ARTICLE:

Electronic signatures in Italian law

By **Aniello Merone**

This paper aims to provide an overview on the different types of electronic signature in Italy and how they affect the value and evidential effectiveness of an electronic document in Italian law. The focus is on the debate concerning the compatibility between electronic signatures and the judicial response in case law when dealing with articles 214 – 220 of the Codice di Procedura Civile (Civil Procedural Code).

Preamble

Italy was one of the first countries in the world to equate the legal effects of an electronic document, subscribed with a digital signature, to documents written and subscribed on paper. Article 15, § 2 of Law 59/1997[1] introduced the fundamental principle of equivalence between paper and electronic documents:

> Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge.
>
> The acts, data and documents drawn up by the government and by individuals with electronic tools, the contracts entered into in the same form, as well as their storage and transmission by electronic means, are valid and relevant to all intents and purposes of law.

This legislation served to enable information technology to be used to improve efficiency in the public administration,[2] but its implementation has proceeded very slowly.[3]

The legislative position is controlled by the Codice dell'Amministrazione Digitale (Digital Administration Code, (CAD)), introduced into law by Law Decree 82/2005.[4] The CAD aims to provide a systematic regulation of the exchange of digital information between public administrations; the storage of electronic documents; the creation of a national network, and electronic documents and signatures. Article 10 of Law n. 229/2003[5] established the guidelines for the CAD regulations, and sets out the aims, as follows:

> garantire la più ampia disponibilità di servizi resi per via telematica dalle pubbliche amministrazioni e dagli altri soggetti pubblici e di assicurare ai cittadini e alle imprese l'accesso a tali servizi secondo il criterio della massima semplificazione degli strumenti e delle procedure necessari e nel rispetto dei principi di eguaglianza, non discriminazione e della normativa sulla riservatezza dei dati personali.
>
> ... ensure the widest availability of informatic services by governments and other public entities and to guarantee to citizens and businesses access to such services in

[1] Legge 25 marzo 1997, n.59 *Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa* (Gazz. Uff. n. 63 del 17 marzo, Suppl. ordinario n. 56/L). This law delegates powers to the Council of Ministers to provide rules and regulations to reform public administration and simplify procedures.

[2] *Growth, competitiveness, employment – The challenges and ways forward into the 21st century*, White Paper (Bulletin of the European Communities, Supplement 6/93, COM (93) 700, 5 December 1993) under the chairmanship of Jacques Delors, identified in Information and Communication Technology (ICT) the economy sector with the highest rates of growth in Europe. Later it was developed in a follow-up paper: *Report on Europe and the global information society Recommendations of the high-level group of the information society to the Corfu European Council* (Bangemann group), (Bulletin of the European Union, Supplement 2/94, 1994), where it was suggested that there was a need to provide 'absolute guarantees in areas such as the integrity of signatures' (p. 22). See Ruggero Paladini, 'Il Libro bianco: principali indicazioni e possibili implicazioni economiche', *Rivista giuridica del lavoro e della previdenza sociale*, 1994, pp 87 – 97.

[3] See Marina Pietrangelo, *La società dell'informazione tra realtà e norma*, (Milano: Giuffrè, 2007), pp 43 – 63.

[4] Decreto Legislativo 7 marzo 2005, n. 82 *Codice dell'amministrazione digitale* (Gazz. Uff. n.112 del 16 maggio, Suppl. ordinario n. 93).

[5] Legge 29 luglio 2003, n. 229, *Interventi in materia di qualità della regolazione, riassetto normativo e codificazione – Legge di semplificazione 2001* (Gazz. Uff. n. 196 del 25 agosto 2003).

accordance with maximum simplification of tools and procedures, in respect of principles of equality and non-discrimination and pursuant regulations on the confidentiality of personal data.[6]

However, the CAD has been amended several times in less than ten years.[7] These continuous changes have fostered uncertainty, discouraging the use of renunciation and verification proceeding against electronic signatures and delaying the evolution of jurisprudence on this topic.[8] Given these premises, this paper will provide an overview how different types of electronic signatures, in the present regulatory framework, provides for value in law and evidential effectiveness of documents in electronic format.

The regulatory framework

A series of changes to the regulatory provisions have entered into force in the last fifteen years, and they have shown an evident uncertainty by the Italian legislator in working with terms defined by information technology from the outset.[9]

The early provisions

At the beginning, Presidential Decree n. 513/1997[10] established 'criteria and modalities for implementation' of the equivalence between an electronic document subscribed with a digital signature and a document with a handwritten signature.[11] For this purpose, article 5 provided the electronic signature with the same effectiveness as provided by article 2702 of the Codice civile (Civil Code) (CC) for the handwritten signature.[12] The 1997 Regulation was subsequently replaced by Presidential Decree n. 445/2000,[13] which brought the rules governing electronic documents in line with the legislation concerning digital signatures without losing the consistency of new system based on the full equivalence of the digital signature to the manuscript signature.

The EU directive

The EU Directive[14] caused changes to be made to the Italian legislation. The Directive aimed at facilitating the use of electronic signatures and contributed to their legal recognition within the Member States of the European Union. To this purpose, the provisions of the Directive are based on the principle of technological neutrality, which prohibits the national legislator from influencing – even indirectly, with reference to technical standards adopted by specific

[6] See Nicola Lugaresi, 'Codice dell'amministrazione digitale e rapporti tra cittadino e Pubblica Amministrazione', in *Giustizia amministrativa*, 2006, pp 460 466; Elena D'Orlando, 'Profili costituzionali dell'amministrazione digitale', in *Diritto dell'informazione e dell'informatica*, 2011, 2, pp 213 – 219.

[7] Since entering into force by Decreto legislativo 4 aprile 2006, n. 159 *Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale* (Gazz. Uff. n. 99 del 29 aprile 2006, Suppl. ordinario n. 105), and Decreto legislativo n. 235 del 30 dicembre 2010, *Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69* (Gazz. Uff. n. 6 del 10 gennaio 2011, Suppl. Ordinario n. 8); iii) Legge 17 dicembre 2012, n. 221, *Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese* (Gazz. Uff. n. 294 del 18 dicembre 2012, Suppl. Ordinario n. 208).

[8] To date, the Supreme Court has not ruled on the provisions of art. 20 and 21 of the CAD and judgments rendered by the courts of the merit of actions regarding this topic are rare.

[9] According to Giusella Finocchiaro, 'Riflessioni su diritto e tecnica', *Diritto dell'informazione e dell'informatica*, 2012, pp 831 – 840, p 835. However, as noted by Stephen Mason, *Electronic Signatures in Law* (3rd edn, Cambridge University Press, 2012), pp 100, 198, the authority for the use, application, and proof of electronic signatures remains in legal principles and not in technology or systems theory.

[10] Decreto del Presidente della Repubblica 10 novembre 1997, n. 513, *Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59* (Gazz. Uff. n. 60 del 13 marzo 1998).

[11] Further technical regulations for the creation, transmission, storage, duplication, reproduction and validation, even temporarily, of electronic documents was established by Decreto del Presidente del Consiglio dei Ministri 8 Febbraio 1999, *Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513* (Gazz. Uff. n. 87 del 15 aprile 1999).

[12] Article 2702 provides: 'La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa e legalmente considerata come riconosciuta' 'The private writing has effectiveness of proof, unless a declaration of false, in relation to the origin of the statements by those who have signed it, if the one against whom the writing is produced acknowledges the subscription, or if this is legally considered as recognized'. See Salvatore Patti, 'L'efficacia probatoria del documento informatico', *Rivista di Diritto processuale,* 2000, pp 60 – 92; Giusella Finocchiaro, 'Il valore probatorio del documento informatico e firma digitale', in *Contratto e impresa*, 2002, pp 76 – 85; on this review, Franco Ruggeri, 'A technician's views on the digital signature in Italy', *Digital Evidence and Electronic Signature Law Review*, 2 (2005), 39 – 45, pp 41 – 43.

