

Main Legal Issues Concerning Information Security

ENISA-FORTH Summer School in Network and Information Security
Heraklion, 15 - 19 September 2008

Prof. Avv. Giusella Finocchiaro
University of Bologna
Studio Legale Finocchiaro
giusella.finocchiaro@studiolegalefinocchiaro.it
tel. +39 051 22.13.09 fax: +39 051 22.02.79

PART I



Electronic signatures in the EU legislation

Electronic document

- There is no specific definition at European level

Electronic document

- Italian definition:
 - Any electronic representation of acts, facts or data which have legal significance

Most substantial problems with EDs

- They are made of bits; therefore
 - can be changed
 - can be reproduced in several copies
 - identical to the original

Legal questions

- Is an ED a writing?
- What is its evidentiary value?
- Have its copies the same value as the original?

Some historical passages

- 1985 Uncitral Recommendation on the legal value of computer records
- 1996 Uncitral Model Law on electronic commerce
- 2001 Uncitral Model Law on electronic signatures
- 2005 UN Convention on the use of electronic communications in international contracts

How to make electronic documents non changeable

- Through technological measures as for example:
 - the use of *encryption*
 - the *RSA* encryption
 - *PKI* infrastructure

The Directive 1999/93/EC

- Whereas no. 4:
 - *“Electronic communication and commerce necessitate ‘electronic signatures’ and related services allowing data authentication; divergent rules with respect to legal recognition of electronic signatures and the accreditations of certification-service providers in Member States may create a significant barrier to the use of electronic communication and electronic commerce...”*

Two kinds of signatures

- Electronic signature
- Advanced electronic signature
 - advanced ES with qualified certificate

Electronic signature

- Data in electronic form which are attached or logically associated with other electronic data and which serve as a method of authentication

Advanced electronic signature

- Uniquely linked to the signatory
- Identifies the signatory
- Under the signatory's control
- Any change of data is detectable

EU approach toward ESs

- Technology-neutral legislation

Examples of ESs

- Pin
- Id and password
- Puk
- Bar code
- Infrared identification
- Rfid identification

Certification-service-providers

- Issue certificates
- Provide other services related to electronic signatures

The electronic certificate

- An ED which:
 - links signature-verification data to a signatory
 - confirms the identity of that signatory

Qualified certificates

- A certificate that:
 - meets the requirements of Annex I; and
 - is issued by an Annex II certification-service-provider

Minimum requirement for Member States

- Pursuant Art. 5.2 of the Directive 1999/93/EC
 - no electronic signatures shall be denied legal effectiveness and admissibility as evidences

Maximum requirement for Member States

- “Qualified signature”; and
- Secure signature-creation device
- Same value of handwritten signature (Art. 5.1)

State Members discretion

- Given the previous parameters, State Members have a degree of discretion in implementing the Directive

Robustness of signatures

- Electronic signatures are not necessarily less robust than qualified signatures
- *E.g.*, a biometric feature may well be an electronic signature but not a qualified one

France: implementation of the Directive

- Electronic Signature Act (Law no. 2000-230 of May 13, 2002)
- Such law added Sections 1316 to 1316-4 of the French Civil Code
- Decree no. 2001-272 of March 30, 2001

France: types of ESs

- Electronic signature
- Secured ES
- Secured ES corresponding to the qualified certificate

France

- France's implementations sticks to the text of the Directive
- France has not issued a specific legislation addressing contractual relationships between parties using ESs

France: qualified signature

- Qualified signature: handwritten signature

Germany: implementation of the Directive

- 2001 Signature Act (Signaturgesetz or SigG), which substituted previous 1997 legislation
- Amended in 2005 by Signature Modification Act

Germany: value of ESs

- Qualified signatures = handwritten signatures

Germany: signatory's identification

- In order to issue a qualified certificate
 - there is no need for the signatory to apply in person,
 - and identification can be based on previous identification processes

UK: implementation of the Directive

- 2000 Electronic Communications Act
- 2002 Electronic Signatures Regulations (SI no. 318 of 2002)

