


THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COURT
Council of Europe & Ministry of Justice Bulgaria
18 December 2007 – Plovdiv, Bulgaria



- **Fredesvinda Insa**
Projects Manager
finsa@cybex.es

- **Carmen Lázaro**
Projects Coordinator
clazaro@cybex.es

| 2



Agenda →

- Introduction
- Definition of Electronic Evidence in Europe
- Legislation and Case Law
- Proceedings and the Admissibility of electronic evidence in Court
- Computer Forensics Experts
- Improvement Guide
- Question time

| 3



INTRODUCTION




| 4

- New technologies have increased exponentially the creation of electronic documents in the organizations
- More than 3 trillion of emails are sent in the world every year
- More than 90% of the documents in an organization are electronic
- Less than 30% are finally printed
- The use of the digital means and the virtual environment is not exempt from dishonest use
- Kinds of crime committed through new technologies and in virtual environments:
 - Unfair competition
 - Abuse of corporate means
 - Menaces
 - Child pornography
 - Phishing
 - Pharming
 - E-bullying

- Traditional evidence is moving from paper support to a virtual environment
- In the context of electronic evidence, management procedures and admissibility criteria are changing with regard to traditional evidence
- *Electronic Evidence* is gaining more and more relevance in legal procedures
- *Electronic Evidence* is the best mean to prove that certain types of crime have been committed through the new technologies. It could be defined as:

ANY KIND OF INFORMATION OBTAINED FROM A DEVICE OR DIGITAL MEANS THAT AIMS FOR HAVING CONVICTION ON THE TRUTH OF A FACT.

OBJECTIVE:

TO FIND ANSWERS TO THE FOLLOWING QUESTIONS


- What is an electronic evidence?
- Is electronic evidence regulated in Europe?
- Which are the problems for the European social actors involved when obtaining, analysing and presenting electronic evidence and how are they really acting?

ADDED VALUE:

- 100% new: admissibility of electronic evidence is under study for the first time
- It develops and reinforces the networking between EU States and candidate countries
- Experience and information exchange at European level
- Cooperation among legal authorities, lawyers, police and private experts
- Development of the European Judicial Space (fight against technological crime)

Introduction
THE PROJECT

aec
THE UNIVERSITY OF ELECTRONIC EVIDENCE

1st Stage: Legal analysis	2nd Stage: Fieldwork	3rd Stage: Improvement Guide
<p>Objective:</p> <ul style="list-style-type: none"> Legal analysis on the <i>electronic evidence</i> and its admissibility in Courts. To know the degree of development and legislative homogeneity achieved in Europe. <p>Data: 78 analyzed laws</p> 	<p>Objective :</p> <ul style="list-style-type: none"> In-depth interviews with the social actors involved in a process of digital analysis of electronic means. <p>Data: 125 interviews with:</p> <ul style="list-style-type: none"> Lawyers Judges Prosecutors Notaries Representatives of the Council of the Judiciary Police Officers Experts in Computer Forensics Businessmen 	<p>Objective :</p> <ul style="list-style-type: none"> Elaboration of an improvement guide

| 9

Introduction
COUNTRIES AND RESEARCHERS


aec
THE UNIVERSITY OF ELECTRONIC EVIDENCE



| 10

Introduction
COUNTRIES AND RESEARCHERS : partners

aec
THE UNIVERSITY OF ELECTRONIC EVIDENCE



Partner Institutions

- **ITALY:**
Associazione Nautilus
- **ROMANIA:**
- National Institute of Criminology
- **SPAIN:**
- University of Barcelona
- University Pompeu Fabra
- Spanish National Police
- Cybex
- **UNITED KINGDOM:**
- University of Edinburg
- QinetiQ

| 11

aec
THE UNIVERSITY OF ELECTRONIC EVIDENCE

DEFINITION



| 12

Definition
LEGAL DEFINITION ON ELECTRONIC EVIDENCE

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

- In the legislation of the studied countries there is **no specific definition on electronic evidence**
- The legislative references are related to:

Traditional evidence
Electronic document
Electronic signature
Means of evidence

}


They can be applied by analogy to the electronic evidence


THERE IS NO SPECIFIC DEFINITION ON ELECTRONIC EVIDENCE

| 13

Definition
LEGAL DEFINITION ON ELECTRONIC EVIDENCE

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS




 **In Spain, the Criminal Proceedings Law**


- Includes among the means of evidence those of reproducing words, sounds and images as well as instruments allowing the archiving 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 supports that can be considered a "document" under the Penal Code is included any support containing data.
- Finally in Spain, the Labor Proceedings Law allows the use of any type of evidence, including those mechanical means of reproducing words, images and sounds.

| 14

Definition
LEGAL DEFINITION ON ELECTRONIC EVIDENCE

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS




 **The French Civil Code**


- Describes documentary evidence, or evidence in writing, as "results from a sequence of letters, characters, figures or of any other signs or symbols having an intelligible meaning, whatever their medium and the ways and means of their transmission may be"

| 15

Definition
LEGAL DEFINITION ON ELECTRONIC EVIDENCE

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS




 **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, the 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, facts 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 with other electronic data used as a method of authentication.

| 16

Definition
LEGAL DEFINITION ON ELECTRONIC EVIDENCE

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COLLECTORS



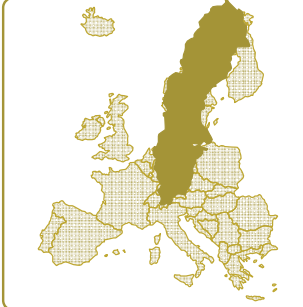
 **In the Police and Criminal Evidence Code of the United Kingdom**