[13] Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* (alla Gazz. Uff. n. 42 del 20 febbraio 2001, Suppl. ordinario n. 30).

[14] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13, 19.01.2000, p 12.

products – the free movement of goods and services that can be used for electronic signatures.[15]

The Directive introduced the concept of an 'electronic signature', defined, in article 2 § 1 as: 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'. Another form of electronic signature, the 'advanced electronic signature' is provided for in article 2 § 2, and described as an electronic signature, which sets out a number of characteristics relating to performance.[16] The 'advanced electronic signature' means 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 the data is detectable.

This definition refers to electronic signatures based on a public key infrastructure and the use of cryptographic tools (private and public keys) for the signing and verification of electronic documents: that is, digital signatures that are capable of providing a number of functions, such as declarative and indicative functions, in relation to the signing of a document. However, the use of such a signature does not prove that the writer affixed the signature to the document, nor can it be related uniquely to the signing party.[17]

Article 5 § 1 provided that only electronic signatures based on a qualified certificate and created by a secure signature device could be equated, under the legal requirements, to a written signature. In this way, such a signature cannot be denied its legal value and acceptance as evidence in legal proceedings. Article 5 § 2 required Member States to adopt of further measures to ensure '... that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the fact that it is in electronic form, or not based on a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure signature creation device'.

The Italian transposition of the Directive

In Italy, the legislation implemented before the adoption of the Directive referred exclusively to public-key encryption. This meant it was necessary to recognize other forms of electronic signature, such as data combinations (a personal identifier associated with a password used to gain access to computer systems); typing a name in an electronic document; the Personal Identification Number (PIN); the name in an e-mail address and a manuscript signature that has been scanned, amongst others.[18]

On 2 March 2002, Legislative Decree n. 10/2002 entered into force.[19] This decree transposed the provisions of the Directive and replaced article 10 of Presidential Decree n. 445/2000, signalling significant changes to the regulation of electronic signatures.[20] In particular the revised article 10L[21] remained in force until 31 December 2005 and prevented the denial of an electronic document subscribed with a digital signature. As a result, greater probative effectiveness was assigned to such documents than a document written and subscribed on paper.[22] Consequently, the

[15] However, Ugo Bechini, 'The Digital Tower of Babel', *Digital Evidence and Electronic Signature Law Review*, 5 (2008), pp 183 – 186, p 183 critically observes: "In fact, each country seems to have adopted a different kind of signature. No less than seven different formats are currently in use (.cms .pkcs7.pdf .p7m .p7s .xml .odt). Italian software, for instance, cannot read digital signatures from France. Even when the extension is the same, there are slight implementation differences that make interoperability a hazy dream".

[16] As noted by Stephen Mason, *Electronic Signatures in Law*, p 118.

[17] *Electronic Signatures in Law*, pp 118 – 120.

[18] For complete list, together with most relevant case law from various jurisdiction, see *Electronic Signatures in Law*, pp 187 − 258.

[19] Decreto Legislativo 23 gennaio 2002, n. 10 *Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche* (Gazz. Uff. n. 39 del 15 febbraio 2002).

[20] On this topic, see Cesare Massimo Bianca, 'La firma elettronica, si apre un nuovo capitolo', *Studium juris*, 2002, pp 1431 – 1434; Francesco Delfini, 'Il d.lgs. n. 10/2002 di attuazione della direttiva 1999/93/CE in tema di firme elettroniche', *I Contratti*, 2002, pp 410 – 413.

[21] Article 6 of Legislative Decree no. 10/2002 amended Article 10 of Presidential Decree n. 445/2000, providing, in article 10L(3): 'Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto' 'The computer document, when it is signed with a digital signature or with another type of advanced electronic signature, and the signature is based on a qualified certificate and created by a device for creating a secure-signature does [...] is full proof of the origin of the statements by those who have signed'.

[22] Luigi Martin and Roberto Pascarelli, 'Electronic signature: value in law and probative effectiveness in the Italian legal system', *Digital Evidence and Electronic Signature Law Review*, 1 (2004), pp 19 – 24; pp 22 – 23.

rule was severely criticized by the scholars[23] because it failed to provide for the idea of full equivalence as imposed by the Directive.

The adoption of Digital Administration Code and following amendments

The Digital Administration Code[24] revised the legislation,[25] in accordance with the principle and guidelines stated by Law n. 229 of 2003.[26]

The rules on electronic documents and electronic signatures were merged in the CAD text, which entered into force on 1 January 2006. The purpose was to provide for a legal framework for their use public in the administration and between the citizen and business.

However, it possible to identify some clear inconsistencies: first, the introduction of four types of electronic signatures. To the 'electronic signature' and 'advanced electronic signature' are (inexplicably) added a 'qualified electronic signature' and a 'digital signature'. The first added a 'qualified certificate' to the definition of 'advanced signature' offered by the EU Directive; the latter is characterized by 'system of cryptographic keys, one public and one private, related to each other'.

Furthermore, a few months after its entry into force, the CAD was changed significantly by Legislative Decree n. 159 of 2006.[27] An entire chapter was added, dedicated to public networking, and articles 20 and 21, dedicated to the fundamental issue of the probative value of an electronic document, were rewritten. The amendments to the latter provisions have extended the free evaluation of the court to the integrity and immutability, as well as quality and safety, of electronic documents signed with an electronic signature (art. 21, § 1), and introduced a 'presumption of subscription' (article 21, §2) intended to have serious consequences in terms of the disowning and verification of the signature:

> L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria.
>
> It is assumed that the person in possession of the signature device is the person that affixes a signature, unless he proves otherwise.

Subsequently, article 14 of Legislative Decree n. 235 of 2010[28] replaced the heading of article 21 of the CAD in *Documento informatico sottoscritto con firma*

[23] See Francesco Ricci, *Scritture private e firme elettroniche*, (Roma: Luiss University Press, 2003), pp 163 – 176; Andrea Graziosi, 'La nuova efficacia probatoria del documento informatico', *Rivista trimestrale di diritto processuale civile*, 2003, pp 53 – 80, pp 61 – 73.

[24] For a commentary of the Digital administration code, see Giovanni Duni, 'Amministrazione digitale', *Enciclopedia del diritto. Annali*, *I [Accertamento – Tutela]*, (Milano: Giuffrè, 2007), pp 13 – 47.