UK: evidentiary value of ESs

- As for the 2000 Act, ESs are admissible as evidence if:
 - they are incorporated into an electronic communication; and
 - there is a suitable certification process

UK: evidentiary value of ESs

- As per the 2002 Regulations, the Secretary of State shall keep a register of “certification services providers who purport to offer ‘qualified certificates’”

Italy: general rule on the full value of electronic documents

- As for art. 15, § 2 of Law no. 59/97:
- All data, acts, documents and contracts which are electronically generated, concluded, stored or transmitted via ICT networks either by Public administration or by privates are legally valid

Italy: implementation of the Directive

- Regulation of ESs since 1997 Decree of the President of Republic no. 513
- Current legislation: Legislative Decree of 7 March 2005, no. 82
- Amended by the Legislative Decree of 4 April 2006, no. 159

Italy: two kinds of signatures

- Electronic signature
- Qualified signature
- No reference to advanced ES as described in the Directive

Italy: firma digitale

- “Firma digitale” (digital signature) is currently the only actual type of qualified signature
- A non technology-neutral approach

Italy: firma digitale

- A qualified signature based on a PKI infrastructure

Italy: uses of “firma digitale”

- “firma digitale” has a full validity in private to private relationships, as well as in C2G, G2C, G2G relationships

Italy: EDs and their value as writings

- All EDs (with or without an ES) may be considered as writings before a Court, taking into account the following:
 - their quality, security, robustness and modification-proof features

Italy: EDs with qualified ESs as writings

- All EDs with a qualified ES are writings, with the same legal value required for compulsory written deeds

Italy: EDs with qualified ESs

- Qualified signature = handwritten signature

Italy: evidentiary value of EDs

- Three cases:
 - EDs without any signature,
 - EDs with an electronic signature,
 - EDs with a qualified signature

Italy: EDs without any signature

- Same value as “mechanical representations” as per article 2712 of the Italian Civil Code
- Full evidence on their content if there is no opposition by the party against which they are brought

Italy: EDs with ESs

- Evidentiary value of EDs depend on these latter's following features:
 - quality,
 - security,
 - robustness
 - modification-proof
- In any case, art. 2712 of the Civil Code applies

Italy: EDs with qualified ESs

- Full evidence that the ED is generated by the signatory
- The signatory has the burden to prove not to have generated the ED

EU: electronic storage of documents

- There is no EU broad-scope legislation on this matter
- Specific legislation on the e-invoice

Directive 2001/115/EC

- Prior acceptance of the recipient
- Security on the origin and non modification of e-invoices

Implementation of Directive 2001/115/EC

- Member States have followed different approaches:
 - some require the use of qualified ES,
 - others admit also advanced ES,
 - others even accept non-signed e-invoices

Italian legislation on the E-storage of documents

- Broad-spectrum legislation for Public Administrations
- Rules for private citizens
- Specific legislation on *e-invoicing* (Legislative Decree of 20 February 2004, no. 52, implementing the Directive 2001/115/EC)

Legislation specific for Public Administrations

- Legislative Decree no. 82/2005 (Code of Digital Administration)
- Decree of the President of the Council of Ministers of 13 January 2004
- Cnipa's Deliberation of 19 February 2004, no. 11

Basic rule: Public Administrations' own assessment

- Pursuant Art. 42 of Legislative Decree no. 82/2005:
- Choosing to dematerialize documents, Public Administrations shall make a balance of pros and cons

Compulsory specifics

- Not any document digitalization has legal validity,
 - only those made pursuant to rules laid down by the lawmakers (compulsory specifics)
- This rule does not apply to previously stored documents by the means of
 - photography,
 - optical recording or else

E-storage requirements

- *Identify* the origin of documents (PA, sector or person in charge)
- *Ensure* the non-modification of documents
- *Grant usability* and the *easy retrieval* of significant information (including those of the original doc.)
- *Meet the security rules* laid down in articles 31-36 of the Data Protection Code

Cnipa's deliberation

- E-archiving: memorization of EDs on any suitable device.
 - each ED shall be identified by a unique code attached to it (prior to the storage process, if any)
- E-storage for document replacement
 - a process which shall follow some fixed specific as laid down in articles 3 and 4 of Cnipa's deliberation.

