experts by European jurists and experts consulted

European lawyers mainly identify police or prosecutors as those who should be experts in Computer Forensics. Furthermore, they believe that these professionals should have certification in forensic analysis issued by the private sector. But the opinion of experts is divided. Experts prefer, considering the absence of a specific degree, that they have at least five years of professional experience. The professions that are considered to be the most adequate for experts are lawyers and police.

IMPROVEMENT GUIDE

The sources that inspire this improvement guide are based on subjective perceptions and views by professionals: jurists, technicians and businessmen in Europe.

- With respect to the **regulation** of *electronic evidence*, **lawyers** think that at a national level, there is a need to effect changes in the current legislative body that would help diminish the degree of legislative insecurity. They advocate better national regulation of *electronic evidence*, specifically in procedures that would permit the collection, preservation and presentation of this evidence complying with all the specific/proper legal guarantees so they can be admitted at trial as a regular type of evidence. At the european and international level, they express the need for developing a series of minimum directives in procedural matters that would assure proper cooperation between states concerning its collection and preservation. International cooperation is essential to achieve greater effectiveness in the individual each country's fight against crimes committed through/by digital means which, due to their nature, are trans-national on many occasions

  The changes that **experts in Computer Forensics**, both in the public and private sectors, feel should be carried out are, first of all, that *electronic evidence* be provided with specific regulations at the national level. Others recommend its regulation through the implementation of protocols developing the protection of fundamental rights in the collection, preservation and presentation phases of *electronic evidence*, thus being able to improve compliance with the guarantees of admissibility for this type of evidence. Agreeing with the lawyers, they feel it is necessary to effect changes at the european level, stating minimum standards of performance. Specifically, they consider it of great importance for countries to comply with the Budapest Convention of Cybercrime of the Council of Europe. They also believe it would be fitting to act at an international level to achieve improvement in the cooperation between states in matters of collection and preservation.

ON THE REGULATION OF *ELECTRONIC EVIDENCE:*

- SPECIFIC REGULATION BOTH AT THE NATIONAL AS WELL AS EUROPEAN LEVEL THAT WOULD PROVIDE LEGAL SECURITY.
- EUROPEAN RULES THAT GUARANTEE THE HOMOGENEITY IN THE TREATMENT OF THIS TYPE OF EVIDENCE.
- INTERNATIONAL STANDARDS THAT CONTRIBUTE TO IMPROVING INTERNATIONAL COOPERATION.

- With respect to **professional practice in Computer Forensics,** both **jurists and experts** agree that for exercising the profession, experience is the relevant characteristic on which great value is conferred, both in the present as well as looking to the future. Both are of the opinion that the profile a Computer Forensic professional must fulfil is to have a degree in computer science, engineering or mathematics. Furthermore, experts feel it necessary to have a certificate of forensic analysis in digital media issued by a public authority and to have at least two years experience with a university degree. For those who do not have university training, they feel that, as a minimum, they should have five years specific experience and they stress the need for ongoing training. For their part, jurists feel that a professional should be a member of the police and have a private certificate of forensic analysis of digital media.

- **Businessmen and professional organizations** in Europe mainly allude to three major issues: prevention, training and legislation. Referring to prevention, they defend the need to create standard computer protocols to be used by businessmen in labour relations. As for training, they feel it wise to put advisory initiatives into effect, measures that would let them know how to proceed in gathering and storing *electronic evidence* so as not to decrease its evidential value in court. Furthermore, they advocate the use of interchange of good practices between countries. With respect to legislation, they express the need for reform and clarification of existing legislation in matters of *electronic evidence*. Specifically, they propose increasing the security of electronic communications, effectively implementing electronic signatures and reducing the time for storing documents. Others, from some European countries in particular, where the principle of free admissibility of *electronic evidence* reigns, insist that the legal situation and jurisprudence is adequate and there is no need to modify the legislation.

ACTIONS OF CHANGE SUGGESTED BY EUROPEAN BUSINESSMEN:

- PREVENTION: COMPUTER PROTOCOLS.
- TRAINING: ADVICE ON GATHERING AND STORING PROCEDURES.
- LEGISLATION: REFORM AND CLARIFICATION OF EXISTING RULES.