- Evidence is cited 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 programme has been executed.

| 17

Definition
LEGAL DEFINITION ON ELECTRONIC EVIDENCE

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COLLECTORS



 **In Sweden, the Code of Juridical Procedure**

- Establishes as definition of evidence that this has to be the best available, relevant and important.

| 18

Definition
PRACTICE DEFINITION ON ELECTRONIC EVIDENCE

PRACTICE **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COLLECTORS


- There is no homogeneity in the criteria of the interviewed **lawyers, judges, notaries, police officers, experts in Computer Forensics and businessmen** about **electronic evidence** at a European level.
- Some of the expressed definitions:
 - It is an electronic document
 - It is the electronic signature
 - It can be recordings and films
 - It is evidence in an electronic support
 - Electronic evidence comes from the usage of technological elements
 - The information obtained, stored and distributed through technological means
 - Any kind of electronic evidence stored in an electronic support which results from the usage of electronic devices or the electronic communications
 - Any kind of fact element able to establish/prove the existence of a certain crime (committed or revealed) in a digital environment to identify the responsible or the source and to know the necessary context for a fair final solution.

| 19

Definition
EQUIVALENCE OF ELECTRONIC EVIDENCE

LEGISLATION PRACTICE **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COLLECTORS

- According to the analyzed legislation and the practice results, as a general rule, we found the equivalence of **electronic evidence** to the documentary evidence.
- In the European legislations there are the following equivalences:


 - **electronic document = paper document**
 - **electronic receipt = paper receipt**
 - **electronic signature = handwritten signature**
 - **electronic contract = paper contract**
 - **electronic notarial deed = notarial deed**
 - **electronic mail = traditional mail**
 - **electronic mail = phone conversation**
- There is a wide group of interviewees denying the fact that **electronic evidence** is a means of evidence. They rather consider it as a different support.

| 20

Definition
VIEWPOINT ON THE ADVANTAGES AND INCONVENIENCES **PRACTICE** **aec**
THE ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

ADVANTAGES

- Information:** accurate, complete, clear, precise, true, objective, new and neutral
- Evidence:** solid, useful, reliable, feasible, relevant to prove certain crime that were impossible to prove before.
- Manipulation:** Easy obtaining, usage, conservation and storage.
- Electronic mail:** together with the electronic signature make the electronic commerce easier, safer and quicker. Email makes mail cheaper.

INCONVENIENCES

- Legal:**
 - Lack of specific and systematic regulation
 - Few jurisprudence
 - Difficult to establish the legal value of the evidence
 - Difficult to know how to process data and how to interpret the specific procedural laws
 - Difficult to identify the source of a crime
- Technical:**
 - Unknown and very technical issue
 - It requires specific skills
 - Few experts in the field
 - Lack of legal support and certification models
 - High cost for examining and interpretation of the information
- Before the Court:**
 - Difficult to present before the Court in an understandable way
 - Admission in Court more difficult; judges claim for more guarantees than in the case of any other kind of evidence
 - Lack of technical infrastructure in judicial premises
- Data:**
 - Volatility of such data and easy to manipulate
 - Difficult to prove the authenticity, integrity, reliability and the source of the data
 - Difficult to keep, preserve and store

| 21

aec
THE ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

LEGISLATION & CASE LAW

| 22

Legislation and Case Law
LEGISLATION ON ELECTRONIC EVIDENCE: analogy **LEGISLATION** **aec**
THE ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

- There is no specific regulation on *electronic evidence* in Europe.
- The *electronic evidence* is regulated by interpreting analogically the traditional evidence.

Laws regulating the *electronic evidence by analogy*
Total analyzed laws: 78

64%

Data source and processing: AEEC's team.

| 23

Legislation and Case Law
LEGISLATION ON ELECTRONIC EVIDENCE: Jurisdictions **LEGISLATION** **aec**
THE ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

- The **jurisdictions** regulating electronic evidence by analogy in general are :
 - Civil Law
 - Criminal Law
 - Social Law

Data source and processing: AEEC's team.

| 24

Legislation and Case Law
LEGISLATION ON THE ELECTRONIC EVIDENCE : Specific rules

LEGISLATION aec²

• The rules regulating electronic evidence by analogy are basically:

Data source and processing: AEEC's team.

| 25

Legislation and Case Law
LEGISLATION ON THE ELECTRONIC EVIDENCE : Changes

PRACTICE aec²

• General changes to be introduced, according to European jurists:

IMPROVEMENTS

- Adapt the law to reality
- Better collaboration between involved actors
- Better regulation on communication law
- Better collaboration between law enforcement authorities
- Better regulation on the access to data
- Better exchange between states
- Better regulation on e-commerce
- Better implementation of the law
- More searching
- Clarify cross-border rules
- Clarify the telecommunication law
- To allow judges to interpret

THE MOST CLAIMED

CHANGES NEEDED

- Specific procedural provisions

BETTER REGULATION OF EVIDENCE

LEGISLATION

- Specific labour procedure
- Specific judicial regulation on the matter
- Specific rules
- Standards
- International regulation
- Implementing European directives
- Regulating the use of digital evidence
- Implementing the Budapest Convention
- Common standards on documents
- Creating a procedure in labour law when no criminal background
- General rules
- Standards for judgments
- Specific directives
- European harmonization
- Worldwide minimum standard
- International data regulation

OTHERS

- In the future
- Records on subjects
- Liability of the information transmitted
- Compensating the standard person
- Cooperation between states
- Control of communications
- International judicial assistance
- Changing standards
- To change the procedure, not the law
- Implementation of judges and policemen

Data source and processing: AEEC's team.

| 26

Legislation and Case Law
LEGISLATION ON THE ELECTRONIC EVIDENCE : Changes

PRACTICE aec²

• Which changes would the jurists introduce in the existing legislation at ...

