5 - 7 october 2017 - Santiago de Compostela

TOPIC I

CONSUMER PROTECTION IN THE DIGITAL ENVIRONMENT

4TH CONGRESS OF THE NOTARIES OF EUROPE

CONSUMER PROTECTION IN THE DIGITAL ENVIRONMENT

I. Electronic commerce and the notarial function

1. Electronic resources: some statistics

2. Electronic commerce in figures

3. European regulations on electronic commerce

3.1. Concept of electronic commerce

3.2. The Directive and the notarial function in electronic commerce

3.3. Development of the European regulations

4. Evolution and types of electronic commerce

4.1. By type of commercial relationship

4.2. By purchase channel

5. What can the notarial function offer to electronic commerce?

5.1. Generating trust regarding the identity of the contractual parties

5.2. Generating trust regarding the object

5.3. Generating trust in the field of data protection

II. The presence of notaries in the pre-contractual phase of e-commerce: *Notarial oversight of pre-contractual acceptance of Standard Contract Terms and Conditions in online consumer contracts of goods and services*

1. Previous.

2. The Digital Single Market strategy

3. Fulfilment of consumer protection standards

4. A homogeneous EU legal framework for consumer protection

5. Some concerns about the inefficient functioning of the internal market, and the Directive 2011/83

6. Downsides of this regulatory framework

7. Notaries could play a valuable role in the satisfactory functioning of the Digital Single Market: A Spanish proposal: The Notarial Seal of Conformity of the Standard Contract Terms

III. The notariat and e-commerce subjects

1. The position of the notariat as regards e-commerce subjects

2. Identification and digital capacity

2.1. Identification of the digital business operator

2.2. Identification of the digital consumer

2.3. Digital capacity

3. The Dutch project: notarisID

IV. The relationship between blockchain, notaries and e-commerce

- **1. Notarial trust and digital trust**
- **2. Is electronic trust infallible?**
- **3. The compatibility of the two types of trust**
- **4. The position of blockchain within the legal system**
- **5. Blockchain and notaries**
- **6. Blockchain and property registers**

V. Digital inheritance

- **1. Digital inheritance in connection with analogue inheritance**
- **2. Digital assets**
  - *2.1. The transfer of digital files*
  - *2.2. The distinction between container and content*
  - *2.3. Succession in BitCoin and similar concepts*
  - *2.4. The position of intrinsically personal relationships*
- **3. Legitimation before service providers**
- **4. Notarial testaments and online testaments**

I. Electronic commerce and the notarial function

1. Electronic resources: some statistics

It is undeniable that electronic commerce is an increasingly important and omnipresent method by means of which people consume goods. Ever more users, and at an ever-younger age, have access to the Internet and mobile devices, which means that within a digital context people become consumers much earlier, to a much greater extent and in many more locations than in the past, as they are exposed to consumption for longer, and from an earlier age.

In fact, and for example, according to figures from the Spanish National Statistical Institute, in the year 2016 the use of digital resources was practically universal from the age of 10, with access to mobile phones rising significantly from this age upwards, to a level of nearly 95 % of the population at the age of 15. Access to mobile phones has increased by nearly 3 percent since 2015 and has risen for the third consecutive year, which is truly significant. From this age upwards, access percentages are lower, but still high: more than 80 percent of the population aged between 16 and 74 have used the Internet in 2016, an increase of nearly 2 percentage points compared with the figures for the previous year.

In parallel, electronic commerce channels are multiplying, with social commerce and virtual commerce now being common terms. It should be borne in mind that nearly 70 % of Internet users take part in social media. The objects of consumption likewise continue to expand: while we are still familiarising ourselves with the consumption of audio-visual media on demand, new objects of commerce that just a few years ago did not even exist are now emerging, such as micro-payments, in-app purchases, and video game expansion packs.

The channels for the development of electronic commerce are likewise expanding, and companies have understood that they can capture customers with new business models aligned not only with their consumption habits, but also their economic status: subscriptions to streaming services at different levels, seasonal subscriptions to videogames or premium and freemium models, allowing each individual to consume exactly what they are able and willing to consume.