[25] Further and prior modifications were introduced by Legge 16 gennaio 2003, n. 3 *Disposizioni ordinamentali in materia di pubblica amministrazione* (Gazz. Uff. n. 15 del 20 Gennaio 2003 – Suppl. ordinario n. 5), from Decreto del Presidente della Repubblica 7 aprile 2003 n. 137, *Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10* (Gazz. Uff. n. 138 del 17 giugno 2003), which affected the rules relating to the certification of keys and amend definitions provided by article 1. This confused jumble of amendments and new rules appear as an effect of the absence of coordination, due to the suppression of Autorità per l'Informatica nella Pubblica Amministrazione (Authority for Information Technology in Public Administration) (AIPA) and the continuous shift of its competences. Indeed, AIPA was replaced by Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali* (Gazz. Uff. n. 174 del 29 luglio 2003 – Suppl. ordinario n. 123) in Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA, data store at http://archivio.cnipa.gov.it), that in turn was replaced by Decreto legislativo 1 dicembre 2009, n. 177, *Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione, a norma dell'articolo 24 della legge 18 giugno 2009, n. 69* (Gazz. Uff. n. 290 del 14 dicembre 2009) in Ente nazionale per la digitalizzazione della pubblica amministrazione (DigitPA, data store at http://archivio.digitpa.gov.it), which was further suppressed and replaced by Decreto legge n. 83/2012, *Misure urgenti per la crescita del paese* (Gazz. Uff. n. 147 del 26 giugno 2012, Suppl. ordinario n. 129), in Agenzia per l'Italia digitale (http://www.agid.gov.it/). The absence of coordination seems confirmed, amongst other things, by the many inaccuracies contained in the provisions on Civil Telematic Trial (*Processo civile telematico*) introduced by Decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, *Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti* (Gazz. Uff. n. 89 del 17 aprile 2001), which was largely grounded on provisions included in Decreto del Presidente della Repubblica 10 novembre 1997, n. 513, *Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59* (Gazz. Uff. n. 60 del 13 marzo 1998), which in turn was repealed by Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* (Gazz. Uff. n. 42 del 20 febbraio 2001, Suppl. Ordinario n. 30).

[26] Legge 29 luglio 2003, n. 229, *Interventi in materia di qualità della regolazione, riassetto normativo e codificazione. – Legge di semplificazione 2001* (Gazz. Uff. n.196 del 25 agosto 2003).

[27] Decreto legislativo 4 aprile 2006, n. 159, *Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale* (Gazz. Uff. n. 99 del 29 aprile 2006, Suppl. ordinario n. 105).

[28] Decreto legislativo n. 235 del 30 dicembre 2010, *Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69* (Gazz. Uff. n. 6 del 10 gennaio 2011, Suppl. Ordinario n. 8).

elettronica (Electronic document subscribed with an electronic signature) and amended § 2 of article 21, extending the effectiveness of article 2702 of the Civil Code, previously assigned only when a digital or qualified electronic signature was used, to any 'electronic document subscribed with an advanced, digital or qualified electronic signature, [...] that ensure identifiably of the author, integrity and immutability of the document':

> Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile.
>
> The electronic document signed with an advanced electronic signature, qualified or digital format in compliance with the technical requirements laid down in article 20, paragraph 3, to ensure the identifiability of the author, integrity and immutability of the paper, the effectiveness under article 2702 of the Civil Code.

Furthermore, article 14 of Legislative Decree n. 235 of 2010 added paragraph 2 *bis* to article 21, that expressly identified which electronic documents meet the requirements of written form as provided by article 1350, of the Civil Code, as follow:

> Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.
>
> Except as provided in article 25, the private writings referred to in article 1350, first paragraph numbers from 1 to 12 of the Civil Code, if done with a computer document, shall be signed, under penalty of nullity, with a qualified electronic signature or with a digital signature.

Law n. 221 of 2012[29] has again set out detailed provisions concerning value in law and the probative effectiveness of electronic documents. These modifications have further amended the regulation in force. The changes will be considered below.

Electronic document

The definition of electronic document set out in article 1(p) of the CAD is 'documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti' 'computer document: the informatic representation of acts, facts or legally relevant data'. Arguably, this definition is not sufficiently detailed. With a few adjustments, it refers to the traditional definition of document (such as 'representation of relevant acts or facts'[30]) and to the 'representative' theory accepted by the Civil Code.[31] However, a proper examination of the topic needs to consider the electronic document as a document comprising digital data that requires hardware and software to exist.[32]

Electronic document and its material support

Contrary to what is imagined by some scholars,[33] the electronic document (or more accurately, data in digital format) requires material support. While the traditional document is recorded on paper, the electronic document is stored on different types of hardware available in alternative formats, such as

[29] Legge 17 dicembre 2012, n. 221 *Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese* (Gazz. Uff. n.294 del 18 dicembre 2012, Suppl. Ordinario n. 208).

[30] See Francesco Carnelutti, 'Documento e negozio giuridico', in *Rivista di diritto processuale*, 1926, I, pp 181 – 220; Emilio Betti, *Diritto processuale civile italiano*, (2nd edn, Roma, 1936) p 356.

[31] An in-depth discussion on the legal nature and function of the document will exceed, of course, the limits of this paper. For a survey of the traditional Italian doctrine on the document see Luigi Carraro, *Il diritto sul documento*, (Padova: CEDAM, 1941); Paolo Guidi, *Teoria Giuridica del documento*, (Milano: Giuffrè, 1950); Francesco Carnelutti, 'Documento (Teoria moderna)', *Novissimo Digesto italiano*, VI, (Torino: Utet, 1957), pp 85 – 89; Aristotele Morello, 'Sottoscrizione', *Novissimo Digesto italiano*, XVII, (Torino: Utet, 1957), pp 1003 – 1014; Carlo Angelici, 'Documentazione e documento (Diritto civile)', *Enciclopedia giuridica*, XIII, (Roma: Treccani, 1989) pp 1 – 9; Salvatore Patti, 'Documento', *Digesto delle discipline privatistiche*, *sezione civile*, VII, (Torino: Utet, 1994), pp 1 – 13.

[32] As widely indicated by Burkhard Schafer and Stephen Mason, chapter 2 'The characteristics of electronic evidence in digital format' in Stephen Mason, general editor, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012).

[33] Paolo Tonalini, *La sottoscrizione elettronica dei documenti*, in *Studium juris*, 1997, p 442; Giorgio Rognetta, *La firma digitale e il documento informatico*, (Napoli: Simone 1999), p 165 – 169; Gianluigi Ciacci, *La firma digitale*, (Milano: Il Sole 24ore, 1999) p 77; Alfonso Masucci, 'Il documento informatico. Profili ricostruttivi della nozione e della disciplina', *Rivista di diritto civile*, 2004, pp 749 – 786, pp 755 – 759; Manlio Cammarata and Enrico Maccarone, *La firma digitale sicura*, (Milano: Giuffrè, 2003), p 55.

magnetic disks (floppy disk), optical disks (CD-ROM - DVD-ROM drive) and hard disks.

In order to ensure and preserve the testimony of a fact (such as the payment of an obligation) or to form a relevant act (such as a statement or a contract) the document will always be stored on hardware – that is a physical element – media on which the data is recorded.[34] Regardless of the medium upon which a document is recorded, as well as its declarative or narrative function, a document must be able to be stored through intelligible signs and in such a way that it is not altered.

With reference to an electronic document, the data are stored through binary language. This sequence of *bits* would be evanescent and not readable without software capable of representing text in human-readable form.[35] Therefore, an electronic document cannot exist without hardware and software,[36] and the definition of article 1(p) could be completed as follows: 'an electronic document is a set of digital data,[37] written in a form that can be read by software, for the informatic representation of acts, facts or legally relevant data'.

Different type of electronic documents

It is possible to distinguish between 'reproduction' and 'writings' with reference to electronic documents.[38] Informatic reproduction of a document that portrays a fact is covered in article 2712 of the Civil Code, entitled Mechanical reproductions ('Riproduzioni meccaniche'), which provides as follows:

> Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.
>
> The photographic or cinematographic reproductions, the phonographic registrations and, in general, each other mechanical reproduction of facts or things are full evidence of the facts and things represented, if the person to whom they are produced does not disown their agreement with the same facts and things.

Informatic reproduction is an electronic document without a signature, and its suitability to satisfy the requirement of written form and its probative value is freely assessable by a judge in view of its objective characteristics of quality, safety, integrity and immutability, as previewed by article 20, § 1 *bis* of the CAD:

> L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.
>
> The suitability of the electronic document to satisfy the requirement of written form and its probative value is freely assessable in judgment, in view of its objective characteristics of quality, safety, integrity and immutability, without prejudice to the provisions of article 21.

