InterPARES 2 Project

International Research on Permanent Authentic Records in Electronic Systems

Policy Cross-domain

Archival Legislation in Italy

Consolidated Version

Compiled by Fiorella Foscarini

March 2005

Table of Contents

1. Scope and Context of the Study 1

2. Methods of Research 1

3. Findings 2

3.1 Definition of record 2
3.2 Assignment of responsibilities for preservation 2
3.3 Governance structure 4
3.4 Scope of acquisition 4
3.5 Lifecycle references 5
3.6 Reference to standards 6
3.7 Access and privacy legislation 7
3.8 E-government legislation 9
3.8.1 Definitions 9
3.8.2 Preservation requirements 11
3.8.3 Authenticity / Authentication 13
3.8.4 Organizational and records management issues 16
3.9 Evidence act (excerpts from the Italian Civil Code) 16

4. List of the Legislative Sources Covered in the Report 20

1. Scope and Context of the Study

This study examines the current enabling legislation and regulations of Italy with reference to records management and archives. From 1963, when the first comprehensive "Archival Law" came into force, until present the Italian lawmaking bodies (Parliament, Government, and President of the Republic) have produced a huge amount of laws, decrees, and directives dealing, whether directly or indirectly, with documentary and archival issues.

In particular in the last decade, with a view to facilitating the relationship between citizens and public, Italy has been very proactive in the field of e-government in the broader context of a general reform of public administration which started in 1990. Both the Government and the Authority for Information Technology in the Public Administration (AIPA, today CNIPA) have made recommendations and issued technical rules about the creation and preservation of authentic electronic records.

This study also makes reference to the Italian Civil Code, in the parts where conditions for the allowance of different kinds of documentary evidence before the Court are settled (evidence acts).

With regard to the hierarchy of the various legislative and regulatory sources involved, it must be specified that, according to the Italian juridical system,

1. The Italian Constitution is the only source of *primary legislation* and is therefore the highest legislative source;
2. Laws (L) and Legislative Decrees (Dlgs), including the Civil Code, are sources of *secondary legislation*;
3. President of the Republic's Decrees (DPR) and Prime Minister's Decrees (DPCM), when they concern regulations or rules, are sources of *tertiary legislation*;
4. Single Texts ('Testi Unici'), as compilations of enabling legislation and regulations on specific matters, have as power as the sources of *secondary legislation*;
5. Directives, Deliberations, Guidelines, and Technical Rules issued by Prime Minister or any governmental Authority (e.g., AIPA or CNIPA) have the lowest enabling power.

2. Methods of Research

Laws and regulations directly dealing with archival matters or concerning records management related issues such as the management of administrative procedures, the impact on documentation of automating public administration's services, the value of records as evidence as well as any technological aspects involved (e.g., digital signatures, e-mails management, e-commerce, etc.) have been identified through the sources which are available on the Internet and on the basis of the indications provided by a survey of the Soprintendenza Archivistica per il Piemonte e la Valle D'Aosta.[1]

A list of the legislative sources covered in this report, including the relevant Web links, is attached at the end of the report.

Each statute has been analyzed following the report outline as described in the Study Definition document. When identified, possible barriers or deficiencies of the legislation as regards record preservation have been highlighted (see parts in *italics*).

[1] Soprintendenza Archivistica per il Piemonte e la Valle D'Aosta, "Obblighi di legge dell'Ente Pubblico riguardo al proprio archivio (nelle tre fasi: corrente, di deposito e storico) e norme sanzionatorie," M. Carassi ed. (vers. 28/05/2004), available at http://www.sato-archivi.it.

3. Findings

3.1 Definition of record

- Public record refers to the record that has been written, according to required formal elements, by a notary or any other public officer who is authorized to confer public trustworthiness to a record in the place where it was created [Civil Code, art. 2699].
- Administrative record is any representation, however created, of the content of any act, whether internal or external, of the Public Administration, which is used to carry out the administrative activity [DPR 445/2000, art. 1, let. a)].
- Electronic record is the electronic representation of legally relevant acts, facts or data [DPR 445/2000, art. 1, let. b)].
- Archives and single records which belong to the State and to any local public administration or institution, as well as those belonging to private individuals and which have recognized historical value, including pictures, moving images and any kind of audio-visual material being particularly rare and precious, all these items are part of the cultural heritage of the Nation [Dlgs 42/2004, art. 10].

  The law does not specify how to determine the 'historical value' of archives and records belonging to private individuals. 'Particularly rare and precious' are vague criteria too. However, this definition of records as cultural goods seems to encompass record types emerging in the artistic and scientific communities.
- The above defined cultural heritage goods are inalienable [Dlgs 42/2004, art. 54] and benefit of all guarantees relating to custody and integral preservation over the long term like any item which is subject to the State property regime [Civil Code, arts. 822-823-824]. In particular, each archival body cannot be divided into parts and must be preserved in its integrity [Dlgs 42/2004, art. 20, par. 2].

3.2 Assignment of responsibilities for preservation

- The person responsible for managing archival repositories in either central or local public institutions or administrations has to hold a specific degree obtained at any of the State Archives' Schools of Archives, Palaeography and Diplomatics or, in alternative, at one of the so-called Special Schools for Archivists and Librarians which belong to universities [DPR 1409/1963, art. 1].
- Following the implementation of electronic records management systems [see below at section h)], every public body has the obligation to establish a service dedicated to the management of active and semi-active records in each of the identified homogeneous areas of the organization [so-called AOO – see below at section h.4)]. The person in charge of such a service, whether a manager or an official, must hold suitable professional requirements or a specific professional degree in archival studies acquired through the procedures that are prescribed by the law [DPR 445/2000, art. 61 pars. 1 and 2].

  The above-mentioned statute extends the specific qualifications that the 1963 law only provided for those who are responsible for archival repositories to the managers of current records, in that implicitly recognizing that in the context of electronic records the preservation duty cannot be left at the end of records lifecycle.