European and International level?

International

- World wide minimum standard
- More international regulation
- Specific procedural provisions

European

CHANGES

- General rules
- European harmonization
- Specific European regulation on the matter
- Special Directives
- Specific procedural provisions
- Common standards on e-signature
- Standards
- Standards for documents
- Clarify cross-border rules

Legislation

Improvements

- Changes needed
- Better exchange between States
- Better cooperation between law enforcement authorities
- Reliability of the information transmitted
- Improve collaboration between electronic service providers

Data source and processing: AEEC's team.

| 27

Legislation and Case Law
LEGISLATION ON THE ELECTRONIC EVIDENCE : Changes

PRACTICE aec²

• Which changes would the jurists introduce in the existing legislation at ...

national level?

IMPROVEMENTS

- Adapt the law to reality
- Better communication between involved actors
- European Directives
- To allow judges to interpret
- More control of e-communications
- Regulating the use of digital signatures
- Compensating the standard person
- Changing formalities
- Records on services
- Standards
- More searching
- Qualification of judges and policemen
- Better implementation of the law

CHANGES

Procedure

- Specific procedural provisions
- Specific labour procedure
- To change the procedure, not the law
- Creating procedure in labour law when no criminal background

Electronic

- Better regulation of e-evidence
- Clarify the telecommunication law
- Better regulation on e-commerce
- Better regulation on the access to data

Data source and processing: AEEC's team.

| 28

Legislation and Case Law
LEGISLATION ON THE ELECTRONIC EVIDENCE : Changes PRACTICE aec²
THE ASSOCIATION OF EUROPEAN CYBERCRIME EXPERTS

- General changes to be introduced, according to the experts:

IMPROVEMENTS <ul style="list-style-type: none"> Improvement of international cooperation Changes at European level Better cooperation world wide Develop judicial and police cooperation More cooperation Better organization, no legislation Improvement of evidence gathering Improvement of data retention Better cooperation with in EU countries Easier procedure to identify an IP address/SIM/PUK 	THE MOST CLAIMED <ul style="list-style-type: none"> Follow the Cybercrime Convention Same policy to security issues Privacy data protection Special regulation
LEGISLATION <ul style="list-style-type: none"> Need of a Digital Evidence Act Better regulation on incident response Legislation against IT crimes Regulation about P2P Update of procedural code Legislation standards for IT crimes Regulation of the Criminalistics Experts Harmonization of procedures More legislation 	OTHERS <ul style="list-style-type: none"> Establish an European Forensics Academy Stop the proliferation of software that helps criminals encrypt evidence Preservation of PC for at least 1 year Quick seizure of host for cross border incident Cooperate means in telecommunication cases Cooperation with law enforcement Less storage period Experts protection International level

Data source and processing: AEEC's team. | 29

Legislation and Case Law
LEGISLATION ON THE ELECTRONIC EVIDENCE : Changes PRACTICE aec²
THE ASSOCIATION OF EUROPEAN CYBERCRIME EXPERTS

- Which changes would the experts introduce in the existing legislation at ...

European and international level?

International <ul style="list-style-type: none"> Improvement of international cooperation Privacy data protection Regulation about P2P Better cooperation world wide Specific regulation Develop judicial and police cooperation Harmonization of procedures Same policy to security issues Follow the Cybercrime Convention Quick seizure of host for cross border incident 	European <ul style="list-style-type: none"> Follow the Cybercrime Convention Same policy to security issues Specific regulation Establish a European Forensics Academy Changes at European level Better cooperation with in EU countries Privacy data protection Need of a Digital Evidence Act Easier procedure to identify an IP address/SIM/PUK
---	--

Data source and processing: AEEC's team. | 30

Legislation and Case Law
LEGISLATION ON THE ELECTRONIC EVIDENCE : Changes PRACTICE aec²
THE ASSOCIATION OF EUROPEAN CYBERCRIME EXPERTS

- Which changes would the experts introduce in the existing legislation at a ...

national level?

<ul style="list-style-type: none"> Better regulation on incident response Better organization, no legislation Better regulation on incident response Improvement of evidence gathering Improvement of data retention Update of the Procedural Code More training More cooperation Cooperation with law enforcement 	<ul style="list-style-type: none"> More legislation Need of a Digital Evidence Act Legislation against IT crimes Special regulation Legislation standards for IT crimes Regulation of the Criminalistics Experts Cooperate means in telecommunication cases Experts protection
IMPROVEMENT <ul style="list-style-type: none"> Same policy to security issues Less storage period Preservation of ISP CDR's for at least 1 year Stop the proliferation of software that help criminals encrypt evidence Privacy data protection 	LEGISLATION
National	OTHERS

Data source and processing: AEEC's team. | 31

Legislation and Case Law
SUBJECTIVE VIEWPOINT ON A EUROPEAN LEGAL FRAMEWORK PRACTICE aec²
THE ASSOCIATION OF EUROPEAN CYBERCRIME EXPERTS

DO THE INTERVIEWEES CONSIDER NECESSARY A EUROPEAN LEGAL FRAMEWORK?