Meanwhile, electronic marketing campaigns are increasingly personalised, and address a greater audience. Big data and cookies provide companies with almost instantaneous knowledge of the tastes of their target audience, while social media provides channels that exponentially increase both the impact of advertising messages and the time period during which audiences are voluntarily exposed to them. However, when Internet users in Spain are asked about their concern that their online activities could be being

monitored to deliver tailored advertising to them, 61.1 % say that they are worried about this aspect.

2. Electronic commerce in figures

What all the above means is that ever more people, of all ages and with a greater need for and knowledge of the digital world, are accessing social media and the Internet, and in short are inevitably accessing electronic commerce.

The percentage of people who purchased over the Internet in 2016 was likewise nearly 3 percent higher than the previous year, reaching a penetration level of nearly 35 % of the population. In 2016, slightly more than 50 percent had performed electronic commerce transactions at some time in their life, the reasons why the other 50 percent had not done so being that they preferred to shop in person in a physical store, that they were concerned about privacy or security, essentially in the payment process, or did not have faith in the delivery or return of the goods.

Half of Internet users had limited or not performed some activity on the Internet for security reasons, including their concerns as to giving up personal information. As a result, while the number of users operating by means of digital resources would seem to rise, their trust in such methods has plateaued, or even fallen. The data regarding concerns as to privacy, and as to trust and security in the transaction, are significant: electronic consumers are increasingly well informed and are more demanding as regards security, privacy, and the handling of their digital footprint.

This is a basic and very general snapshot of the present of electronic commerce, while it is also clear that those who in a few years will be the potential users of electronic commerce, of online public services or notarial operations, will not be 'digital natives' as such, but in fact exist within a world where it no longer makes sense even to talk of such a concept.

The question we need to ask ourselves is: could we, as notaries, do something to help eliminate this lack of trust, since if there is one thing that notaries generate, it is trust? In order to offer a response, we need to define what we understand by electronic commerce, and to open up the debate as to the presence of notaries in the digital world in general, and in digital commerce in particular.

3. European regulations on electronic commerce

3.1. Concept of electronic commerce

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) represented an initial and hugely important step in guaranteeing the legal integration of the EU, and establishing a borderless space within the context of information society services.

As indicated by Recital 17 of the Directive, the definition of information society services already exists in European legislation:

Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998, and in Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998, and may be understood as any service normally provided for remuneration, at a distance, by means of electronic equipment and at the individual request of a recipient.

Recital 18 nuances and clarifies the inclusion of activities comprising the contracting and selling of goods, provided this is performed online. Likewise, potentially included are non-remunerated services involving economic activity, such as the offering of online information or commercial communications, or those providing tools allowing for search, access and retrieval of data, and likewise services consisting of the transmission of information via a communication network, or the hosting of information provided by a recipient of the service.

It is likewise clarified that this does not include the provision of services off-line, nor the delivery of goods themselves, nor activities which, by their very nature, cannot be carried out at a distance and by electronic means, such as the statutory auditing of company accounts or medical advice requiring the physical examination of a patient.

Article 9.2 of the Directive provides that the Member States may lay down that the terms would not apply, among other aspects, to contracts that create or transfer rights in real estate, except for rental rights. In Spain, for example, Article 3.2 of Act 34/2002 establishes as a consequence that the creation, transfer, modification, and cancellation of real rights over real estate assets located in Spain will be subject to the formal validity and efficacy requirements established in the Spanish legal system.

Meanwhile, Article 2 of the Directive establishes other important definitions, such as those of service provider (subsection (b) - any natural or legal person providing an information society service), recipient of the service (subsection (d) - any natural or legal person who, for professional ends or otherwise, uses an information society service), and consumer (subsection (e) - any natural person who is acting for purposes which are outside his or her trade, business, or profession).

3.2. The Directive and the notarial function in electronic commerce

Recital 36 of the Directive states that the Member States may maintain restrictions for the use of electronic contracts with regard to contracts requiring by law the involvement of courts, public authorities or professions exercising public authority. This possibility likewise applies to contracts requiring the involvement of courts, public authorities or professions exercising public authority in order to have an effect with regard to third parties, as well as contracts requiring by law certification or attestation by a notary.