- Specific tasks and responsibilities of the manager or official responsible for the electronic records management service and archives are: a) to elaborate a "Documentary System Management Manual" ('Manuale di gestione') to be adopted by his or her administration; b) to suggest timeframe, procedures, and organizational and technical measures to implement the new electronic records management system; c) to elaborate, together with the information systems' and the personal data protection officers, a "Security Plan" ('Piano per la sicurezza informatica') relevant to creation, management, transmission, exchange, access, and preservation of electronic records [DPCM 31 October 2000, art. 4].
- The "Documentary System Management Manual" includes:
  a) planning of any necessary organizational and functional changes for the implementation of the new records management system;
  b) security plan with reference to electronic records;
  c) how to use electronic devices for exchanging records inside and outside the AOO;
  d) work flow description with reference to all incoming, outgoing, or internal records, including registration rules for those records that are received through particular means, such as telecom-tools, fax, registered and insured mail;
  e) specification of routing rules, including the assignment of received records to the units responsible for their treatment;
  f) identification of the units that are responsible for records registration, organization and maintenance within each AOO;
  g) list of those records which are excluded from the protocol registration[2] *[This means that each administration is free to choose which records to capture in its own recordkeeping system. The criteria for selection are not stated and this might impact on preservation.]*;
  h) list of those records which are meant to be registered in "special registers," including the procedures for their management *[The reason for that may be confidentiality, but the law does not specify the purpose of such "special registers." This might also impact on preservation.]*;
  i) classification system integrated with records schedules (i.e., information about timeframe, criteria, and rules for selection and preservation), including reference to the use of substitute media;
  l) procedures for compiling and preserving all data entered in the electronic protocol register, with particular regard to any technological and organizational strategy which is adopted to guarantee the integrity of the data (non-modifiability), the simultaneousness (contemporaneity) of the operation of entering the data in the system and that of attaching the registration data to the record (in It., 'segnatura,' which corresponds to the operation of stamping some of the registration data – identification number, date, classification code - on the paper-based record), as well

[2] Every time the Italian legislation mentions the terms registration or register, it refers is to the so-called "protocol register" ('registro di protocollo'), which is a mandatory tool that all Italian public bodies have to put in place in order to produce legal evidence of their actions. The protocol register (which used to be a manual register and since January 1, 2004, should have been replaced by electronic systems in all PAs) implies the timely registration of the metadata necessary to identify all incoming and outgoing records (including the classification code), and the assignment of a unique consecutive number to each of them. It is meant to be permanently preserved. "Registration serves not only administrative accountability but also historical accountability over time because the protocol register preserves evidence of the existence of records and the act to which they relate even after the records themselves no longer exist" (L. Duranti, T. Eastwood and H. MacNeil, *Preservation of the Integrity of Electronic Records*, Kluwer Academic Publishers, 2003, p. 48).

as the procedure for registering cancelled or modified information within each registration session;
m) functional and operational description of the electronic protocol registration system;
n) criteria and conditions of authorizing internal and external access to the information registered in the system; and
o) how to use the emergency register (i.e., manual register to be used in cases of "force majeure" when it is not possible to use the electronic system) [DPCM 31 October 2000, art. 5].

- State, Regions and all other local public administrations (i.e., Provinces and Communes) have the obligation to guarantee safety and preservation of the archival material they own. Private individuals who are in possession of archives that have been notified as of historical interest are responsible for the proper custody of their holdings as well [Dlgs 42/2004, art. 30].
- The Minister may impose any necessary preventive intervention – or directly provide for it –in case the owner of archival material (whether public or private) fails in his or her duty [Dlgs 42/2004, art. 32].
- The Minister may impose temporarily coercive custody in public archival institutions in order to guarantee proper preservation of archival material [Dlgs 42/2004, art. 43].

3.3 Governance structure

- Public archives are on the responsibility of the Ministry for Arts and Culture ('Ministero per i beni e le attivita' culturali') that exercises such a responsibility both directly on central authorities' archives and indirectly through the Archival Offices ('Soprintendenze Archivistiche'), which are the regional bodies in charge of supervising all local bodies' (Regions, Provinces, and Communes) archives [Dlgs 42/2004, art. 4]. The latter are also responsible for private archives [Dlgs 42/2004, art. 5, par. 2].
- The Central State Archives in Rome and 17 State Archives, one in each provincial capital, preserve the documentation produced by State (central) authorities and which is older than forty years [Dlgs 42/2004, art. 41, par. 1 - see below at section e)].
- Commissions consisting of representatives of the Ministry for Arts and Culture and the Ministry of the Interior are established at the State administrations with the purpose to supervise current records management, cooperate in defining the criteria for records organization, management and preservation, propose records disposal, take care of records transfer to State Archives, and identify confidential records. Any disposal decision must be authorized by the Ministry for Arts and Culture. In case disposition involves confidential or secret records, the Ministry of the Interior must be consulted as well [Dlgs 42/2004, art. 41, par. 5].
- Ministry of Foreign Affairs, as well as Army, Navy and Air Force are not subjected to the law with regard to their military and operational documentation [Dlgs 42/2004, art. 41, par. 6].

3.4 Scope of acquisition

- The legislation concerns all records produced, received, and kept for whatever reason by any public administration, i.e., public records [DPR 1409/1963, art. 1]. Public records

belong and are accessible to the public, according to institutional use needs and preservation considerations [Dlgs 42/2004, art. 2, par. 4].
- State protection and supervision also refer to single records and archives belonging to private individuals, i.e., private records, which have been notified in reason of the assumption of their historical value [DPR 1409/1963, art. 1; Dlgs 42/2004, art. 10].

3.5 Lifecycle references

- The person in charge of the electronic records management service and archives provides for accurately copying all data entered in the protocol register system on to a removable electronic medium. The transfer or copy of those data on to a removable electronic medium is only allowed for those data which are relevant to semi-active files [i.e., files referring to concluded business procedures]. The transferred information must be always accessible. To this end, the responsible for the service provides that the information contained in the protocol register system is copied on to new electronic media at least every five years, according to the developments of scientific and technological knowledge [DPR 445/2000, art. 62].

  Because of the short life of electronic media, the law assigns preservation tasks to the person responsible for the records management service and archives, who is requested to monitor the status of files and provide for backup copies as soon as files are no longer active.
- At least once a year, the person in charge of the electronic records management service and archives provides for the transfer of all files and records referring to closed procedures to an intermediate archival repository ['archivio di deposito'] that every public administration ought to establish in order to store its semi-active records. In such intermediate repository, transferred files and records must be arranged according to the original order they had when they were in their active phase [DPR 445/2000, art. 67].

  Principle of provenance and respect for the original order are prescribed by the law.
- The electronic records management system keeps track of all records which are returned to offices as well as of the relevant requests of access [DPR 445/2000, art. 68, par. 2].
- Files and records which have been selected for long-term preservation together with the relevant finding aids are transferred to either the competent State Archives or the archival repository, aka "historical archives," that every public administration ought to establish, according to the archival law [DPR 445/2000, art. 69].

  Although DPR 445/2000 recognizes the specific characteristics of electronic records and the challenges as regards their preservation, the three phases of records lifecycle (active – semi-active – inactive) still seem to correspond to three different physical archival spaces (offices – intermediate repository – historical archives).
- Public authorities have the obligation to ensure proper custody and preservation of their archives [Dlgs 42/2004, art. 30, par. 1].
- This entails to ensure that records are maintained integral and in their original order from the moment of their creation, as well as to re-order, when necessary, and describe the archival material that is kept in their "historical archives." The latter are made of the records relevant to affairs (business cases, transactions) which are no longer current for more than forty years. Private owners of archives with recognized historical value have the same obligations of preservation [Dlgs 42/2004, art. 30, par. 4].