(yes) (no)

FISCALES/ PROSECUTEURS/ PROSECUTEURS

Prosecutors justification

- Because of the trans-national dimension of the matter
- As far as the States regulate the admissibility according to their national law
- It would facilitate the international cooperation between judges
- It would provide with a bigger uniformity between national regulations

| 32

Legislation and Case Law
SUBJECTIVE VIEWPOINT ON A EUROPEAN LEGAL FRAMEWORK

aec
ASSOCIATION OF ELECTRONIC EVIDENCE COLLECTORS

PRACTICE

DO THE INTERVIEWEES CONSIDER NECESSARY A EUROPEAN LEGAL FRAMEWORK?

yes no

ABOGADOS/LAWYERS/AVOCATS

Lawyers justification

YES

- Proceeding for collecting electronic evidence must be standardized
- It will facilitate the international cooperation
- It will harmonize data protection issue

NO

- National regulations are enough

| 33

Legislation and Case Law
SUBJECTIVE VIEWPOINT ON A EUROPEAN LEGAL FRAMEWORK

aec
ASSOCIATION OF ELECTRONIC EVIDENCE COLLECTORS

PRACTICE

DO THE INTERVIEWEES CONSIDER NECESSARY A EUROPEAN LEGAL FRAMEWORK?

yes no

EXPERTS IN COMPUTER FORENSICS

Experts justification

YES

- Cooperation between countries, International Cooperation and standardization

NO

- There is no difference between the electronic evidence and the traditional evidence
- They consider that it just will carry more red tape
- Admissibility must be kept at national level. It will involve more cost

| 34

Legislation and Case Law
SUBJECTIVE VIEWPOINT ON A EUROPEAN LEGAL FRAMEWORK

aec
ASSOCIATION OF ELECTRONIC EVIDENCE COLLECTORS

PRACTICE

DO THE INTERVIEWEES CONSIDER NECESSARY A EUROPEAN LEGAL FRAMEWORK?

yes no

NOTARIOS / NOTARIES

Notaries justification

YES

- Will help the States to implement the existing laws
- It will help the free movement of documents at European level
- It will help to develop the freedom and security area
- It will allow the set up of a European register

NO

- They consider the situation is over-regulated

| 35

Legislation and Case Law
SUBJECTIVE VIEWPOINT ON A EUROPEAN LEGAL FRAMEWORK

aec
ASSOCIATION OF ELECTRONIC EVIDENCE COLLECTORS

PRACTICE

DO THE INTERVIEWEES CONSIDER NECESSARY A EUROPEAN LEGAL FRAMEWORK?

yes no

JUECES/JUDGE/JUGE

Judges justification

YES

- It will help national regulation to be developed
- It will be very useful to obtain evidence when there are different countries involved

NO

- Denmark and Finland: they think it is irrelevant and that it is not convenient
- Austria: does not say its arguments

| 36

Legislation and Case Law
SUBJECTIVE VIEWPOINT ON A EUROPEAN LEGAL FRAMEWORK

PRACTICE aec²
INSTITUTE FOR ELECTRONIC EVIDENCE IN COURT

WHY DO THE INTERVIEWEES CONSIDER NECESSARY A EUROPEAN LEGAL FRAMEWORK?

- A EUROPEAN FRAMEWORK ON ELECTRONIC EVIDENCE WILL HELP WITH THE LEGAL NATIONAL DEVELOPMENT OF THE ISSUE
- IT WILL HELP TO DEVELOP IN A UNIFORM WAY THE LEGISLATION
- IT WILL FACILITATE THE INTERNATIONAL COOPERATION BETWEEN JUDGES



37

Legislation and Case Law
JURISPRUDENCE: Jurists

PRACTICE aec²
INSTITUTE FOR ELECTRONIC EVIDENCE IN COURT

Viewpoint of jurists on the cases in which electronic evidence is relevant:

- CONTRADICTIONARY CASE LAW
- PERSONAL DATA
- LABOUR CASES
- CYBERCRIME
- INTERCEPTION OF COMMUNICATIONS

DATA

- COPYING & DESTROYING EXTRA-COMPUTER DATA (2002)
- ACCESS TO ITALIAN AGATA - NOT COMPULSA - NOT A CRIME
- SCANNED CONTRACT - AVOID CONTRACT (2005)
- RESPONSIBILITY PROVIDER OF PHONE LINE
- ENTERPRISE CAN CHECK EMPLOYEES ACTIVITY BUT NOT ACCESS PRIVATE CONTENT
- DISCONNECTING TELECOMMUNICATIONS PROVISIONS BETWEEN PROVIDER & SERVICE
- CONFIDENTIALITY
- FRAUD MATTERS
- FRAUD CASES
- SUPREME COURT
- VIOLATION OF ARTICLE 206(1)
- SPENDING COMPANIES
- ITALY/ENGLAND CHANNEL
- TRAFFIC CASE IN SCOTLAND

LABOUR CASES

- EVIDENCE = DOCUMENTARY OR REAL EVIDENCE
- ONLINE = EVIDENCE
- EMAILS = CORRESPONDENCE
- IDENTIFIABLE
- EMAIL = EVIDENCE LABOUR
- CORRESPONDENCE IN FILES & COMPUTER FILES = EVIDENCE (DSS FRENCH MATTERS)
- ONLINE = EVIDENCE (DSS CONFIDENTIAL MATTERS)
- INCLUDING LABORERS IN VISIBILITY
- ONLINE = EVIDENCE (DSS MATTERS)
- AUTHENTICITY & RELIABILITY OF EVIDENCE (FRG)

Data source and processing: AEEC's team.