In this regard, Article 1.5 states that the Directive will not apply to the activities of notaries or equivalent professions to the

extent that they involve a direct and specific connection with the exercise of public authority. In a manner consistent with this, for example, in Spain, Article 5 of Information Society and Electronic Commerce Services Act 34/2002, the purpose of which is to incorporate the Directive within the Spanish legal system, states that the scope of application of the Act does not apply to services provided by notaries and property and companies registrars in exercising their respective public functions, but also the services provided by lawyers and court agents in exercising their functions of representation and defence.

Lastly, Article 9.1 of the Directive states that the Member States shall ensure that their legal system allows contracts to be concluded by electronic means, and they shall in particular ensure that the legal requirements applicable to the contractual process neither create obstacles for the use of electronic contracts, nor result in such contracts being deprived of legal effectiveness and validity on account of their having been made by electronic means.

3.3. Development of the European regulations

The development of these regulations led to the creation within the European Union of the European Digital Agenda and the Digital Single Market, based on three cornerstones: first, improved access by consumers and enterprises to digital goods and services within the European Union; second, the laying of foundations to guarantee equal conditions in the development of digital services; and third, the generation of greater benefits within the digital economy.

To this aim, secure forms of access to funding will be promoted for start-ups and SMEs, but also for larger companies by means of cross-border investment.

Not only is bank finance called on to foster trade within the EU general, but also electronic commerce specifically: non-bank or collaborative funding, either on its own or as a supplement to other forms of traditional finance, will have a key role to play in the e-commerce of the future.

The trade in digital content and goods will likewise be promoted, as a hugely important part of this digital commerce, essentially through two Proposals for Directives of the European Parliament and of the Council one on certain aspects of contracts for the supply of digital content and one on contracts for online sales and other distance sales of goods, both of them directly connecting online commerce and consumer protection.

The first Proposal for a Directive is based on the need to harmonise digital content supply contracts irrespective of the storage medium used for transfer, such as the transfer of digital content on a durable storage medium, like a CD or DVD, downloading by consumers onto their devices, transfer via the web, permission to access digital content storage capacities, or access to the use of social media. The Proposal goes further, however, since Recital 13 sets out and accepts as a means of counter-

performance for this digital content not only money, but also information about people as a value comparable to money. The object includes not only music, video files, photographs, games, or applications, but also customer-generated content, such as blogs, publications, chats, tweets, etc.

The proposal is based on a high level of consumer protection, in accordance with the idea of mistrust that prevails among consumers with regard to cross-border purchases, and in particular those conducted online, as indicated in Recital 4. One of the main factors behind this lack of trust among consumers is the uncertainty as to their essential contractual rights, and the lack of a clear contractual framework for digital content.

The key point of this standard is the concept of conformity with the contract, as defined in Article 6, and improper integration, in Article 7. As Article 9 states, the burden of proof with respect to the conformity with the contract will be on the supplier. Recitals 36 and 37 state that in the case of non-conformity with the contract, consumers should as a first step be entitled to have the digital content brought to conformity with the contract, as governed by Article 12. As a second step, the consumer should be entitled to have the price reduced or the contract terminated, as provided in Article 13. The right of a consumer to terminate the contract must be confined to those cases in which, for example, it would not be possible to bring the content to conformity, and where the non-conformity impairs the main performance features of the content.

The second Proposal for a Directive accepts that the potential of the Single Digital Market can only be fully exploited if all participants in the market enjoy ease of access to the online purchase of goods, and can participate in electronic commerce on the basis of trust. The object thereof is compatible with and supplementary to the previous Proposal, and the basis of the regulations is once again the concept of conformity, with similar regulations to the above.

As a key concept, Article 2 defines the distance sales contract as any sales contract concluded under an organised distance scheme without the simultaneous physical presence of the seller and the consumer, with the exclusive use of one or more means of distance communication, including via Internet, up to and including the time at which the contract is concluded.