The forty-year rule for the transfer of records to historical archives (and maybe the concept of historical archives itself) is a clear barrier to preservation. However, according to the law, archival responsibilities emerge at the point of record creation and the whole lifecycle is therefore under control. The problem is that in public administrations the management of current records is often left in the hands of non qualified staff and for long time one could only find archivists in historical archives. Today, the use of electronic records management systems (ERMS) enables monitoring the whole process and having uniform records treatments in all units of administrations and in all phases of the lifecycle. If well conceived and organized, ERMS may realize the record continuum.

- State juridical and administrative bodies have the obligation to transfer the records relevant to affairs which have been concluded more than forty years before, together with the tools necessary for granting access to them, to the Central State Archives or to the State Archives. Call up lists are transferred seventy years after the year they refer to; notarial acts one hundred years after the relevant notary's activity ended [Dlgs 42/2004, art. 41, par. 1].
- Central State Archives and State Archives may accept early transfers, in case of danger of documents dispersion or damage [Dlgs 42/2004, art. 41, par. 2].
- No transfer of archival material will be accepted unless such material has previously been appraised and selected [Dlgs 42/2004, art. 41, par. 3].

  The consequence of such a provision is that normally appraisal does not happen before the moment of transfer, i.e. before the documentation is at least forty years old.

3.6 Reference to standards

- Exchange of electronic records which have been entered in public protocol registers are done through e-mail systems which have to be compliant with SMTP/MIME protocol as defined in RFC 821-822, RFC 2045-2049 public specifications and following modifications [DPCM 31 October 2000, art. 15, par. 1].
- Every public administration vouches for the readability over time of all records sent or received, by using the standards approved by the Authority for Information Technology in the Public Administration (AIPA) in its circulars or any other non-proprietary format [DPCM 31 October 2000, art. 16, par. 1; AIPA's Circular 7 May 2001, n. 28].
- The provision of message integrity checks and digital signatures is done by using the hash function as it is defined by ISO/IEC 10118-3:1998, *Dedicated Hash-Function 3*, which corresponds to the SHA-1 function [DPCM 31 October 2000, art. 17, par. 2].
- All metadata describing all records entered in the protocol register system are contained in a file which has to be XML 1.0 compliant and compatible with a DTD file that is available on the AIPA Web site [DPCM 31 October 2000, art. 18, par. 1]. The same Web site also provides an index of all public administration using electronic protocol registers and can be accessed by any public or private person by means of any LDAP protocol compliant systems as defined in RFC 1777 public specification [DPCM 31 October 2000, art. 11, par. 3].

- AIPA indicates and periodically updates through its circulars the standards, transmission modalities, formats, as well as minimum and optional metadata[3] that are usually exchanged among public administrations and are associated to registered records. All that is available on the AIPA (today CNIPA) Web site (http://www.cnipa.gov.it/site/it-IT) [DPCM 31 October 2000, art. 18, par. 2].
- With regard to digital signature and technologies relevant to implementing and managing a Public Key Infrastructure (PKI), see AIPA circulars on interoperability rules [DPCM 31 October 2000, art. 18, par. 3].

3.7 Access and privacy legislation

- Access to records that are stored in archival repositories (such as State Archives or historical archives of local public administrations) is free, with the exception of those confidential records which refer to foreign or domestic politics – which become accessible fifty years after the date of their creation -, and to merely personal situations of private individuals – which become accessible after seventy years. The Minister of the Interior may allow access to records classified as confidential before the above mentioned deadlines for reasons of study. Same rules apply to private records which have been deposited or donated to State Archives, although givers can ask for restricting access to all or part of their records that have been created during the last seventy years [DPR 1409/1963, art. 21].
- Access is always restricted with reference to those records which are labelled as State secret, as well as in all other secret or highly confidential circumstances as provided by the law or internal regulations. Access is in any case excluded when there is the need to protect: a) safety, national defence and international relations; b) monetary politics; c) public order and prevention of criminality; d) third parts,' people's, groups' and firms' confidentiality, yet allowing access to anybody who needs to see those records in order to defend his or her own legal interests [L 241/1990, art. 24, pars. 1 and 2].
- Access to administrative records is guaranteed to anyone who has a personal and concrete interest for the protection of legally important situations. Every citizen or group of citizens or organization is entitled to exercise this right towards the public authority that is responsible for permanently keeping the record(s) he or she is interested in [DPR 352/1992, art. 2].
- The access procedure must be completed by thirty days from the day the request for access had been received. Responsible for such a procedure is the manager in charge of the office that is in charge of creatingor permanently keeping the requested record [DPR 352/1992, art. 4, pars. 5 and 7].
- Public authorities have to periodically monitor that the sensitive data they hold are accurate, up-to-date, relevant, complete, non-redundant, and necessary to the purposes those data have been collected for. Redundant, non-relevant or non-necessary data cannot

[3] The law considers as minimum information to be included in the registration metadata the following elements: a) administration identification code; b) homogeneous organizational area code; c) protocol registration date; d) registration progressive number; e) record subject; f) author; and g) addressee(s). Optional information is identified as follows: a) person or office that is responsible for carrying out the action the record is about; b) classification code; c) enclosures identification; d) information about document flow or about any relevant procedure. [DPCM 31 October 2000, arts. 9 and 19].

be utilized, provided that, if they are meant to be preserved, the records which carry those data are always kept [Dlgs 135/1999, art. 3, par. 3].

Privacy legislation does not affect record preservation, as it clearly concerns only the use of data.

- Sensitive data that are contained in electronic registers or databases have to be encoded or ciphered or however manipulated through codes or other systems which allow identifying the people concerned only when that is necessary [Dlgs 135/1999, art. 3, par. 4].

  Such a provision may negatively impact on the preservation of the original structure of records and on our capacity of reading encoded data over time.
- It is considered of high public interest and is therefore allowed to use sensitive data in scientific and historical research, with reference to preserving, arranging, and communicating records which are kept in State Archives and in historical archives of public bodies, according to the archival law [Dlgs 135/1999, art. 23].
- The person concerned has the right to obtain: a) updating, amendment or integration of the data regarding him- or herself; b) deletion, anonymation or block of the data that are illegally managed, including those whose storage is not necessary for the purposes they were collected for [Dlgs 196/2003, art. 7, par. 3].
- When, for any reasons, management of sensitive data ceases, data must be: a) deleted; b) given to different holder that will use them for same or consistent purposes; c) preserved for personal purposes only and not for being communicated to anyone; d) preserved or given to different holder for historical, statistical or scientific purposes, according to laws and ethical codes [Dlgs 196/2003, art. 16, par. 1].