DIVERGING CASE LAW IN THE SAME COUNTRY
LACK OF HOMOGENEITY

38

Legislation and Case Law
CASE LAW: Experts and businessmen

PRACTICE aec²
INSTITUTE FOR ELECTRONIC EVIDENCE IN COURT

The most frequent cases:

POLICE OFFICERS AND EXPERTS IN COMPUTER FORENSICS (private)

- Child pornography
- Financial crime
- Cyberterrorism
- Hacking
- Unfair competition
- Abuse of corporate means
- Intellectual property

BUSINESSMEN

- Abuse of corporate means
- Bank fraud
- In the labour field (dismissal)
- Unfair competition
- Crime related to intellectual property

39

aec²
INSTITUTE FOR ELECTRONIC EVIDENCE IN COURT

PROCEEDINGS & ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COURT

cybex
INTEGRATED EVIDENCE MANAGEMENT

40


Procedure
LEGAL PROCEDURE: Analogy

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

- There is no specific procedure in the studied countries for the obtaining, analysis and presentation of *electronic evidence*.
- Sometimes, the evidence's general proceeding is applied, other times the proceeding established for a traditional means of evidence is applied by analogy – e.g. documentary evidence.
- A 48% of the evaluated rules contains procedural proceedings to apply to *electronic evidence* by analogy.
- In the United Kingdom, Belgium and Rumania have national rules allowing to obtain evidence from computers: *Police and Criminal Evidence Act*, *Loi relative à la criminalité informatique* and *Law on measures to ensure transparency in the exercise of public dignity, in the business environment, to prevent and sanction corruption*, respectively.

Laws containing proceedings to apply to *electronic evidence* by analogy.

48%



Data source and processing: AEEC's team.

| 41

Procedure
EUROPEAN VIEWPOINT ON THE EXISTENCE OF A PROCEDURE

PRACTICE **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

- The most common viewpoint among **jurists** is that legislation does not regulate any specific procedure on *electronic evidence*.

- There must be always a judicial order to carry out an investigation/obtaining of evidence
- A general proceeding is to be applied for the obtaining of evidence
- There is no specific proceeding for the *electronic evidence*


- **Police** has inner protocols of performance in practice.

| 42

The Admissibility of the electronic evidence in Court
COMPETENT AUTHORITY AND MOTIVATION

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

- The competent authority in Europe for the admission of electronic evidence from a legislative point of view is the Judge
- He can always ask for the original support



- Who keeps the original evidence in safety?

CIVIL	CRIMINAL
<p>Previous stages: The parties</p> <p>During the trial: The parties</p> <p>Some countries: Notary/Expert</p>	<p>Investigation stage: Police</p> <p>Trial stage: The Court administrative services</p>

THE JUDGE / COURT MUST ALWAYS REASON A REJECTION

| 43

The Admissibility of the Electronic evidence in Court
RESPONSIBLE FOR THE OBTAINING OF ELECTRONIC EVIDENCE

LEGISLATION **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

Criminal matters	Civil matters
<p style="text-align: center;">● COURT</p> <p style="text-align: center;">● POLICE</p> <p style="text-align: center;">● EXPERT</p> <p style="text-align: center;">Traditional actors</p>	<p style="text-align: center;">● PARTIES</p> <ul style="list-style-type: none"> ● CERTIFIED E-MAIL PROVIDER ● INTERNET PROVIDER ● MINISTRY OF COMMERCE ● DATA HOLDER ● DATA PROVIDER <p style="text-align: center;">New actors</p>

THE PARTIES ARE THE MAIN RESPONSIBLE FOR THE OBTAINING OF ELECTRONIC EVIDENCE IN CIVIL LAW

THE POLICE AND THE COURTS ARE THE RESPONSIBLE ONES IN CRIMINAL LAW

Data source and processing: AEEC's team.

| 44

The Admissibility of the electronic evidence in Court
LEGAL REQUIREMENTS FOR THE ADMISSIBILITY LEGISLATION aec²

Legal requirements of the electronic evidence to be accepted in a trial

GENERAL REQUIREMENTS

- LEGITIMACY / LAWFUL PENALTY
- USEFUL
- RESPECT FOR FUNDAMENTAL RIGHTS
- RELEVANT
- EFFECTIVENESS
- PERTINENT
- NECESSARY
- RESPECT FOR DATA PROTECTION RULES
- PROPORTIONATE / REASONABLE
- TRANSPARENCY IN THE GATHERING
- LIMITED TO AN ADEQUATE PROCESS

TECHNICAL REQUIREMENTS

- RESPECT FOR INDIVIDUAL PRIVACY
- PROPORTIONALITY BY THE GATHERING
- RESPECT FOR THE SECRECY OF COMMUNICATIONS
- AVOIDING DISPLAY TRAPS
- IMPERIAL
- RELIABLE
- JUSTIFIED
- EFFICIENT
- BEST AVAILABLE
- ORIGINAL
- IDENTIFICATION OF THE SENDER
- GUARANTEE OF INTEGRITY
- STORAGE SAFETY CONDITIONS
- TECHNICAL REQUIREMENTS FOR THE ELECTRONIC EVIDENCE
- CONFIDENTIALITY
- REQUIREMENTS TO CHECK THE DELIVERY
- SECURITY OF THE EVIDENCE
- PREVIOUS INFORMATION TO THE COMPUTERS OWNER
- TECHNICAL REQUIREMENTS FOR THE ELECTRONIC CERTIFICATED