E-storage for document replacement

- Compulsory requirements:
 - use of optical storage devices
 - “firma digitale” with time-stamp of the person in charge for e-storage, granting for the process
 - in some cases, a further “fd” with time-stamp of a public officer is needed

PART II



Data protection and security

Free flow of data and fundamental rights

- Directive 95/46/EC, whereas No. 3
 - *“Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;”*

Right to privacy

- A fundamental right protecting the individual's private sphere from unauthorized third parties' intrusions

Right to data protection

- The right to control the processing of personal data

Privacy and data protection

- Privacy protection is not a synonym of data protection
- Data protection contributes to privacy protection

Some differences

- Privacy protection does not concern exclusively data
 - also facts, actions and behaviors
- Data protection also concerns
 - data which have been already placed outside the private sphere and therefore cannot be considered as private

European legal framework on data protection

- EU Charter of Fundamental Rights of 7 December 2000, Article 8
- Treaty on the European Union, Article 6
- EU Directives

European legal framework on data protection

- COE resolutions and recommendations
- Art. 29 Working Party's reports
- EDPS publications
- European Court of Justice decisions

Directives

- *Directive 95/46/EC* - processing of personal data and free movement of data
- *Directive 97/66/EC* - electronic communications
- *Directive 2002/58/EC* - electronic communications (“e-Privacy Directive”)
- *Directive 2006/24/EC* - data retention

Council of Europe (1/2)

- *Resolution (74) 29*: electronic data banks in the public sector
- *Resolution (73) 22*: electronic data banks in the private sector
- *1981, Strasbourg Convention*: Automatic Processing of Personal Data

Council of Europe (2/2)

- *R (97) 18*: personal data and statistical purposes
- *R (97) 5*: medical data
- *R (99) 5*: privacy on the Internet
- *R (2002) 9*: insurance purposes

Art. 29 Working Party

- *WP 150* - Review of the e-Privacy Directive
- *WP 148* - Search engines
- *WP 147* - Children's personal data
- *WP 136* - Concept of personal data
- *WP 131* - EHR

European Data Protection Supervisor

- Entry/Exit system and profiling, June 2008
- The role of data protection authorities, October 2007
- Privacy and personal data, February 2007
- Public access to documents and data protection, July 2005

European Court of Justice

- P2P: C-275/06 - Productores de Música de España v. Telefónica de España
- PNR: C-317/04 and C-318/04 - Agreement between the European Community and the United States of America
- Data transfer to a third country: C-101/01 - Bodil Lindqvist

URLs (1/3)

- EU Charter and TEU:
 - <http://eur-lex.europa.eu/en/treaties/index.htm>
- Directives:
 - [http:// ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm)

URLs (2/3)

- COE:
 - http://www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection/documents/international_legal_instruments/2Recommendations
 - and resolutions of the Committee of Ministers.asp#TopOfPage

URLs (3/3)

- WP:
 - http://ec.europa.eu/justice_home/fsj/privacy/workinggroup
- EDPS:
 - <http://ww.edps.europa.eu/EDPSWEB/edps/lang/en/pid/26>
- ECJ:
 - <http://vcuria.europa.eu/jurisp/cgi-bin/form.pl?lang=en>

Directive 96/45/EC

- First comprehensive regulation at Eu level
- Provides the general setting on data protection

Directive 96/45/EC

- Basic definitions
- Subjects: data subject, controller, processor, data protection authority

Directive 96/45/EC

- The essential principle of data subject's consent
- Need of security measures
- Data transfer to third countries

Directive 97/66/EC

- First regulation in the sector of data protection and electronic communication before Directive 2002/58/EC

Directive 2002/58/EC

- Art. 4: Security
- Art. 5: Confidentiality of the communications
- Art. 7: Itemised billing

Directive 2002/58/EC

- Art. 8: Connected line identification
- Art. 9: Location data
- Art. 13: Unsolicited communications