  In general, all privacy laws confirm that any decisions about deletion or block only refer to data and not to records, which must anyway be kept according to archival preservation needs.
- Personal data must be kept and controlled by using appropriate security measures and taking also the latest developments of IT into consideration, in order to minimize the risks of even accidental destruction or loss, non-authorized access or non-allowed use of those data [Dlgs 196/2003, art. 31].
- True copies, either complete or partial, of original records can be made by using any procedure which is able to guarantee an exact and stable copy of such records [DPR 445/2000, art. 18, par. 1].
- Copy authentication can be done by the public officer who is responsible for issuing or keeping the original or by the one who is supposed to collect such copy, as well as by a notary, chancellor, municipal secretary or any other officer who has been delegated by the mayor. Authentication involves attesting that such a copy is compliant with the original, by writing so at the very end of the copy. The authorized public officer is also requested to state the date and place of the making of the copy, the number of pages the copy consists of, his/her own name, surname and role in the organization, as well as to sign in the margin of each intermediate page [DPR 445/2000, art. 18, par. 2].

3.8 E-government legislation

3.8.1 Definitions

- a) **Electronic signature**: the whole of the data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of computerized authentication;
  b) Certification-service-providers: entities that issue electronic certificates and provides other services related to electronic signatures;
  c) Accredited certification-service-providers: certification-service-providers that have been accredited in Italy or in other Member States;
  d) Electronic certificates: electronic attestations which link signature-verification data to the relevant holders and confirm the identity of those holders;
  e) Qualified certificates: electronic certificates which meet the requirements laid down in Annex I of the EU Directive No. 1999/93/CE and are provided by certification-service-providers who fulfil the requirements laid down in Annex II of that EU Directive;
  f) Secure-signature-creation device: device which is used to create an electronic signature and meets the requirements laid down in Annex III of the EU Directive;
  g) **Advanced electronic signature**: electronic signature which is the result of a computerized procedure able to guarantee the univocal link to the signatory and his univocal identification, and which is created using means that the signatory can maintain under his sole control, and is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable [Dlgs 10/2002, art. 2, lets. a)-g)].
- e) **Qualified electronic signature**: advanced electronic signature that is based on a qualified certificate and has been created by means of a secure-signature-creation device;
  n) **Digital signature**: a special kind of qualified electronic signature that is based on a system of asymmetric keys, of which one public and one private, and that allows both signatory and addressee, through the private and the public key respectively, to make evident as well as verify provenance and integrity of any electronic record or group of electronic records [DPR 137/2003, art. 1, lets. e) and n)].[4]

[4] The distinction between "electronic signature" and "advanced electronic signature" comes from the EU Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (available at http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett), which has been put into effect by the Italian Government through the Dlgs 10/2002. Art. 2 of the above mentioned EU Directive defines "electronic signature" (aka "light signature") as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication" and "advanced electronic signature" (aka "strong signature") as "an electronic signature which meets the following requirements: a) it is uniquely linked to the signatory; b) it is capable of identifying the signatory; c) it is created using means that the signatory can maintain under his sole control; and d) it is linked to the data to which it relates in such a manner that any subsequent change of data is detectable." The EU Directive also specifies that "advanced electronic signatures based on qualified certificates aim at a higher level of security; advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled" (par. 20 of the recitals). Following the latter indications, the DPR 137/2003 made the distinction between "qualified

- a) Record: electronic or analogue configuration of acts, facts and data which are intelligible directly or through an electronic processing;
  b) Analogue record: record created using a physic quantity that assumes continuous values, such as signs on paper (e.g., paper documents), images on film (e.g., microfiche and microfilm), magnetization on tape (e.g., magnetic audio- and video-tapes). It may be an original or a copy;
  c) Original analogue record: analogue document that may be the only existing one or not if, in this case, one can know its content by means of other documents whose preservation is mandatory, even if they belong to different owners;
  d) Electronic record: the electronic configuration of acts, facts or data which are legally relevant;
  e) Digital storage medium: physical medium which allows electronic records storage by means of laser technology (such as, for instance, optical disks, magnetic-optical disks, DVD);
  f) Storing: process of transposition of analogue or electronic records, signed ones included, on to any suitable medium through processing them;
  g) Electronic archiving: process of storing electronic records, signed ones included, on any suitable medium. Records must be uniquely identified by means of a reference code before any possible preservation process;
  h) Archived record: electronic records, signed ones included, which has been subjected to the process of electronic archiving;
  i) Substitute preservation: process carried out according to arts. 3 and 4 of this deliberation;
  l) Preserved record: record subjected to the process of substitute preservation;
  m) Exhibiting: operation which allows visualizing a preserved record and making a copy;
  n) Direct copying: process of transferring one or more preserved records from a storage digital medium to another one, without altering their electronic configuration *[i.e.,. conversion]*. For such a process, no special procedures are provided;
  o) Substitutive copying: process of transferring one or more preserved records from a storage digital medium to another one, altering their electronic configuration *[i.e., migration]*. For such a process, special procedures are provided as to arts. 3 and 4 of this deliberation;
  p) Time reference: information about day and time which is associated to one or more electronic records;
  q) Public officer: a notary or another authorized officer;
  r) Electronic string: bit string that can be elaborated through an electronic procedure;
  s) Message digest: predefined length bit string that is generated by applying a proper hash function to the string;
  t) Hash function: mathematical function that, starting from a generic bit string, generates a message digest in such a way that it would actually be impossible, starting from the latter, to determine a bit string which could generate it, as well as it would be impossible to determine a pair of bit strings for which the hash function could

electronic signature" and "digital signature," thus amending the previous legislation – the DPR 445/2000 in particular – where the term digital signature was generally used as a synonym for electronic signature.

generate two identical message digests [CNIPA[5]'s Deliberation 11/2004, art. 1, lets. a)–t)].

