DIRITTO MERCATO TECNOLOGIA

INDICE DEL FASCICOLO N. 1
(gennaio – aprile 2016)

FOCUS
IL SISTEMA IMPOSITIVO NELL'ECONOMIA DIGITALE

THE DIGITAL IDENTITY: THE GLOBAL PROSPECTIVE

Francesco Delfini
University of Milan

Nowadays, the digital identity is the main issue in electronic commerce since the challenge the parties to every electronic transaction are facing is to answer two simple questions reliably, in reference to each other: "Who are you?" and "How can you prove it?".

In digital identity management, the ultimate and most efficient tool is so-called *federated* identity management. As we have just learned and as has been clearly depicted,[1] "*[in a federated system, transacting parties can avoid the cost and expense of setting up their own identity management process, relying instead on identification and authentication services provided by trustworthy third parties. And users can avoid the need to obtain separate identity credentials (such as usernames and passwords) for every business they deal with. It is like replacing the need to carry a separate credit card from every business where an individual shops, with two or three credit cards (e.g., a Visa and a MasterCard) that all businesses will accept."*

At one point, the main issue was answering the questions "Who is the author of an electronic document?" and "Who is bound by it or responsible for it?", and the corresponding answers were the electronic signatures and their management. But as opportunities to interact and establish economic relationships via the Internet grow – and as a vast number of economic transactions are entered into without a proper electronic document – the main point has become the assessment of each party's identity and therefore identity management.

Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.

[1] Thomas J. Smedinghoff and Laurie Kamaiko, *Identity Management: The Key to Cyber Security and Online Commerce*, New York Law Journal, March 2, 2015.

A variety of approaches may be taken to implement such management of individuals' identity.

The US approach, as we have heard, relies on the contract and on "soft law", encouraging the private sector to set its own rules on the topic.[2]

On the other hand, the European Union has preferred "hard law" and since the end of the last century has provided a complete set of rules to furnish parties that had never met before with the mutual assurance of each other's digital identity. The legal framework progressed from EU Directive 1999/93/CE on electronic signatures to the recent regulation (EU) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 "*on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*" that is due to apply, for the most part of it, from 1 July 2016.

This difference in approaches does not come as a surprise.

They depict in a simple way the different traditional attitudes of the two legal systems toward lawmaking. Montesquieu's theory of the separation of political power among the legislature, executive and judiciary – which was the political background of the French Revolution – led to the idea of a civil code as the whole and entire summary of rules in private law arising from the people's representatives. This feature of a civil law system involves a particular attitude and approach for the civil lawyer toward contracts: on one hand, the parties to a contract may agree on the basic elements of the deal – e.g. price and item purchased – while the civil code will provide the entire set of rules to solve any dispute which may arise and

[2] «*In 2011, the U.S. government formally began its efforts to enable a federated identity ecosystem by issuing its National Strategy for Trusted Identities in Cyberspace (NSTIC), which it characterized as "a strategy to make online transactions more secure for businesses and consumers alike." And in 2012 it established a public-private partnership known as the Identity Ecosystem Steering Group (IDESG) in an attempt to encourage the private sector to implement the NSTIC strategy on a voluntary basis. Separately, several private sector companies (such as Google, Microsoft, Experian, Lexis/Nexis, Barclay's Bank, Verizon, and many others), as well as trade associations like the Open Identity Exchange, standards groups like the OpenID Foundation, and certification groups like the Kantara Initiative, are independently working on the issue of federated identity*» (Thomas J. Smedinghoff and Laurie Kamaiko, *Identity Management: The Key to Cyber Security and Online Commerce*, New York Law Journal, March 2, 2015).

any aspect of the deal not covered by an express agreement; on the other hand, civil lawyers are less likely than common lawyers to rely on contract to solve general problems, trusting better the intervention of lawmakers.

On the contrary, common law lawyers, not having the possibility to fill the gaps in contract with rules "subject to agreement otherwise" because of the lack of a code, are used to drafting contracts intended to be self-sufficient. They do not leave room for judge-made rules[3] and have developed a stronger attitude to recourse to the contract to set *erga omnes* or at least multi-party rules that meet the market's needs.

As a consequence, it is more natural for a common law lawyer to suggest using a contract – and, in this case, a multi-party contract or a contract open to other parties to adhere to[4] – to regulate also the management of digital identity. And in some ways this can be regarded as an evolution of the electronic data interchange (EDI)[5] that constituted the basic framework of B2B electronic commerce in the Eighties.

The "hard law" approach has been chosen also by the People's Republic of China. Article 2 of the 2004 Electronic Signature Law (ESL) of

[3] However judge-made rules are in any case largely delivered by Courts via the doctrine of construing the contract with its "implied terms"). *«The emphasis during the nineteenth century on individual freedom and the role of agreement in extending that freedom would seem to have required that no obligation in the nature of a contract should be enforced unless willed by the parties; yet the judges were ready to import terms into contracts and develop and enlarge restrictions in the public interest although the parties themselves had not expressed those terms or established those restrictions»* (Sir David Hughes Parry, *The Sanctity of Contracts in English Law*, London, 1959, 39).

[4] See art. 1332 Italian civil code: «*Adherence of other parties to the contract. If other parties can adhere to a contract and the manner of adherence has not been determined, the question can be directed to such agency as may have constituted for the implementation of the contract or, in the absence thereof, to all original contracting parities*» Italian Civil Code, version translated by M. Beltramo, G.E.Longo and J.H. Merryman, published by Oceana Publ., Inc.

[5] As it can be read in Wikipedia, «*Electronic data interchange (EDI) is an electronic communication method that provides standards for exchanging data via any electronic means. By adhering to the same standard, two different companies or organizations, even in two different countries, can electronically exchange documents (such as purchase orders, invoices, shipping notices, and many others)*».

the People's Republic of China[6] provides a definition of electronic signature, with the same approach and broad content of EU Directive 1999/93/CE: *For the purposes of this Law, electronic signature means the data in electronic form contained in and attached to a data message to be used for identifying the identity of the signatory and for showing that the signatory recognizes what is in the message. The data message as mentioned in this Law means the information generated, dispatched, received or stored by electronic, optical, magnetic or similar means.*

Furthermore, the reliability of an electronic signature is considered in Article 13 of China ESL[7] in the same manner as UE Directive 1999/93 CE did.

The material convergence on digital identity management therefore appears to be stronger than the formal differences in approaches.

[6] Adopted at the 11th Meeting of the Standing Committee of the Tenth National People's Congress on August 28, 2004 and promulgated by Order No.18 of the President of the People's Republic of China on August 28, 2004.

[7] Article 13 ESL: «*If an electronic signature concurrently meets the following conditions, it shall be deemed as a reliable electronic signature:(1) when the creation data of the electronic signature are used for electronic signature, it exclusively belongs to an electronic signatory; (2) when the signature is entered, its creation data are controlled only by the electronic signatory; (3) after the signature is entered, any alteration made to the electronic signature can be detected; and (4) after the signature is entered, any alteration made to the contents and form of a data message can be detectThe parties concerned may also choose to use the electronic signatures which meet the conditions of reliability they have agreed to*».