[34] Natalino Irti, 'Forma del contratto e prova', in *Le prove nel diritto civile e tributario*, edited by Cesare Glendi, Salvatore Patti and, Eugenio Picozza, (Torino: Giappichelli, 1986), p. 33, observes: "… the signs are always incorporated, for physical needs, in something representative".

[35] F. Ricci, 'Firma Digitale', *Diritto Civile*, edited by Silvio Martuccelli and Valerio Pescatore, (Milano: Giuffrè, 2011), p 784, observes: 'all documented information not only express concepts but also binary system magnitudes and, therefore, can be measured and correlated with each other.'

[36] An electronic document (digital data) cannot exist without hardware and software, and it does not matter what form of hardware the data is stored on. Anyway, the specificity of the electronic document cannot be exhausted because of the peculiarities of the material support. See Stephen Mason, *Electronic Signatures in Law*, p 6. On the systematic classification of electronic documents, see Renato Clarizia, *Informatica e conclusione del contratto*, (Milano: Giuffrè, 1985), p 100; Renato Borruso, *Computer e diritto. Problemi giuridici dell'informatica*, II, (Milano: Giuffrè, 1988), p 218; Mauro Orlandi, *La paternità delle scritture – sottoscrizione e forme equivalenti*, (Milano: Giuffrè, 1997), p 97; Ettore Giannantonio, 'Il valore giuridico del documento elettronico', *La forma degli atti nel diritto privato. Studi in onore di Michele Giorgianni,* (Napoli, 1988), p 383; Andrea Graziosi, 'Documento informatico (diritto processuale civile)', *Enciclopedia del diritto. Annali*, II, 2, (Milano: Giuffrè, 2008), p 495; Francesco Ricci, 'Firma Digitale', *Diritto Civile*, edited by Silvio Martuccelli and Valerio Pescatore, (Milano: Giuffrè, 2011) pp 783-797.

[37] Also electronic signatures are always defined as a 'set of data in electronic form'. This shows how signature needs to adhere to a document and, for this purpose, should be consistent of the same signs that form and characterize that document.

[38] For the meaning of 'document' in a digital context, see Stephen Mason, general editor, *Electronic Evidence*, chapter 10.

In contrast, there are documents created digitally, called 'informatic writings', which are formed via software and hardware and are displayed on a screen, or on paper when printed out, where the type of electronic signatures affects the value in law and the probative effectiveness of the document.

The four types of electronic signatures provided for in the CAD

The four distinct electronic signatures identified by CAD are essentially referable to two general categories described by article 2 of the EU Directive: an electronic signature intended as 'data combined with other data' and the advanced electronic signature intended as 'data associated to a document'. Indeed, qualified electronic signatures and digital signatures meet the requirements of 'traceability' and 'exclusive control' of a signature device and 'immutability' of data that are related to the advanced electronic signature. However, they are characterized by the need for a qualified certificate or a system of cryptographic keys.

Electronic signature

Article 1(q) of the CAD defines electronic signature as follows:

> firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
>
> electronic signature: the set of data in electronic form attached to or logically associated with other electronic data, used as method of identification;

Therefore, in accordance with this definition, the electronic signature is used for an indicative function and not for subscribing a declaration.

An example is the PIN of the debit and credit card. A card is presented to the machine, usually an ATM. The card could be in the possession of the customer of the bank, or the card might be in the possession of another person who has been obtained it from the actual customer, or a thief might insert a forged card. The software in the ATM communicates with the software on the card. The software purports to identify that the correct PIN has been entered. The PIN acts as evidence for the bank to assume that the customer and correct card are present in order to provide the service.[39]

Similarly, the username and password, used by a user to identify themselves to an e-mail service supplier also has an indicative function. It is contended that there is some questionable case law in relation to this issue. Italian courts[40] have repeatedly held that an unsigned e-mail message is capable of constituting an electronic document signed with an electronic signature.[41] This analysis moves from idea that the sender, in order to create and send an e-mail, must perform an act of validation by entering his personal identification (username) and the password of his access code.[42] It is possible to argue that the identification codes used as the signature of the

[39] For more information, see Stephen Mason, 'Debit cards, ATMs and negligence of the bank and customer', *Butterworths Journal of International Banking and Financial Law*, Volume 27, Number 3, March 2012, pp 163 – 173; Roger Porkess and Stephen Mason, 'Looking at debit and credit card fraud', *Teaching Statistics*, Volume 34, Number 3, Autumn 2012, pp 87 – 91; Stephen Mason, 'Electronic banking and how courts approach the evidence', *Computer Law and Security Review*, Volume 29, Issue 2 (April 2013), pp 144 – 151.

[40] See Trib. Prato, 15 April 2011, *Foro italiano*, 2011, I, c 3198 e *Corriere merito*, 2011, p 802, with observation of Clara Sgobbo, 'Il valore probatorio della e-mail', pp 803 – 805. See also, under provision of the DPR 445/2000, GdP Pesaro, 2 November 2004, n. 1156/2004 in *Giurisprudenza italiana*, I, 2005, c 1024. Pursuing this approach, courts have often held that a simple e-mail message is a valid and sufficient written proof to issue an injunction, in accordance with artt. 633 and 634 of Italian Civil Procedural Code: Trib. Verona, 26 November 2005, *Giurisprudenza di merito*, 2005, p 2129; Trib. Mondovì, 7 June 2004, *Nuova giurisprudenza civile commentata*, 2005, I, p 9*35,* with observation of Matteo Lupano*,* 'Natura dell'e-mail, sua efficacia probatoria nella normativa vigente e nel d. lgs. 7.3.2005, n. 82', pp 936 – 940*;* Trib. Bari, 20 gennaio 2004 and Trib. Lucca, 17 luglio 2004, in *Giurisprudenza italiana*, I, 2005, c 1025-1027, with observation of Giacomo Jori 'L'efficacia probatoria dell'e-mail'; Trib. Cuneo, 15 December 2003**,** *Diritto dell'Internet*, 2005, pp *33* – 34**,** with observation of Giorgio Rognetta**,** 'Decreti ingiuntivi basati su e-mail: la configurabilità della firma elettronica ai fini della prova scritta', pp 34 – 38 and *Giurisprudenza di merito*, 2005, I, p 560 with observation of Mattia Pani*,* 'Il valore di prova scritta di una e-mail: la giustizia inizia a porsi al passo coi tempi', pp 560 – 568*.*

[41] For an analysis of this particular issue, and the fact that judges in jurisdictions across the globe have also accepted this proposition, see *Electronic Signatures in Law*, pp 221 – 253.