3.8.2 Preservation requirements

- Public administrations and private entities are allowed, for all legal purposes, to replace the original records in their archives, as well as all accounting records, correspondence, and any other kinds of deeds that are meant to be preserved according to the law, with their copy on any photographic or digital medium which is suitable for producing true copies [DPR 445/2000, art. 6, par. 1].
- Preservation obligations are fully satisfied, both for administrative and probative purposes, also with the use of digital media when the employed procedures comply with the technical rules provided by the Authority for Information Technology in the Public Administration (AIPA) [DPR 445/2000, art. 6, par. 2].
- Technical rules for creation, transmission, preservation, duplication, copy, and validation of electronic records are established by Prime Minister's Decree, in accord with AIPA and the Guarantor for the protection of sensitive data. In order to be abreast of technological progress, those technical rules should be updated every second year at least [DPR 445/2000, art. 8, par. 2].
- All laws and regulations concerning privacy issue are still valid [DPR 445/2000, art. 8 par. 4].
- The obligations concerning records' substitute preservation, which are provided by the current legislation as regards both public administrations and private entities, are fulfilled for any legal purpose when the preservation process is carried out according to the following arts. 3 and 4. Electronic records, signed ones included, can be electronically archived before undergoing the preservation process. This deliberation does not provide any obligations as regards electronic archiving [CNIPA's Deliberation 11/2004, art. 2].
- The process of substitute preservation of electronic records, signed ones included, and, in case, of their digests as well, consists in storing them on digital media and ends with affixing time reference and digital signature of the person responsible for preservation, testifying the proper execution of the process, on the whole of the records or on an electronic string containing one or more digests of those records or groups of them [CNIPA's Deliberation 11/2004, art. 3, par. 1].
- The process of substitute copying *[migrating]* preserved electronic records consists in storing them on another digital medium and ends with affixing time reference and digital

[5] CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) has replaced AIPA (Autorita' per l'Informatica nella Pubblica Amministrazione) in 2003. Such Authority (established in 1993 according to art. 4 of the Legislative Decree 39/1993, as amended by art. 176 of the Legislative Decree 196/2003) operates as a branch of the Council of Ministers' Presidency with the mandate to put the Ministry for Innovation and Technologies' policies into practice. In particular, CNIPA is responsible for bringing about important reforms relevant to PA's modernization, the spread of e-government and the development of nation-wide networks to allow better communication among public offices and between citizens and the State. In the Italian juridical system, CNIPA's deliberations have a lower enabling power, but they nevertheless are part of the State's body of laws. The technical rules provided in CNIPA's deliberation 11/2004 derive from art. 6, par. 2 of the DPR 445/2000, which says: "Preservation obligations are fully satisfied, both for administrative and probative purposes, also with the use of digital media when the employed procedures comply with the technical rules provided by AIPA." To keep those rules up to date according to the latest technological developments, AIPA's deliberation no. 42 of 13 December 2001 on "Technical rules for documents reproduction and preservation on digital media that are suitable to guarantee true copies of the original documents" has been replaced by the current CNIPA's deliberation.

signature of the person responsible for preservation, testifying the proper execution of the process, on the whole of the records or on an electronic string containing one or more digests of those records or groups of them. Additionally, if the process concerns signed electronic records, a public officer is required to affix time reference and digital signature, in order to testify that what has been copied *[migrated]* is a true copy [CNIPA's Deliberation 11/2004, art. 3, par. 2].

- The process of substitute preservation of analogue records consists in directly storing the relevant image and, in case, the relevant digest as well, on digital media and ends with affixing time reference and digital signature of the person responsible for preservation, testifying the proper execution of the process, on the whole of the records or on an electronic string containing one or more digests of those records or groups of them [CNIPA's Deliberation 11/2004, art. 4, par. 1].
- The process of substitute preservation of original and sole analogue records ends with further affixing of time reference and digital signature of a public officer, in order to testify that what has been copied is a true copy [CNIPA's Deliberation 11/2004, art. 4, par. 2].
- Destruction of analogue records whose preservation is mandatory is only allowed after completion of the substitute preservation procedure [CNIPA's Deliberation 11/2004, art. 4, par. 3].
- The process of substitutive copying *[migrating]* preserved analogue records consists in storing them on another digital medium. When copying *[migration]* is completed, the person responsible for preservation testifies the proper execution of the process through affixing time reference and digital signature on the whole of the records or on an electronic string containing one or more digests of those records or groups of them. If the process concerns original and sole records, a public officer is further required to affix time reference and digital signature, in order to testify that what has been copied is a true copy [CNIPA's Deliberation 11/2004, art. 4, par. 4].
- The person in charge of the preservation function has the following tasks and responsibilities:
  a) To specify the features and requirements of the preservation system according to types of records (analogue or electronic) to be preserved. To consequently organize the digital media content and to manage the security and tracking procedures which assure proper preservation, with also the purpose to allow exhibiting of each preserved record;
  b) By employing specific processing procedures according to the kinds of storage media utilized, to archive and make available the following information:
     1) content description of the whole of the records *[i.e., series description]*;
     2) data which identify the person responsible for preservation;
     3) if it is the case, data which identify the persons delegated by the responsible for preservation, with the indication of their tasks; and
     4) information about security copies.
  c) To maintain and make accessible a data bank of the software applications in use in all their different versions;
  d) To check proper functioning of the system and applications in use;

e) To take the necessary measures to guarantee the physical and logical security of the system which manages the substitute preservation process, as well as of the security copies of storage media;
f) To ask for public officer's assistance, when that is required *[In the public administrations, the public officer's role is performed by the top manager in charge of the office responsible for the preservation function – art. 5, par. 4]*;
g) To identify and document the safety measures to be observed as regards time reference affixing;
h) To check periodically, at least every 5 years, whether the preserved records are actually readable, and, when necessary, to provide for direct or substitute copying of the content of the media [CNIPA's Deliberation 11/2004, art. 5].

- Preserved records should be readable at any time through the substitute preservation system as well as be available on paper upon request. They can also be exhibited via telecom tools. Every time preserved records are exhibited on paper outside the place where the substitute preservation system is located, a public officer has to testify their authenticity, in case the preservation of those records requires his or her intervention [CNIPA's Deliberation 11/2004, art. 6].
- Taking technological developments into considerations and according to the DPR 445/2000, public administrations and private entities are allowed to use any kind of storage medium, not necessarily a digital one, which must however be suitable for guaranteeing that copies are true copies, in both substitute preservation and substitute copying *[migration]* processes [CNIPA's Deliberation 11/2004, art. 8].

  CNIPA's deliberation recognizes that preservation of authentic electronic records means preservation of authentic/true copies. Thus, the preservation process is called substitute preservation process, and the authenticity of a preserved record is not established on the object itself (as it was with traditional media), but through the authority of the preserver (and a notary, when it is the case) who would attest to the identity and integrity of the whole of the reproduced records every time a migration occurs. As regards the preserver's tasks list, describing archival units stands out as an essential activity (not replaceable by any metadata set that may be associated to each single document) with the purpose to have and maintain intellectual control over archives holdings. Unlike previous AIPA's acts, this deliberation far from being mainly concerned with merely technological specifications makes an effort to tackle more general and methodological issues.