- Some consider that the future of *electronic evidence* requires specific regulation at both national and European levels that assures the progressive development of the material, adapting legislation in an adequate manner to new existing social realities. Others expect that in regulating *electronic evidence* the principle of freedom of evidence should prevail and that it will evolve toward non-regulation. That is to say, they feel that the current situation of admissibility is adequate and there is no need to change it in the future.

Another change that jurists feel should be implemented is an improvement in communication between the actors involved in the admissibility of *electronic evidence*, among whom are those responsible for the collection, preservation and presentation of the same at trial, and the judges in charge of deciding on its admissibility. Technicians on the other hand, emphasize the importance of applying changes in protecting the privacy of personal data and applying homogenous policies in matters of security.

VIEWS OF THE FUTURE:

- CONTRADICTORY ON SPECIFIC REGULATIONS.
- IMPROVEMENT IN COMMUNICATION.
- INCREASE IN PROTECTING PRIVACY OF PERSONAL DATA.

KEY POINTS FOR IMPROVING REGULATION AND PRACTICE:

- JUDGES ARE THE KEY ACTORS IN ADMITTING ELECTRONIC EVIDENCE AND POLICE EXPERTS HOLD THE MAIN POSITION IN GATHERING EVIDENCE. *LET US ACT ON THESE TWO TYPES OF ACTORS.*
- LEGISLATION HAS THE EFFECT OF POSITIVELY INFLUENCING THE PERCEPTIONS OF SECURITY HELD BY DIFFERENT SOCIAL AGENTS. *LET US ADAPT EXISTING LEGISLATION.*
- CONFIDENCE IN THE EXPERTS RELATED TO THE COLLECTION, ANALYSIS AND CONSERVATION OF ELECTRONIC EVIDENCE. *LET US FOLLOW THE TECHNICAL PROCEDURES OF THE EXPERTS.*
- TRAINING, KNOWLEDGE AND EXPERIENCE ARE THE NECESSARY AND INDISPENSABLE ELEMENTS THAT EXPERTS MUST SATISFY. *LET US WORK ON THE TRAINING.*
- IMPROVEMENT IN COMMUNICATION BETWEEN THE ACTORS RELATED TO ELECTRONIC EVIDENCE, AT THE NATIONAL, EUROPEAN AND INTERNATIONAL LEVEL, IS A UNANIMOUSLY PRIZED AND DESIRED ASSET. *LET US IMPROVE UNDERSTANDING BETWEEN JUDGES AND TECHNICIANS.*

REFERENCES

- *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.

SUMMARY

THE ADMISSIBILITY OF *ELECTRONIC EVIDENCE* IN EUROPEAN COURTS IS REGULATED BY THE GENERAL PROVISIONS ON TRADITIONAL EVIDENCE THROUGHOUT EUROPEAN COUNTRIES. AS OF THIS TIME, NO SPECIFIC NATIONAL REGULATIONS HAVE BEEN DEVELOPED IN EUROPE.

THE SUBJECTIVE PERCEPTIONS EXPRESSED BY THE SOCIAL ACTORS INVOLVED IN THE PROCESS OF ADMITTING *ELECTRONIC EVIDENCE,* ALONG WITH THE EXISTING LEGAL VOID, PROVE THAT THIS TYPE OF EVIDENCE IN PARTICULAR CONTRIBUTES TO GENERATING A CERTAIN AMOUNT OF LEGAL AND PROFESSIONAL INSECURITY. CONSEQUENTLY, IN THEIR PERSPECTIVES FOR THE FUTURE, THEY PERCEIVE FAILINGS AND DEMAND SPECIFIC TRAINING, QUALIFICATION AND REGULATIONS TO PROVIDE SUFFICIENT STANDARDS AND GUARANTEES TO PROTECT VICTIMS OF CRIMES COMMITTED BY MEANS OF NEW TECHNOLOGIES.

KEY WORDS

ELECTRONIC EVIDENCE, PROCEDURAL LAW, COMPARATIVE LAW, LEGAL SOCIOLOGY, ADMISSIBILITY, JUDICIAL NETWORKS, COGNITIVE NETWORKS AND 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