[42] As confirmed by the opinion no. 31/06 of the Council of State, issued on 30 January 2006 regarding the draft of Legislative Decree n. 159/2006 (*Parere emesso dalla sezione consultiva per gli atti normativi del Consiglio di Stato, sullo schema di decreto legislativo recante disposizioni correttive e integrative al codice dell'amministrazione digitale, di cui al d.leg. 7 marzo 2005 n. 82, emanato ai sensi dell'art. 10 l. 29 luglio 2003 n. 229*, published on *Foro italiano*, 2006, III, c 237): the signature, consisting of a combination of username and password, is only meant to identify the sender by service provider and has to be excluded any declarative function (see § 10.1.).

author should be sent to the message receiver and not to the supplier of the mail service.[43]

Advanced electronic signature

The advanced electronic signature is defined by article 1(q*bis*) of the CAD as follows:

> firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
>
> advanced electronic signature: the set of data in electronic form attached to or associated with an electronic document, allowing the identification of the signatory of the document and providing a unique connection to the signatory, created using means that the signatory can maintain under his exclusive control, linked to data to which that sign relates in such a way as to detect if the data have been subsequently modified;

Scholars are inclined to qualify the graphometric signature,[44] affixed with a stylus on an electronic tablet, as an example of an advanced electronic signature.[45] The software records the behavioural biometric features of the writer[46] (such as speed, accuracy, inclination angle, acceleration and the number of times that pen is lifted from the writing surface). The software transforms the biometric data recorded digitally into a human-readable image of the signature, and compares the data with the data acquired from previous signatures by the same person.[47]

This method is becoming widespread, especially in the banking sector, because of the capacity of collecting biometric data as the customer signs using the traditional signing gesture. Biometric data collected during the subscription will be encrypted with a public key[48] issued by a certification body and affixed as electronic signature on a document.[49] Indeed, the subscription on the tablet can also be used for mere identification purposes, in order to accede to a service or to be combined with other electronic signatures.[50]

Moreover, nothing seems to prevent that biometric data collected during the subscription to be used for generation of the private key which, when associated with a public key safeguarded by the certifier, allows a digital signature to be affixed on a document. Encrypting the text through the biometric data and adding a qualified certificate appears achievable by using a cryptographic system of asymmetric keys grounded on the use of the hand.

---

[43] See Matteo Giacomo Jori, 'L'efficacia probatoria dell'e-mail', *Giurisprudenza italiana,* 2005, pp 1028 – 1030*;* Massino Farina 'Riflessioni sul valore legale delle e-mail a seguito della pronuncia di alcuni decreti ingiuntivi basati esclusivamente sulla produzione di una e-mail', *Rassegna di diritto civile,* 2005, pp 615 – 629.

[44] On this topic see Giusella Finocchiaro, 'La metafora e il diritto nella normativa sulla cosiddetta «firma grafometrica»', *Diritto dell'informazione e dell'informatica*, 2013, pp 1 – 16, p. 14; Gianluigi Ciacci, 'Firme grafometriche e tutela dei dati personali', *Rivista elettronica di diritto economia e management*, 2014, 1, pp 50 – 62.

[45] Alessandro Mastomatteo and Benedetto Santacroce, '*Validità della firma elettronica: la firma biometrica come modello operativo avanzato*', in *Corriere tributario*, 2012, pp 183 – 187. Doubts are raised by Giusella Finocchiaro, 'La metafora e il diritto nella normativa sulla cosiddetta «firma grafometrica»', pp 14–16.

[46] The authority for personal data protection (Garante per la protezione dei dati personali) issued on 21 May 2014, 'General Guidelines on biometric identification and graphometric signature' (*Linee guida in materia di riconoscimento biometrico e firma grafometrica*, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3132361). Note by the editor: translations into English of applications by Fineco Bank S.p.A (12 September 2013); IT Telecom s.r.l. and Cassa di Risparmio di Parma e Piacenza S.p.A. (31 January 2013) and Unicredit S.p.A. (31 January 2013) are published in this edition of the *Digital Evidence and Electronic Signature Law Review*.

[47] For case law on this method, see *Electronic Signatures in Law*, 256 – 258; also Heidi H. Harralson, 'Forensic document examination of electronically captured signatures', *Digital Evidence and Electronic Signature Law Review,* 9 (2012) pp 67 – 73.

[48] The signatory can clearly maintain his hand under his exclusive control, but he cannot control the digital data that is recorded by the process. Without encrypting such data the 'signature' can be used by thieves if a thief successfully obtains a copy of the digital data comprising the signature.

[49] See the request on 'System for subscription in electronic form of acts, contracts and other documents related to products and services offered by a bank' sent by Fineco Bank SpA to the Authority for personal data protection. This system refers to a double process of encryption: an intermediate encryption based on a symmetric key, which excludes the possibility of view 'in clear' all the data collected, and an additional encryption using the public key of a digital certificate. The authority gave a favourable opinion with application n. 396, issued on 12 September 2013. Note by the editor: a translation into English of this application is published in this edition of the *Digital Evidence and Electronic Signature Law Review*.

[50] Hypothesis specifically envisaged in the request on 'Treatment of biometrics' sent by Unicredit SpA to the Authority for personal data protection. After client's identification made through the graphometric signature, the bank documents will be signed using exclusively the digital signature. The authority gave a favourable opinion with application n. 37, issued on 31 January 2013. Note by the editor: a translation into English of this application is published in this edition of the *Digital Evidence and Electronic Signature Law Review*.

Qualified electronic signature

It is unlikely to find an example of a qualified electronic signature,[51] which in turn is defined by article 1(r) of the CAD as:

> firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
>
> qualified electronic signature: a particular type of advanced electronic signature based on a qualified certificate and created by a secure device for the creation of the signature.

The general opinion among scholars is that a qualified electronic signature cannot be distinguish from a digital one, since it is only possible to use a technology that is based on asymmetric key encryption.[52]

The distinction can be analysed by referring to applications used for remote management of banking activities.[53] Some banks provide their customers with a device that generates a pseudo-random number code called a token. The number is synchronized with an authentication server, under control of the bank that generates the same pseudo-random code. In this scheme, the 'secure' channel on which the code is transferred from the customer to the bank is created by encrypting the message with the public key generated by the receiver (the bank). Afterwards, the message will be decrypted with the private key, which was created by the bank, and remained under its control. At the end of the (single) operation, the pair of keys will be deleted.

The system described is clearly based on asymmetric key encryption, but the certificate issued by a qualified certifier performs a different function: it is matched with a (public) key used to encrypt, only temporarily, the message containing the number code. It is difficult to agree that the certificate in this case 'manifests and verifies the origin and integrity of an electronic document' (in accordance with the definition of 'digital signature' in article 1(s) of the CAD), since the sender does not intend to 'sign' a document, but simply identify himself. Therefore, it is possible to conclude that a qualified electronic signature is a kind of advanced signature, but it does not come within the definition of a digital signature.

Digital signature

The fourth signature is the digital signature, defined by article 1(s) of the CAD as follows:

> firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
>
> digital signature: a particular type of advanced electronic signature based on a qualified certificate and a system of cryptographic keys, one public and one private, related to each other, which allows to the holder, using the private key, and to the recipient, using the private key respectively, to show and verify the origin and integrity of an electronic document or a set of electronic documents;

In other words, the oldest and most widespread advanced digital signature consists of applying a sequence of alphanumeric characters to an electronic document that are obtained by extracting from the text a representative sample ('hash value' or 'message digest') and is encrypted with a 'private' key, as part of a cryptographic system of asymmetric keys.[54]

[51] According to Mason, *Electronic signatures in Law*, p 130: 'A qualified electronic signature consist of three component parts: an advanced electronic signature, a qualified certificate and a secure-signature-creation device that must comply with the requirements set out in Annexes I, II and III [of Directive]'. See also, Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures, COM(2006) 120 final, 15.3.2006, 2.3.2.

[52] Andrea Graziosi, 'Documento informatico (diritto processuale civile)', *Enciclopedia del diritto. Annali*, II, 2, (Milano: Giuffrè, 2008), p 500; Alessandra Villecco, *Il processo civile telematico*, (Milano: UTET Giuridica, 2011), p 25; Giusella Finocchiaro, 'Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale', *Contratto e impresa*, 2011, pp 495 – 504, p 499.

[53] Widely, Giovanni Buonomo and Aniello Merone, 'La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio', *Diritto dell'informazione e dell'informatica*, 2013, pp 255 – 286, pp 270 – 271.