3.8.3 Authenticity / Authentication

- Documents, records, and data created by public and private entities by means of computerized or telecom-tools, as well as contracts drawn up in the same way, and their filing and transmission via electronic devices, are valid and effective for all legal purposes. Criteria and methods on how to enforce this article will be defined in specific regulations to be issued [L 59/1997, art. 15].
- Electronic records that are created by anybody, as well as their registration on digital media, and transmission via telecom-tools, are valid and effective for all legal purposes when complying whit this regulation [DPR 445/2000, art. 8, par. 1].

- Any data or document electronically created by any public administration represents a primary and original source of information that may be used to make copies on any kind of medium for all legal purposes [DPR 445/2000, art. 9 par. 1].
- In all operations relevant to creation, transmission, preservation, and reproduction of data and documents by using computerized systems, data *[i.e., metadata]* about both the concerned administrations and the authors of such operations must be easily identifiable [DPR 445/2000, art. 9 par. 2].
- 1. An electronic record has probative value according to art. 2712 of the Civil Code with regard to the facts and things it documents;
  2. An electronic record which has been signed by means of electronic signature meets the legal requirement of the written form. As regards its probative value, the record itself is freely assessable, taking its objective quality and security features under consideration. It also fulfils all obligations as laid down in art. 2214 of the Civil Code, as well as any other similar legislative or regulatory disposition;
  3. An electronic record, when it has been signed by means of digital signature or any other kind of advanced electronic signature, and the signature is based on a qualified certificate and has been created by means of a secure-signature-creation device, represents full evidence of the provenance of its content from the person who signed it, until anybody actions for forgery *[in Italian, 'querela di falso']*;
  4. An electronic record which has been signed by means of electronic signature cannot, however, be rejected as legally irrelevant, nor its admissibility as evidence can be denied just because it has been electronically signed, or because its signature is not based on a qualified certificate, or because the signature has not been created by means of a secure-signature-creation device [Dlgs 10/2002, art. 6 – which replaces art. 10 of the DPR 445/2000].
- Contracts that are stipulated electronically or via telecom-tools and that are signed by means of qualified electronic signature according to the present rules are valid and effective for all legal purposes [DPR 137/2003, art. 4 – which replaces art. 11 of the DPR 445/2000].
- Duplicates, copies and abstracts of electronic records, also those reproduced on different kinds of media, are valid and effective for all legal purposes if they comply with the present provisions [DPR 445/2000, art. 20, par. 1].
- Electronic records containing copies or reproductions of public records, private deeds or documents in general, included any kinds of administrative records sent or received by authorized public depositories and public officers, are fully effective according to arts. 2714 and 2715 of the Civil Code, if they are associated with a qualified electronic signature [DPR 137/2003, art. 6 – which replaces DPR 445/2000, art. 20, par. 2].
- Any electronic copy of records which had originally been created on paper, have the full capacity to replace the original record if such a copy is authenticated by a notary or any other public officer authorized to make certified copies [DPR 445/2000, art. 20, par. 3].
- The obligation of preserving and exhibiting records according to the current enabling legislation is perfectly fulfilled by means of electronic records when the latter are created by following the procedures established in the technical rules [DPR 445/2000, art. 20, par. 5].

- Affixing a digital signature supplements and replaces, for any legal purposes, the use of seals, punches, stamps, countermarks and any kinds of marks [DPR 137/2003, art. 9 – which replaces DPR 445/2000, art. 23, par. 6].
- It is considered as an acknowledged digital signature, according to art. 2703 of the Civil Code, the digital signature whose affixing is authenticated by a notary or any other authorized public officer [DPR 445/2000, art. 24, par. 1].
- Authenticating a digital signature involves a public officer to attest that the digital signature has been affixed in front of him/her by the holder, against previous assessment of the latter's personal identity, of the key validity, and of the fact that the signed document corresponds to the party's will and is not in conflict with art. 28, par. 1 of L. 89/1913 [DPR 445/2000, art. 24, par. 2].
- In all electronic records created by public administrations, the original hand signature or whatever provided signature is replaced by the digital signature according to the present regulation [DPR 445/2000, art. 25, par. 1].
- Certification-service-providers have to:
  h) publish notice of the annulment or suspension of the electronic certificate upon request of the holder, in case the key has been lost, upon request of the authority, when there are limiting causes of the holder's capacity, in cases of suspicion of abuses or forgery;
  m) preserve electronic or manual recording of all information relevant to any qualified certification for ten years, with the purpose to provide evidence of such certification in case of legal proceedings;
  n) neither copy nor keep any of the private keys that have been provided the holder with;
  p) use secure systems for the management of the certification register, in order to guarantee that all entries and changes be exclusively made by the authorized individuals, the authenticity of information be verifiable, certifications be accessible to the public only when that is allowed by the holder, and the operator be in the position to know about any event that might jeopardize the security requirements.

  Instead of the holder's name, the certification-service-provider can report on the electronic certificate a pseudonym. In case of qualified certification, information relevant to the holder's real identity must be preserved for at least ten years after the expiration of the relevant certification.

  To sign electronic records of external relevance *[i.e., records which are meant to produce effects on the outside world]*, when signature is required, public administrations are allowed to either directly issue qualified certifications, after having been accredited to do so, or refer to accredited certification-service-providers.

  With reference to creating, managing and signing electronic records of solely internal relevance *[i.e., records which circulate only within the creating organization]*, each administration is allowed to autonomously adopt its own internal rules.

  The differentiation between internal and incoming/outgoing records, which is related to the complexities and costs of such a certification system, may impact on the long term preservation of heavy-signed and light-signed records and poses questions about different records legal values and organizations' accountability.

  The certification-service-provider that intends to close down must inform the Innovation and Technology Department no later than sixty days before the cut-back date. He has to contextually communicate either the name of the certification-service-provider

that will take over his documentation or the cancellation of that documentation. The certification register and relevant documentation must be transferred to other depository [DPR 137/2003, art. 15 – addendum to DPR 445/2000].