Directive 2006/24

- Amendment of the e-Privacy Directive
- Data to be retained
- Periods of retention
- Obligation to destroy data at the end of the period of retention

Directive 2006/24

- Italy: data retention v. anti-terrorism legislation

Principles

- Directive 96/45/EC, Whereas no. 28:
 - *“Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified”*

General principles

- Free and informed consent
- Fair and lawful processing
- Specified, explicit and legitimate purposes

General principles

- Adequate, relevant and not excessive data
- Accuracy and update
- Limited retention

Consent

- To which extent consent can be considered free and informed?
- The case of the healthcare sector

Adequacy of the processing

- Such principle may limit the controller's processing even in case the data subject has given his/her consent
- Example of application: CCTVs in Italy

Limited data retention

- Does the data subject enjoy a right similar to the so-called “right to oblivion” existing in other legal areas?

The principle of necessity

- Italian Data Protection Code provides an additional principle, after German legislation
 - the principle of necessity

The principle of necessity

- ICT systems and computer programmes shall process personal data only when these latter are necessary.
Use of anonymity techniques whenever possible
- Privacy by design
- WP 150 advocates the principle of data minimisation

Data security

- Art. 17, § 1:
 - *“controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing”*

Objectives

- *Integrity*: avoid destruction, loss, alteration
- *Confidentiality*: avoid unauthorized access
- *Lawfulness*: avoid unlawful processing
- *Availability*: effective data retrieval

Security as a system

- Security does not only concern technological measures

Security as a system

- Technological measures
- Organizational measures
- Human factor
- Constant check and supervision

Technological measures

- Software measures
- Hardware measures
- Physical measures

Organizational measures

- Clear “chain of command”
- Clear procedures
- Specific formation of employees processing data
- Manual or guidelines for reference

Human factor

- Measures to contrast social engineering

Constant check and supervision

- Measures in force should be periodically revised in order to assess their adequacy

Controllers and security

- It is up to the controller to determine and establish all appropriate security measures
- Processor shall follow controller's indications
- Responsibility for inadequacy or disregard of security measures is on the controller, in the first place

Processors

- Contract or legal act in writing or equivalent form by which
 - the processor act only on instructions from the controller,
 - and is responsible for the implementation of the security measures

Appropriateness of measures

- Factor to be considered:
- actual risks
- nature of the data to be protected
- state of the art
- cost of implementation

Security measures in Italy

- Minimum compulsory measures, resulting in criminal liability
- Suitable measures, resulting in civil liability

Minimum compulsory measures

- Data processing by electronic means:
 - authentication
 - management procedures for credentials
 - periodical check on personnel in charge

Minimum compulsory measures

- Hardware and software measures
- Backup and restore procedures
- Updated “document on security”
- Encryption of certain categories of data

Minimum compulsory measures

- Data processing without electronic means:
 - periodical check on personnel in charge
 - procedures for the appropriate storage of acts and documents
 - selective access to document archives

Encryption

- In Italy, data encryption is required only in limited cases:
- sensitive and judicial data processed by public bodies through databases, registries, lists
- health-related data processed by healthcare providers
- genetic data

Security measures in Member States

- Not all States have adopted detailed sets of security measures
- The sets adopted are not uniform
- The evaluation of risks differs from State to State

EU position

- The Commission has expressed dissatisfaction with such lack of harmonization
- See COM(2006)334 final (28 June 2006) 28-29

Security breaches and secrecy

- Absolute secrecy on security breaches
 - may preserve controller's public image and reputation,
 - but worsens the effect of those breaches
- Authorities and any third party damaged by security breaches should be informed

The proposed strengthening of art. 4 of Directive 2002/58/EC

- Provider of publicly available communication services shall notify security breaches
- All persons concerned shall be informed when their data have been compromised or are at risk of being compromised

WP 150

- In favour of the strengthening of art. 4
- Further measures:
- providers of information society should also be under obligation to inform
- more recipients should be informed
- disclosure to the public in certain circumstances

The end