[54] Among many essays on this topic, Renato Borruso and Gianluigi Ciacci, *Diritto civile e informatica,* (Napoli: Edizioni Scientifiche Italiane – ESI, 2004), chapter 7, pp 410 – 423, 452 – 459**;** Giovanni Buonomo**,** 'Processo telematico e firma digitale', (Milano: Giuffrè, 2004), chapter 5 and 7**;** Francesco Ricci, *Scritture private e firme elettroniche*, (Roma: Luiss University Press, 2003), *pp 108 – 117;*

The CAD requires that the cryptographic system of keys is based on a certificate issued by a qualified certifier,[55] and that the signature 'is created using tools that the signatory can maintain under is exclusive control'.[56]

Legal value and evidential effectiveness of informatics writing

As previously observed, the electronic signature affects the legal and evidential value of the electronic document. According to the provisions of articles 20 and 21 of the CAD, all electronic documents, even if they are not signed, are effective because of their objective characteristics of quality, safety, integrity and immutability. However, the free evaluation of the judge is excluded by the presence of an advanced, digital or qualified electronic signature.

Legal value

Concerning value in law, it is necessary to distinguish the following:

> 1. Writings provided by article 1350, nn. 1-12 CC,[57] in which the requirement of written form under penalty of invalidity will be satisfied by an electronic document signed with a qualified electronic or digital signature (article 21, § 2/bis, CAD).
>
> 2. Other writings that require written form under penalty of invalidity, provided by article 1350, n. 13 CC,[58] have to be signed with an advanced, digital or qualified electronic signature, (article 21, § 2/bis, CAD).
>
> 3. All other writings, in which the written form is required only for evidentiary purposes, can be subscribed with any form of electronic signature.[59]

After the amendments to article 21 of the CAD introduced by Law n. 221 of 2012, digital and qualified electronic signatures continue to be the only electronic signatures capable of meeting the requirements of article 1350 nn. 1-12, CC.

However, a new assessment will be added in the text of article 21, § 2*bis*:

> […] Gli atti di cui all'articolo 1350, numero 13), del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale.
>
> […] The acts referred to in article 1350, number 13 of the Civil Code still meet the requirement of written form if signed with an advanced electronic signature, qualified or digital.

Therefore, even an advanced electronic signature (without a certificate and not based on a system of cryptographic keys) can be included in 'all other acts' that require a written form under penalty of invalidity. On the other hand, the means used for the purpose of electronic identification that are compatible with the notion of an electronic signature may be only relevant as evidence, and are subject to the free evaluation of the court.

Evidential effectiveness

In terms of evidential value, article 21 of the CAD offers two options.

The probative value of an electronic document subscribed with an electronic signature is freely assessable in light of its objective characteristics of quality, safety, integrity and immutability (article 21, §

Alberto Maria Gambino, 'Firma digitale (dir. civ.)', *Enciclopedia giuridica,* XV, (Roma: Treccani, 1999), pp 1 – 9; Mason, *Electronic Signatures in Law,* chapter 7.

[55] It should be noted that technology based on asymmetric key encryption can also be used to sign an electronic document without recourse to the certification of keys.

[56] To complete overview of the regulations, the CAD rules have to be integrated with the technical rules issued by Decreto del presidente del Consiglio dei Ministri del 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*, (Gazz. Uff. n. 117, del 21 maggio 2013), in force since May 2013, that in turn repealed and replaced the previous Decreto del presidente del Consiglio dei Ministri del 30 marzo 2009, *Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici* (Gazz. Uff. n. 129, del 6 giugno 2009).

[57] Article 1350, CC, is entitled 'Atti che devono farsi per iscritto' 'Acts which must be in written form' and the list offered by nn. 1-12 is referable, in summary, to contracts that establish modify or transfer the ownership of real estate property and/or other real property rights, and acts of division or renunciation of the rights referred above.

[58] Article 1350, n.13, CC, is a general clause that refers to all other acts for which the requirement of written form under penalty of invalidity is expressly provided by law.

[59] On the suitability of an electronic document to satisfy the requirement of written form, see Aurelio Gentili, 'Documento elettronico: validità ed efficacia probatoria', *I contratti informatici*, edited by Renato Clarizia, (Milano: UTET, 2007), pp 119 – 167, pp 141 – 152.

1, CAD). It should be noted that the same evidential value is referred by article 20, § 1-*bis*, CAD for an electronic document without a signature. However, it seems correct to assume that the presence of an electronic signature is sufficient to provide the document with a higher degree of reliability, and thus to restrict the discretion of the court. The presence of an electronic signature prevents the judge from refusing to admit the effectiveness of the document. The combined provisions of article 21, § 2 of the CAD and article 2702 CC act to avoid giving full evidential value to a signature that is affixed without using a device that the signatory can maintain under his exclusive control. This means that the probative value of an electronic document signed using a method other than an advanced electronic signature will be determined by the court through the use of presumptions.

Otherwise, according to article 21, § 2, CAD, an electronic document subscribed with an advanced, digital or qualified electronic signature benefits from the legal presumption of effectiveness of proof, unless the signing party provides a declaration that the origin of the statements are false (as provided by article 2702, CC). The probative value assigned in 1997 by the Italian legislator to the digital signature, as the equivalent to a traditional writing signed on paper, is now extended to the advanced electronic signature.

Documents that are signed by digital and qualified electronic signatures, as set out in article 21, § 2 of the CAD, are presumed to be signed by the owner of the signature device, unless he proves otherwise:

> L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.
>
> The use of the device of electronic signature or digital is presumed due to be the holder, unless he proves to the contrary.

This presumption is justified by the objective and relevant guarantees that are asserted in terms of security and reliability of such signatures, because of the cryptographic mechanism and qualified certificate that make it almost impossible to counterfeit a signature, and are able to highlight any subsequent manipulation or alteration of the document.[60]

The reference to article 2702 of the Civil Code

Despite the clear reference to article 2702 CC, scholars have offered two conflicting interpretations of it,[61] and, consequently, two different reconstructions of the effectiveness of a subscribed electronic document.[62]

According to one view, data in digital format (informatic writing) acquires effectiveness of proof only if the signatory expressly recognized the subscription of the document, or if the signature is legally considered as recognized because of its authentication by a notary, the lack of the signature's disavowal or the negative outcome of verification at trial.[63]

Other scholars consider that an electronic document signed with a digital, qualified or advanced electronic signature would immediately gain the effectiveness of a legally recognized writing, even in absence of an express or implied recognition of the signature.[64] This second opinion had been formally accepted by Italian

[60] Digital signatures are not as 'safe' as is commonly asserted. See the Russian banking cases: Olga I. Kudryavtseva, 'The use of electronic digital signatures in banking relationships in the Russian Federation', *Digital Evidence and Electronic Signature Law Review*, 5 (2008) pp 51 – 57; Olga I. Kudryavtseva, 'Resolution of the Federal Arbitration Court of Moscow Region of 5 November 2003 N КГ-А 40/8531-03-П', *Digital Evidence and Electronic Signature Law Review*, 5 (2008) pp 149 – 151; see also for other examples from across the world Stephen Mason, *Electronic Signatures in Law*, pp 292 – 302.

[61] Salvatore Patti, 'La sottoscrizione del documento informatico: la firma digitale', *Studi e materiali. Quaderni trimestrali del Consiglio Nazionale del Notariato: La sicurezza giuridica nella società dell'informazione,* Suppl. n. 1, 2008, pp 127 – 139. The author reconstructs this debate opposing the idea of 'weak' probative effectiveness to a 'strong' one.