3.8.4 Organizational and records management issues

- All public administrations have to implement or revise existing electronic records management systems according to the present law by January 1, 2004 [DPR 445/2000, art. 50 par. 3].
- Within each public administration, homogeneous organizational areas ('Aree Organizzative Omogenee (AOO)'), where common or coordinated management of records is recommendable, have to be identified. To assure uniformity, common criteria for classifying and archiving records must be implemented in each of the identified AOO [DPR 445/2000, art. 50 par. 4].
- Electronic systems to be implemented by the public administrations should be targeted to the complete automation of the whole records life cycle [DPR 445/2000, art. 51 par. 2].
- Public administrations have to evaluate costs and benefits of digitization of those paper-based records whose preservation is either mandatory or recommendable. Consequently, they also provide plans for the replacement of paper-based archives with electronic ones [DPR 445/2000, art. 51 par. 3].
- Electronic records management systems must: a) guarantee system security and integrity; b) guarantee accurate and timely registration of all incoming and outgoing records ('registrazione di protocollo'); c) provide information about the link between each received record and all other records created or received by the administration in the course of the business activity those records refer to (i.e., the "archival bond"); d) allow retrieval of all information relevant to the registered records; e) allow any interested people to have secure access to all information which is stored in the system, according to sensitive data protection and privacy laws; f) guarantee the right arrangement of records within the adopted archival classification system [DPR 445/2000, art. 52 par. 1].
- Public administrations should ensure the interoperability of their electronic records management systems, in the frame of the public administration unitary network ('Rete Unitaria delle Pubbliche Amministrazioni') [DPR 445/2000, art. 60 par. 1].
- In order to guarantee integrity of the data entered in the electronic protocol register, the content of the latter should be daily copied on non-rewritable electronic media. Such a copy should be kept by a different person from the one responsible for the records management and archives service [DPCM 31 October 2000, art. 7, par. 4].

3.9 Evidence act (excerpts from the Italian Civil Code)

- Registry Office Records
  - Records issued by the Registry Office fully prove what the public officer attests to be happened in front of him/her or to be done by him/her, until anybody actions for forgery ('querela di falso'). Witnesses' declarations make proof to the contrary [art. 451].
  - In case either the registers have not been kept or have been destroyed or lost, or, for any other reason, the registration of the act is completely or partially missing, birth or

death proof can be given by any means. In case of absence, partial or total destruction, manipulation or concealment due to the requester's fraudulent intention, the latter is not admitted to the proof as above [art. 452].
  - No annotation can be made on any record that has already been registered, unless such annotation had been provided by law or ordered by the judicial authority [art. 453].
  - Amendments on civil status records must be ordered via final judgement of the court to the public officer. The latter can be ordered either to correct an existing record or to enter an omitted one in the register, or to remake a record which has been lost or destroyed. Such final judgements must be recorded in the registers [art. 454].
- Land Registry Office Records
  - The party who wants to register a contract must provide the Land Registry officer with either a certified copy, in case of public records or sentences, or the original, in case of private deeds, unless the latter has been deposited in a public archives or at a notary. In this case, a true copy signed by either the archivist or the notary is enough [art. 2658].
  - The Land Registry officer must issue copies of the registration entries and annotations – or a certificate which states that there is no registration or annotation – to anybody asking for them. (…) He or she also must issue copies of the original records that have been deposited at the Land Registry or of those records whose originals have been deposited at a notary or in a public archives, both located outside the jurisdiction of the Land Registry [art. 2673].
  - In case of differences among the register entries and what is stated in the copies or in the certificates issued by the Land Registry officer, the content of the registers prevails [art. 2676].
- A public record[6] fully proves the provenance of a record from the public officer that has created it, and is evidence of parties' declarations and any other facts which the public officer attests to be happened in front of him/her or to be done by him/her, until anybody actions for forgery [art. 2700].
- A record which has been created by an incompetent or unable public officer, or which is not compliant with the required formal elements, if it has been signed by the parties, has the same probative value as that of a private deed [art. 2701].
- A private deed fully proves the provenance of the declarations from the person who has signed it, if the signature either is recognized by whom the deed has been made against or is legally ascertained, until anybody actions for forgery [art. 2702].
- Signature authentication[7]: The law recognizes the signature that has been authenticated by a notary or any other authorized public officer. Authentication involves the public officer attesting that the signature has been affixed in front of him/her. The public officer must ascertain the identity of the signatory beforehand [art. 2703].
- Probative value of mechanical copies[8]: Photographic or cinematographic copies, phonographic recordings and in general any other mechanic representations of facts and things, fully prove the facts and things they document, if the person against whom those

[6] For the definition of public record according to art. 2699, see at section a).
[7] As regards electronic signature authentication, see DPR 445/2000, art. 24 at section h.3).
[8] For the extension of this article to electronic records and copies of electronic records, see Dlgs 10/2002, art. 6 and DPR 445/2000, art. 20, at section h.3).

copies are introduced does not deny that they correspond to those facts and things [art. 2712].

- Copies of public records that are sent from authorized public depositories according to the prescribed forms have the same probative value as that of the original. The same probative value is also recognized to the copies of the copies of original public records that are sent from authorized public depositories [art. 2714].
- Copies of private deeds which are deposited in public offices and are sent from authorized public depositories have the same probative value as that of the original record they are made from [art. 2715].
- In case of absence of the original public record or a copy of it in a public depository, the copies that have been sent according to art. 2714 have full probative value. However, if such copies, as well as an existing copy of a missing original which is kept by a public depository, show deletions, erasures, insertions or any other external defects, it is up to the judge to weigh their probative value. The same principle applies to private deeds [art. 2716].
- Copies made by public officers outside the above mentioned cases have the value of written presumptive evidence [art. 2717].
- Incomplete copies or abstracts which are made according to the prescribed form by authorized public officers, who are the depositories of the originals, have full probative value only with regard to the portion of the original they literally reproduce [art. 2718].
- Photocopies of records or deeds have the same probative value as that of true copies, if the fact that they are compliant with the original is attested by a competent public officer or it is not explicitly unrecognized [art. 2719].
- Ascertainment or renovation records fully prove the content of the original record, if one does not demonstrate, by showing the latter, that a mistake was made in the ascertainment or renovation [art. 2720].
- Account books and other documentation: Entrepreneurs are obliged to preserve account books and inventories. They also have to keep any other account documentation and, in an orderly way for each business transaction, preserve the originals of every received letter, telegram and invoice, as well as the copies of every sent letter, telegram and invoice. All these rules do not apply to minor entrepreneurs [art. 2214].
- Testimonial evidence with regard to contracts is not admissible when the object's value exceeds Euro 2.58. However, the judicial authority may allow testimonial evidence below the above-mentioned limit taking into consideration the parties' quality, the nature of the contract and any other circumstance [art. 2721].
- Testimonial evidence is not admissible when it refers to agreements which have been added to or are against the content of a record, and which have been stipulated beforehand or contemporaneously [art. 2722].
- If an added or opposite agreement that was stipulated after the creation of a record is introduced, the judicial authority can admit testimonial evidence only if, after considering the parties' quality, the nature of the contract and any other circumstance, it looks likely that additions or changes to the record have been made [art. 2723].
- Testimonial evidence is always admissible when:
  1) a written evidence basis exists: that is, any written document made by the inquired person which supports the facts;
  2) the contracting party could not morally or physically get a written evidence; or

3) the contracting party has guiltlessly lost the record that was his/her evidence [art. 2724].