Data source and processing: AEEC's team. | 45

The Admissibility of the electronic evidence in Court
LEGAL REQUIREMENTS FOR THE ADMISSIBILITY PRACTICE aec²

Viewpoint of the jurists on the legal requirements which are usually overlooked

- Respect for fundamental rights
- Right to data protection
- Respect to the Law of Telecommunications
- The chain of custody
- Lack of measures related to the authenticity of evidence
- The absence of electronic signature in the documents

| 46

The Admissibility of the *electronic evidence* in Court
INFLUENCE OF LEGALITY GUARANTEES ON THE ADMISSIBILITY PRACTICE aec²

INFLUENCE OF LEGALITY GUARANTEES ON THE ADMISSION OF ELECTRONIC EVIDENCE

ABOGADOS / LAWYERS / AVOCATS

yes no

Lawyers justification

NO

- **Denmark:** The material truth is what counts here
- **Finland:** A fair trial is the most important thing

| 47

The Admissibility of the *electronic evidence* in Court
INFLUENCE OF LEGALITY GUARANTEES ON THE ADMISSIBILITY PRACTICE aec²

INFLUENCE OF LEGALITY GUARANTEES ON THE ADMISSION OF ELECTRONIC EVIDENCE

JUEZ / JUDGE / JUGE

yes no

Judge justification

no

- **Denmark:** it would only affect in case one of the parties objects in relation to the respect to the guarantees of legality

| 48

The Admissibility of the electronic evidence in Court
INFLUENCE OF LEGALITY GUARANTEES ON THE ADMISSIBILITY

PRACTICE aec²
THE ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

INFLUENCE OF LEGALITY GUARANTEES ON THE ADMISSION OF ELECTRONIC EVIDENCE

yes no

FISCALES / PROSECUTORS / PROSECUTEURS

Justification Prosecutors

no
 • Ireland:
 In case of illegality in the obtaining of the evidence, the judges must take into account the seriousness of the crime

49

The Admissibility of the electronic evidence in Court
INFLUENCE OF LEGALITY GUARANTEES ON THE ADMISSIBILITY

PRACTICE aec²
THE ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

INFLUENCE OF LEGALITY GUARANTEES ON THE ADMISSION OF ELECTRONIC EVIDENCE

yes no

NOTARIOS / NOTARIES / NOTAIRES

50

The Admissibility of the electronic evidence in Court
VIEWPOINT ON THE GUARANTEES OF LEGALITY

PRACTICE aec²
THE ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

Viewpoint on the **guarantees of legality** considered by jurists to be respected when obtaining, analyzing and presenting electronic evidence in courts

Data source and processing: AEEC's team.

51

The Admissibility of the electronic evidence in Court
VIEWPOINT ON THE PRINCIPLES AFFECTING THE ADMISSIBILITY

LEGISLATION aec²
THE ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

According to the **analyzed rules**, the legal principles affecting the admissibility of electronic evidence are the following

Data source and processing: AEEC's team.

52

The Admissibility of the electronic evidence in Court
VIEWPOINT ON THE PRINCIPLES AFFECTING THE ADMISSIBILITY

PRACTICE **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

Viewpoint of the jurists on the principles affecting the admissibility of electronic evidence

LEGITIMACY

- PERTINENCE
- UTILITY
- TRANSPARENCY
- EFFECTIVENESS
- LAWFUL FINALITY
- NECESSITY IN THE GATHERING
- PROPORTIONALITY IN THE GATHERING
- RESPECT FOR FUNDAMENTAL RIGHTS
- FREEDOM OF EXPRESSION
- INDIVIDUAL PRIVACY
- SECRECY OF COMMUNICATIONS
- WORKERS RIGHTS
- DATA PROTECTION RULES

Data source and processing: AEEC's team.

53

The Admissibility of the electronic evidence in Court
VIEWPOINT ON THE PRINCIPLES AFFECTING THE ADMISSIBILITY

PRACTICE **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

Viewpoint of the technical experts on the principles affecting the admissibility of electronic evidence.

- Respect to the individual rights
- Keeping the confidentiality
- Respect to the general rules of data protection
- They have the legal support from a notary
- Witness presence

54

The Admissibility of the electronic evidence in Court
VIEWPOINT ON THE PROBATORY VALUE

PRACTICE **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

Viewpoint of the jurists on the factors providing the best probative value to electronic evidence:

Factor	Frequency (approx.)
Who collects it	21
Like traditional evidence	10
Technical support	9
Guarantees of authenticity	6
Case by case	5
No relevant practice	5
Type of evidence	4
Utility	2
Relevance	1
Reliability of technical proceeding	1

THE PERSON WHO OBTAINS THE ELECTRONIC EVIDENCE IS THE FACTOR PROVIDING THE BEST PROBATORY VALUE .

Data source and processing: AEEC's team.

55

aec
ASSOCIATION OF ELECTRONIC EVIDENCE COURTS

COMPUTER FORENSICS EXPERTS

56

Experts
TRAINING OF EXPERTS IN COMPUTER FORENSICS

PRACTICE aec²

- There are no rules about who should/must become an expert in Computer Forensics.
- Jurists and technical experts consider the years of experience of an expert in Computer Forensics as the most important factor.
- Computer Forensic experts should have a degree in Engineering, Computer Engineering or Mathematics, if possible.
- An expert with a degree must have at least 2 year experience. An expert without a degree must have 5 years experience.
- They must undergo continuous training to keep their knowledge updated.
- In all studied countries, there are private Computer Forensic experts, together with police specialist. In Romania, all of them have to hold an official certification issued from the State.