[62] Before the digital signature, the doctrine use to apply regulations on mechanical reproductions to an electronic document presented as 'writing', as provided by article 2712 CC. See Luigi Montesano, 'Sul documento informatico come rappresentazione meccanica nella prova civile e nella forma negoziale', *Rivista di diritto processuale*, 1987, pp 1 – 13; Giovanni Verde, 'Per la chiarezza di idee in tema di documentazione informatica', *Rivista di diritto processuale*, 1990, pp 715 – 736; Gian Franco Ricci, '*Aspetti processuali della documentazione informatica', Rivista trimestrale di diritto e procedura civile*, 1994, pp 863 – 887.

[63] Giovanni Verde, 'Prove nuove', *Rivista di diritto processuale*, 2006, pp 35 – 52, p. 44; Francesco Ricci, *Scritture private e firme elettroniche*, pp 61 – 84; Umberto Romano, 'Firma digitale', *Digesto delle discipline privatistiche, Sezione civile – Aggiornamento*, (Torino: UTET, 2000), pp 386 – 399, p. 388; Salvatore Patti, 'L'efficacia probatoria del documento informatico', *Rivista di diritto processuale*, 2000, pp 60 – 92, p. 73; Francesco De Santis, 'La disciplina normativa del documento informatico', *Corriere giuridico,* 1998, pp 379 – 396, pp 392 – 393.

[64] Giusella Finocchiaro, 'Il valore probatorio del documento informatico e firma digitale', in *Contratto e impresa*, 2002, pp 76 – 85; Andrea Graziosi, 'Premesse ad una teoria probatoria del documento informatico', *Rivista trimestrale di diritto processuale civile*, 1998, pp 481 – 529, pp 512 − 518; Aurelio Gentili, 'Documento informatico e tutela dell'affidamento', *Rivista di diritto civile*, 1998, pp 163 – 179, pp 171 – 174.

legislator in the past, via the amendments introduced by Legislative Decree n. 10/2002 to article 10 of Presidential Decree n. 445/2000,[65] but later abandoned with the enter in force of the CAD.

In the current legal framework, the first opinion is cogent. If an informatic writing could gain the effectiveness of proof by reason of its subscription with a digital, qualified or advanced electronic signature, the provisions of article 25 of the CAD will have to be described as of no value:

> Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o d' altro pubblico ufficiale a ciò autorizzato.
>
> It has to be recognized, pursuant to article 2703 of the Civil Code, the electronic signature or any other type of advanced signature authenticated by a notary or other public official authorized to do so.

The possibility of providing for the authentication of any form of electronic signature would be ineffective if the document, signed with a digital, qualified or advanced electronic signature, was already equipped by the law (article 2702) with the same effectiveness that authentication is able to confer. However, the contrast is strictly linked to another debate concerning the applicability to the electronic signature of the rules governing the disowning of a signature and the verification of a signature, as provided by articles 214 – 220 of the Codice di procedura civile (Civil Procedural Code (CPC)), as discussed below.

Recognition, authentication and verification of advanced electronic signatures

The value of proof that is ruled by article 2702 CC is conditioned by the expressed recognition of the signature by the party against whom the writing is filed, or if the signature is 'legally considered' as being recognized in order to avoid its repudiation. Where an author expressly recognises the signature, this in itself enables the court to give value of proof to the document. The provenance of the statements contained in the document and the authenticity of the signature are not controversial facts. It follows that verification is unnecessary.

On the other hand, subscription is legally considered as recognized when the author of the signature has not expressly disavowed the subscription during the first hearing or statement of defence, subsequent to documents being filed in deed by the other party (referred to as 'tacit recognition', article 215 CPC); or where the signature has been declared legally 'authentic' by a notary or other authorized public officer, according to the rules provided by article 25 of the CAD. A notarized signature is equivalent to a signature that is recognized.

When the signature is recognized or authenticated, it follows that the author will not have the opportunity to disown it at trial (article 214 CPC). The author can only claim the signature is a forgery (articles 221 – 227 CPC), in case of 'tacit recognition'[66] or in order to determine a false statement made by the notary or other authorized public officer.[67]

If the signature is not recognized (expressly or legally), or it has been disowned, the counter party that has filed the document in deeds and still intends to rely on this evidence, will request judicial verification (article 216 CPC) to ascertain the authenticity of the signature.[68] A positive assessment arising from a judgment of the court has the same effect of both recognition and authentication of the signature.

[65] On the critics raised against such choice, see Francesco Ricci, *Scritture private e firme elettroniche*, (Roma: Luiss University Press, 2003), pp 163 – 176; Andrea Graziosi, 'La nuova efficacia probatoria del documento informatico', *Rivista trimestrale di diritto processuale civile*, 2003, pp 53 – 80, pp 61 – 73.

[66] Expressed recognition has value of confession and can be repealed only by reason of a 'mistake of fact' or an 'act of violence', as provided by art. 2732 CC.

[67] Called 'ideological false'; see Francesca Ferrari**,** 'Il codice dell'amministrazione digitale e le norme dedicate al documento informatico', *Rivista di diritto processuale civile*, 2007, pp 415 – 431, p 428**;** Andrea Graziosi, 'Premesse ad una teoria probatoria del documento informatico', *Rivista trimestrale di diritto processuale civile***,** 1998, pp 481 – 529, p. 501; Francesco Rizzo, *Il documento informatico. «paternità» e «falsità»*, *(*Napoli: Edizioni Scientifiche Italiane – ESI, 2005), pp 303 – 307, pp 374 – 405**;** Aurelio Gentili, 'Documento elettronico: validità ed efficacia probatoria', *I contratti informatici*, edited by Renato Clarizia, (Milano: UTET, 2007), pp 119 – 167, pp 158 – 167; Mauro Orlandi**,** *Il falso digitale*, (Milano: Giuffrè, 2003), pp 135 – 139.

[68] Such regulation is not referable to mechanical reproductions. As well explained by Cass., sez. III, March 4 2004, n.4395; Cass., sez II, May 12 2000, n.6090, the disavowal previewed by article 2712 CC is other than one ruled by article 214 CPC. Indeed, it does not preevnet the court from asertaining the compliance of the reproduction with the original, using other evidence or presumtions. See on this topic Mariaserena Iozzo 'Orientamenti (e disorientamenti) in tema di disconoscimento delle riproduzioni meccaniche', *Foro italiano*, 2002, I, c 2793.

Furthermore, pursuant to article 216, § 2, of the CPC, judicial verification of the signature's origin can also be requested by the party as a separate legal action, not for the purpose of using the document as evidence in a previous trial, but to obtain a judgment uniquely concerning the authenticity of the document. The regulations provided by article 214 and following of the CPC, as described above, are applied to both the hand-written and advanced electronic signature.[69]

This statement is not modified by the presumptive use of a signature device by the holder, as set out in article 21, § 2, CAD. This presumption, that only refers to digital and qualified electronic signatures, cannot be equated to the recognition or authentication of the signature: while the latter attributes value of proof to the use of the signature, the presumption involves shifting the burden of proof. Indeed, the signature's holder (and device owner) may overcome the presumption proving otherwise.

Arguments against the applicability of the rules on verification and disavowal

As mentioned above, Italian scholars have proposed several critical arguments in order to not apply the provisions denying an author affixed a signature to digital, qualified and advanced electronic signatures.