- When, according to the law or parties' will, a contract must be proved in writing, testimonial evidence is only allowed according to no. 3 of the before mentioned article. The same rule applies when the written form is necessary to not incur the nullity of a deed [art. 2725].
- Presumptions of law exempt from any evidence those in whose favour they are established. Evidence to the contrary cannot be given against those presumptions on which basis the law declares invalid certain documents or when lawsuit is not admissible [art. 2728].
- Simple presumptions, i.e., presumptions which are not established by the law are left to the judge's prudence. The judge can only admit serious, detailed and consistent presumptions. In such cases when the law does not admit testimonial evidence, presumptions cannot be admitted as well [art. 2729].

4. List of the Legislative Sources Covered in the Report

- **Legislative Decree No. 42/2004 of 22 January 2004**: "**Code Regarding Cultural and Environmental Heritage"** ('Codice dei beni culturali e del paesaggio') - http://wwwdb.archivi.beniculturali.it/download.aspx?chiave=467&tabella=UNITARIA
- **National Centre for Information Technology in the Public Administration (CNIPA)'s Deliberation No. 11/2004 of 19 February 2004: "Technical Rules for Reproducing and Preserving Documents on Digital Media which are Suitable to Guarantee the Production of True Copies"** ('Regole techiche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformita' dei documenti agli originali') - http://wwwdb.archivi.beniculturali.it/download.aspx?chiave=469&tabella=UNITARIA
- **Legislative Decree No. 196/2003 of 30 June 2003: "Code Regarding Personal Data Protection - Privacy"** ('Codice in materia di protezione dei dati personali') - http://wwwdb.archivi.beniculturali.it/download.aspx?chiave=458&tabella=UNITARIA
- **President of the Republic's Decree No. 137/2003 of 7 April 2003: "Regulation on Coordination Provisions in Matter of Electronic Signature According to Art. 13 of the Legislative Decree No. 10 of 23 January 2002"** ('Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislative 23 gennaio 2002, n. 10') - http://www.interlex.it/testi/dpr03_137.htm
- **Legislative Decree No. 10 of 23 January 2002: "Acknowledgement of the EU Directive No. 1999/93/CE on a Community Framework for Electronic Signature"** ('Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche') - http://wwwdb.archivi.beniculturali.it/download.aspx?chiave=435&tabella=UNITARIA
- **Authority for Information Technology in the Public Administration (AIPA – today's CNIPA)'s Circular No. 28 of 7 May 2001: "Technical Rules for the Application of the DPR No. 445/2000: Standards, Transmission Procedures, Formats, and Definitions of the Kinds of Minimum and Additional Information that Are Commonly Exchanged Among Public Administrations and Are Associated to Registered Records"** ('Regole tecniche per l'applicazione del DPR 445/2000: Standard, modalita' di trasmissione, formato e definizione dei tipi di informazioni minime ed accessorie comunemente scambiate tra le pubbliche amministrazioni ed associate ai documenti protocollati') – http://wwwdb.archivi.beniculturali.it/download.aspx?chiave=243&tabella=UNITARIA
- **President of the Republic's Decree No. 445/2000 of 28 December 2000: "Single Text of Legislative and Regulatory Provisions Regarding Administrative Documentation"** ('Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa') - http://www.unipd.it/ammi/archivio/2000_445.htm
- **Prime Minister's Decree of 31 October 2000: "Technical Rules for the Electronic Protocol Register According to the DPR No. 428/1998"** ('Regole tecniche per il protocollo informatico di cui al DPR 20 ottobre 1998, n. 428') - http://www.unipd.it/ammi/archivio/2000_dpcm.htm

- **Legislative Decree No. 135 of 11 May 1999: "Integrative Provisions of the Law 675/1996 on Public Bodies' Sensitive Data Management – Privacy Law"** ('Disposizioni integrative della L. 675/1996 sul trattamento dei dati sensibili da parte dei soggetti pubblici') - http://www.lexitalia.it/dlvo_1999-135.htm
- **President of the Republic's Decree No. 513 of 10 November 1997: "Regulation on the Criteria and Procedures for Creating, Registering, Filing, and Transmitting Documents by Means of Electronic and Telecommunication Systems According to Article 15, Paragraph 2, of the Law No. 59/1997"** ('Regolamento recante criteri e modalita' per la formazione, l'archiviazione e la trasmissione di documenti informatici e telematici, a norma dell'articolo 15, comma 2 della Legge 59/1997') - http://wwwdb.archivi.beniculturali.it/download.aspx?chiave=111&tabella=UNITARIA
- **Law No. 59 of 15 March 1997: "Delegation of Powers to the Government as regards the Transfer of Functions and Tasks to Regions and Local Authorities, in the Frame of the Public Administration Reform and the Process of Administrative Simplification"** ('Delega al Governo per il conferimento di funzioni e compiti alle Regioni ed Enti Locali, per la riforma della PA e per la semplificazione amministrativa') - http://wwwdb.archivi.beniculturali.it/download.aspx?chiave=104&tabella=UNITARIA
- **Legislative Decree No. 39 of 12 February 1993: "Dispositions Regarding Automated Information Systems of the Public Administrations According to Article 2 of the Law No. 421/1992"** ('Norme in material di sistemi informative automatizzati delle amministrazioni pubbliche, a norma dell'art. 2 della L. 421/1992') - http://www.giustizia.it/cassazione/leggi/dlgs39_93.html
- **President of the Republic's Decree No. 352 of 27 June 1992: "Regulation on Executive Procedures for Allowing and Restricting Access Rights to Administrative Documents According to Article 24 of the Law No. 241/1990 Concerning New Rules on Administrative Procedures and Access Rights to Administrative Documents"** ('Regolamento per la disciplina delle modalita' di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24 della L. 241/1990, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi') - http://www.unipd.it/ammi/archivio/992_352.htm
- **Law No. 241 of 7 August 1990: "New Dispositions on Administrative Procedures and Access Rights to Administrative Documents"** ('Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi') - http://www.unipd.it/ammi/archivio/990_241.htm
- **President of the Republic's Decree No. 1409 of 30 September 1963: "Dispositions on Organizational Structure and Personnel of the State Archives"** ('Norme relative all'ordinamento ed al personale degli Archivi di Stato') - http://www.uinipd.it/ammi/archivio/963_1409.htm
- **Royal Decree of 16 March 1942: "Approval of the Civil Code Text"** ('Approvazione del testo del Codice Civile') - http://www.jus.unitn.it/cardozo/Obiter_Dictum/codciv/Codciv.htm