57

Experts
VIEWPOINT ON THE REQUIREMENTS TO ACT AS AN EXPERT

PRACTICE aec²

Viewpoint of jurists on the special requirements to act as a Computer Forensic expert before the courts:

- No special requirements
- Legal list at Court
- Computers Experts
- There is no requirements established by law
- Must have experience
- Must be certified by a public authority

Data source and processing: AEEC's team.

58

Experts
VIEWPOINT OF JURISTS ON WHO SHOULD/MUST BE AN EXPERT

PRACTICE aec²

Jurists point of view on who should/must be an expert in Computer Forensics:

POLICE IN THE PUBLIC SECTOR AND EXPERTS WITH KNOWLEDGE IN COMPUTER SCIENCE AND A PUBLIC CERTIFICATION IN THE PRIVATE SHOULD BE THE EXPERTS ACCORDING TO THE JURISTS

Data source and processing: AEEC's team.

59

Experts
VIEWPOINT OF EXPERTS ON WHO SHOULD/MUST BE AN EXPERT

PRACTICE aec²

Specialist in Computer Forensics point of view on who should be an expert in Computer Forensics:

EXPERTS CONSIDER SPECIFIC EXPERIENCE IN COMPUTER FORENSICS ANALYSIS IS ESSENTIAL

Data source and processing: AEEC's team.

60

a²
ASSOCIATION OF
EUROPEAN COURTS

IMPROVEMENT GUIDE

Based on the European professionals' perceptions and subject views

61

PRACTICE a²
ASSOCIATION OF
EUROPEAN COURTS

IMPROVEMENT GUIDE LEGISLATION ON THE ELECTRONIC EVIDENCE : objects

DO YOU THINK ELECTRONIC EVIDENCE IS ENOUGH / WELL REGULATED?

- There is no common criteria in Europe (contradictions)
- The general trend: electronic evidence is not well regulated

YES

- Lawyers
- Prosecutors
- Notaries

}

NO

- Civil Judges
- Criminal Judges
- Social Judges
- Commercial Judges
- Experts in Computer Forensics
- Representatives of the Judiciary

62

PRACTICE a²
ASSOCIATION OF
EUROPEAN COURTS

IMPROVEMENT GUIDE LEGISLATION ON THE ELECTRONIC EVIDENCE : Changes

- Are European jurists for the changes?

77%

Data source and processing: AEEC's team.

63

PRACTICE a²
ASSOCIATION OF
EUROPEAN COURTS

IMPROVEMENT GUIDE CHANGES SUGGESTED

CHANGES SUGGESTED BY JURISTS

IMPROVEMENTS

- ADAPT THE LAW TO REALITY
- BETTER COOPERATION BETWEEN INVOLVED ACTORS
- BETTER REGULATION ON COMMUNICATION LAW
- BETTER COOPERATION BETWEEN LAW ENFORCEMENT AUTHORITIES
- BETTER COLLABORATION BETWEEN ELECTRONIC SERVICE PROVIDERS
- BETTER REGULATION ON THE ACCESS TO DATA
- BETTER EXCHANGE BETWEEN STATES
- BETTER REGULATION ON LICENSING
- BETTER REGULATION OF THE LAW
- MORE GUIDANCE
- CLARIFY CROSS-BORDER RULES
- CLARIFY THE TELECOMMUNICATION LAW
- VALIDITY ASSES TO EXTERRITE

THE MOST CLAIMED

CHANGES NEEDED

BETTER REGULATION OF E-EVIDENCE

SPECIFIC PROCEDURAL PROVISIONS

LEGISLATION

- SPECIFIC LEGAL PROCEDURE
- SPECIFIC EUROPEAN REGULATION ON THE MATTER
- BEPIL RULES
- STANDARDS
- INTERNATIONAL REGULATION
- ESTABLISHING THE LEGAL OBJECTIVES
- REGULATING THE USE OF DIGITAL IDENTITIES
- ESTABLISHING THE LEGAL COOPERATION
- COMMON STANDARDS ON JURISDICTION
- CHANGING PROCEDURES BY NATIONAL LAW WHEN NO CRIMINAL BACKGROUND
- GENERAL RULES
- STANDARDS FOR DOCUMENTS
- SPECIAL OBJECTIVES
- EUROPEAN HARMONIZATION
- WORLD WIDE HARMONIZATION STANDARDS
- INTERNATIONAL DATA REGULATION

OTHERS

- IN THE FUTURE
- ACCESS ON SERVICES
- RELIABILITY OF THE INFORMATION TRANSMITTED
- CRYPTOGRAPHY OF THE BUSINESS PERSON
- COOPERATION BETWEEN STATES
- CONTROL OF LICENSING
- INTERNATIONAL MUTUAL ASSISTANCE
- CHANGING PROCEDURES
- TO CHANGE THE PROCEDURES NOT THE LAW
- RESOLUTION OF JUDGES AND FORENSICS

Data source and processing: AEEC's team.