According to some authors,[70] the use of a signature device (ruled by articles 32 and 35 of the CAD) causes a gap between the will of the subscribing party and the creation of the encrypted code. The verification procedure is impossible (or rather useless): it is only capable of revealing the use of a signature device. It cannot demonstrate the owner used the device. According to this perspective, in the event of the forgery of a signature (the use of the device by an unauthorized third party), the subscription would be attributed to the holder of keys, since the digital signature (like any other advanced signature) is a mere 'seal' affixed to the document through an encryption system.[71] The owner of the device can only take an action for forgery to prove the unauthorized use of the signature device by third parties and overcome the evidence concerning the origin of the document.

This opinion cannot be shared, because it means that the electronic document is more effective than one written on paper, in contrast with the objectives of Directive 1999/93/EC. Furthermore, accepting those arguments, we lead to the exclusion of the action provided by article 216, § 2, CPC against an electronic document in order to deny its signatures, with an unacceptable reduction of the right of action safeguarded by the Constitution.

For other scholars,[72] the presumptive use of a signature device by the holder, with the attendant shifting of the burden of proof, would lead to conclude that data in digital format (informatic writing) has greater evidential value than a document written and signed on paper. Such circumstance would prevent the enforcement of the disavowal and verification provided by articles 214 – 220, requiring a different verification procedure dedicated to the electronic document and signatures.

This view moves from, arguably, the incorrect understanding that the only scope of the verification procedure is to certify the identity of the signature in respect to previous 'authentic' sample. Otherwise, the verification set out in articles 216 – 220 CPC aims to link the origin of the document to someone who appears as the author.[73] For electronic signatures it means not to give evidence of identity of the different

[69] Otherwise, for electronic signatures there is no reference to article 2702 CC and they are always subject to free evaluation of the judge. According to Giovanni Verde**,** 'Prove nuove', *Rivista di diritto processuale*, 2006, pp 35 – 52, p. 42; Francesco Ricci, *Scritture private e firme elettroniche,* pp 123 – 126, the applicability of regulations provided by articles 2702 CC and 214 – 220 CPC have to be exclude for electronic signatures by reason of their indicative function.

[70] Giusella Finocchiaro, **'**Tecniche di imputazione della volontà negoziale; le firme elettroniche e la firma digitale', *I contratti informatici*, edited by Renato Clarizia, (Milano: UTET, 2007), pp 201 – 233, pp 226 – 231; Aurelio Gentili, 'Documento elettronico: validità ed efficacia probatoria', *I contratti informatici*, edited by Renato Clarizia, (Milano: UTET, 2007), pp 119 – 167, pp 152 – 157.

[71] Giusella Finocchiaro, 'Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale', *Contratto e impresa*, 2011, pp 495 – 504, p 502, argues that use of word 'signature' in the context of the electronic document assumes a metaphorical value, as foreign to the traditional handwritten signature.

[72] Fabio Rota, 'Il documento informatico', *La prova nel processo civile*, *Trattato di diritto civile e commerciale Cicu-Messineo*, edited by Michele Taruffo, Milano, 2012, pp 728 – 775, p 760; Francesca Ferrari 'Il codice dell'amministrazione digitale e le norme dedicate al documento informatico', *Rivista di diritto processuale civile*, 2007, pp 415 – 431, p 426; Claudia Sandei 'Valore formale e probatorio del documento informatico alla luce del d.lgs. 4 aprile 2006, n. 159', *Nuove leggi civili commentate*, 2008, pp 3 – 42, pp 27 – 30.

[73] Indeed, according to article 21, § 2 of the CAD, digital, qualified or advanced electronic signatures have to be made in accordance with the technical requirements, as stated in article 20, § 3, CAD, intended to provide for the identification of the subscriber and the integrity of the document.

signatures, nor the mere possession of the signature device, but its use under the control of the owner.

Validation procedure, presumption and burden of proof

Article 21, § 2 of CAD provides that 'the use of the qualified electronic and digital signature device is assumed due to the holder, unless he proves otherwise'. This explains that the presumption necessarily involves a process by which the owner can (and has to) prove they did not use the device. In the current legal framework this process has to be found in the judicial verification. Moreover, given the absence of Italian case law concerning the disavowal of digital, qualified or advanced electronic signature, any other opinion would appear inconsistent or arbitrary.

The cryptographic system of asymmetric keys purports to grant security, integrity and authenticity through a validation procedure: it is possible to trace back from the public key associated with a certificate to the private key that has encrypted the text.[74] This does not prove that the signatory caused the action. However, since article 216 of the CPC clearly indicates that verification can be achieved through any form of evidence, the validation procedure cannot be ignored in a similar way to a graphic report, which allows a link between the signature present on the document and its presumed author. Therefore, if the signatory denies signing an electronic document, the other party, with an interest to avail themselves of the disowned informatic writing, must be able to request a judicial verification under the rules of articles 216 – 220 of the CPC.

It follows that this party can both request a judicial verification within the limits of relevance that the electronic document assumes in a different judgment, and request a legal action concerning the verification of authentication of the document; and has the burden to provide evidence of the actual use of signature device by the holder. This evidence is usually offered by the certifier, who 'certificates' that the key used to sign belongs to the pair generated by signature device assigned to the signatory. To this purpose the party will request the certifier of the digital record (art. 1, (e) and (f), CAD) associated to the electronic document. Otherwise, it will be the party against whom the document has been filed that has to overcome the presumption of the authenticity of the signature, and, to this end, he needs to proceed with the validation procedure.

The burden of proof shifts regarding the ownership of a digital or qualified signature. Since the use of the signature device can be (even habitually) performed by someone who is not associated with the device, it cannot be sufficient to demonstrate that the signature was made by a third party. It will be necessary to give evidence that the device was used by somebody other than the holder, and it occurred outside of the holder's control.

The holder, even if he has lost the signature device, will always be able to ascertain the date, time and place in which the device has been used to sign. The regulatory provisions impose a continuous activity of recording and transcription on users and signature service providers. In theory, it is always possible to prove that the signature device may not have been used by someone who, at the recorded time, was in another place.

In the light of the above, the shifting of the burden of proof appears to be the best way to balance the evidential activity. The party that repudiates an electronic document has evident difficulties in proving its authenticity, while the absence of control over the signature device can most easily be demonstrated by the party that owns it. This analysis appears coherent with opinion of the Italian Supreme Court in affirming that the burden of proof must be shared according to closeness or availability of a probative tool, avoiding the impossible or excessively difficult burden of proof in legal proceedings.[75]

Likewise, the enforceability of article 2702 of the CC and articles 214 – 220 of the CPC regarding electronic signatures fulfils the purpose of ensuring the equivalence between electronic and handwritten documents, and to avoid the easy repudiation of an electronic signature by its author, and not to assign to the signature device holder those writings that are not attributable to his will and control.

[74] The same possibility is offered by the graphometric signature when using an encryption key to sign the document.

[75] Cass., Sez. II, August 9 2013, n. 19146; Cass. Sez. I, April 12 2013, n. 8931; Cass., Sez. V, June 6 2012, n. 9099; Cass., sez. lav., July 1 2009, n. 15406; Cass., sez. lav., July 25 2008, n. 20484; Cass., Sez. Un., January 10 2006 n. 141; Cass, Sez. Un, October 30 ottobre, n. 13533.

Furthermore, the absence of case law and judgments on electronic signatures disavowal seems to highlight as they are considered subscription means that grant an high level of security and integrity and they are evaluated more difficult to challenge in trial than a handwritten signature.

Aniello Merone, PhD in Arbitration Law (LUISS University), is a Research Professor of Civil Procedure Law (Università Europea di Roma), Lawyer at the bar of Rome, a member of the Institute for Advanced Studies on Arbitration and the Italian Association between Experts of the Civil Procedure.

aniello.merone@unier.it