64

Improvement guide
CHANGES SUGGESTED

PRACTICE aec²
THE AUTHORITY OF ELECTRONIC EVIDENCE

CHANGES SUGGESTED BY COMPUTER FORENSIC EXPERTS AND POLICE OFFICERS

<p>IMPROVEMENTS</p> <ul style="list-style-type: none"> ● IMPROVEMENT OF INTERNATIONAL COOPERATION ● CHANGES AT EUROPEAN LEVEL ○ BETTER COOPERATION WORLD WIDE ○ DEVELOP JUDICIAL AND POLICE COOPERATION ○ HOME COOPERATION ○ BETTER ORGANISATION, NO LEGISLATION ○ IMPROVEMENT OF EVIDENCE GATHERING ○ IMPROVEMENT OF DATA RETENTION ○ BETTER COOPERATION WITH IN EU COUNTRIES ○ EASER PROCEDURE TO IDENTIFY AND ACCESS IP/URL 	<p>THE MOST CLAIMED</p> <ul style="list-style-type: none"> ● FOLLOW THE CYBERCRIME CONVENTION ● SAME POLICY TO SECURITY ISSUES ● PRIVACY DATA PROTECTION ● SPECIAL REGULATION
<p>LEGISLATION</p> <ul style="list-style-type: none"> ● NEED OF A DIGITAL EVIDENCE ACT ● BETTER REGULATION ON INCIDENT RESPONSE ○ LEGISLATION AGAINST IT CRIMES ○ REGULATION ABOUT ISP ○ UPDATE OF PROCEDURAL CODE ○ LEGISLATION STANDARDS FOR IT CRIMES ○ REGULATION OF THE CYBERNETICS EXPERTS ○ HARMONISATION OF PROCEDURES ○ HOME LEGISLATION 	<p>OTHERS</p> <ul style="list-style-type: none"> ○ ESTABLISH AN EUROPEAN FORENSICS ACADEMY ○ STOP THE INDUSTRISATION OF SOFTWARE THAT HELPS CRIMINALS ENCRYPT EVIDENCE ○ PRESERVATION OF SP COPIES FOR AT LEAST 1 YEAR ○ QUICK SECURE OF HOST FOR CROSS BORDER INCIDENT ○ COORDINE NON-IP IN TELECOMMUNICATION CASES ○ COOPERATION WITH LAW ENFORCEMENT ○ LESS STORAGE PERIOD ○ IMPROVE PROTECTION ○ INTERNATIONAL LEVEL

Data source and processing: AEEC's team.

65

Improvement guide
SUGGESTED CHANGES

PRACTICE aec²
THE AUTHORITY OF ELECTRONIC EVIDENCE

- Suggested changes are:
 - Specific provisions for the *electronic evidence*
 - Better regulation/ Specific regulation for the *electronic evidence*
 - In compliance with the Cybercrime Convention from the Council of Europe
 - Homogeneous policy in security matters
 - Better protection of personal data

66

Improvement guide
DESIRABLE DEGREE OF TRAINING AND EXPERIENCE OF THE EXPERTS

PRACTICE aec²
THE AUTHORITY OF ELECTRONIC EVIDENCE

ACCORDING TO THE JURISTS:

- Computer Engineers (IT, Civil Engineers, Technicians, etc..)

PARTICULAR SUGGESTIONS:

- The judge himself must decide who should act as expert.
- Specific training on electronic evidence.
- Expert lawyers in Right of the Telecommunications.

ACCORDING TO THE EXPERTS

- Graduates in Computer Sciences, Engineering or Mathematics
- At least 2 years experience (for graduates) and 5 years experience (for not graduates)
- Continuous training

THE PROFESSIONAL EXPERIENCE HAS A GREAT RELEVANCE AND IT HAS BEEN EVALUATED AS A VERY POSITIVE FACTOR BY JURISTS AND EXPERTS

67

Improvement guide
VIEWPOINT OF THE BUSINESSMEN

PRACTICE aec²
THE AUTHORITY OF ELECTRONIC EVIDENCE

SUGGESTIONS:

- ✓ The legal situation is appropriate. There no need of changes (Denmark, Finland and Luxembourg)
- ✓ We need to reinforce and clarify the legislation
- ✓ We need to reduce the time of document storage
- ✓ Prevention
- ✓ Businessmen must be advised on how to collect and store electronic evidence in order to maximize the probative value of such evidence
- ✓ Exchange of best practice with other countries
- ✓ Implementation of the electronic signature
- ✓ Security in electronic communications
- ✓ Freedom in the admissibility of the electronic evidence

68

Improvement guide
PROSPECTS OF THE *ELECTRONIC EVIDENCE*

PRACTICE **aec**
ASSOCIATION OF ELECTRONIC EVIDENCE EXPERTS

• How the future of the *electronic evidence* is perceived in Europe?

- Judges will decide
- Guarantees for e-signature
- Implementing the law
- Regulated at European level
- Balanced with individual rights
- Protecting 3rd parts
- Tools to serve the legal system
- According to the Budapest Convention

Specific legislation

Progressively

More important

Adapting legislation

- Not regulated in the future
- Long time evolution
- Slowly to common guidelines
- No problems=no changes
- e-evidence=paper documents

- According to the practice
- More private investigation
- More measures for the praxis
- Providing education & training
- Reliable evidence
- Technology develops faster than legislation

Data source and processing: AEEC's team.

| 69

Recommendations
KEY POINTS FOR THE IMPROVEMENT OF THE REGULATION & PRACTICE

aec
ASSOCIATION OF ELECTRONIC EVIDENCE EXPERTS

- 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 the current 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.*

| 70

aec
ASSOCIATION OF ELECTRONIC EVIDENCE EXPERTS

→

Thank you for your attention

QUESTIONS TIME

| 71