4. Evolution and types of electronic commerce

The fact is that the concept of online commerce continues to generate questions as it progressively mutates, evolves, or branches out. Not all business conducted at distance is online commerce, but must all online commerce be at distance? Are contracts between those present at a distance online commerce? Queries likewise arise as regards the influence of the deferred delivery of the goods. Is it essential that the delivery not be performed physically and at the time in

question to the acquiring party? One could even consider whether a sale between two private individuals conducted via electronic channels and using portals or applications for exchange is online commerce.

Notwithstanding these theoretical questions, there is agreement that online transactions are a specific case of distance contracts in the European Directives, and that a clear distinction can be applied between the concept of electronic contract and the concept of electronic commerce. It is, though, likewise unquestionable that as electronic commerce changes, there may also be changes in its categorisation with regard to the initial concept.

4.1. By type of commercial relationship

By nature, the typical object of electronic commerce, in the strict sense, would be goods, whether tangible or intangible. With the former, there is an important difference, since physical delivery is required, and as a result one of the goals of the European Union is the elimination of barriers as regards the delivery of content. With the second there is likewise delivery in the technical sense, even if this is digital, and as a result the two Proposals for Directives have already addressed these concepts and the concept of conformity.

As a result, even if there is one single concept of e-commerce and the object thereof, depending on the type of commercial relationship a distinction may ultimately be made between:

B2G, or e-commerce between businesses and governmental agencies.

B2B, or e-commerce between businesses.

B2C, or e-commerce between businesses and consumers.

B2E, or e-commerce between businesses and employees.

C2C, or e-commerce between consumers.

4.2. By purchase channel

Likewise depending on the type of format or relationship, we may find an evolution or specialisation in mobile commerce, m-commerce, namely electronic commerce conducted by means of a telephone, tablet, or another mobile device. The reason why this type of commerce raises certain specific issues lies not only in the geographical mobility of the subjects, but also the growing increase in the consumption of content via such devices. The fundamental difference between the two is the purchase channel, which is not a traditional website but a responsive website or app, and as a result the interface and the method of purchasing are different.

Likewise, social commerce, s-commerce, is a variant of electronic commerce and of mobile commerce which involves transactions being conducted online as a result of the use of or actions within social media. In this variant of commerce, the purchasing decision, the information, and the giving of consent take place within the context of a social media platform. In other words, the product is taken to the (virtual) location of the consumer,

adding a social and shared component to the process and the outcome of the purchase.

Continuing with this natural evolution, electronic commerce will soon encounter a new space which we could call VR-commerce, which would be commerce for which the space of interaction exists within virtual reality applications and devices, as well as augmented reality (AR-commerce), and also the purchasing of physical products within videogames.

5. What can the notarial function offer to electronic commerce?

The notarial function could help provide legal certainty and security for electronic commerce, which it currently already offers for many other legal transactions.

The involvement of a notary in legal business offers authenticity and certainty in all areas in which they perform their operations, whether inheritance, corporate matters, or real estate. The legal security that notaries generate through their actions inspires trust in individuals, companies, and public institutions. This does not simply add value to the transaction, but is also a decisive economic factor in guaranteeing freedom of action within the marketplace, since there can be no freedom without certainty, and no certainty without authenticity.

In the field of electronic commerce, mobile commerce or social commerce, the role of notaries has yet to be defined, as is likewise the case with much of the technology underpinning electronic transactions, such as the true extent of an electronic signature, virtual identities, electronic addresses, and digital inheritance. Meanwhile, we still do not know which technological elements will define the electronic commerce of the future. Will blockchain be the standard? Will notaries be programming smart contracts? Will algorithms be further defining our online actions? What role will artificial intelligence have in our offices and beyond? Will crowdfunding be the standard method of finance?

All these issues have yet to be decided, but the fact is that serious reflection on all of them is needed. Their impact on people and on the adaptations that the notarial function will need to undertake in order to remain useful to society are still unknown

Even if there is no one single possibility, we should in abstract terms consider whether notarial intervention, could be of use in different moments of the contractual procedure (pre-contractual, contracting, post-contractual). At the pre-contractual point notaries could for example host or supply prior information mandated by the European consumer law or verify the General Contractual Terms (more later in the description of a Spanish project). At the point of contracting notaries could play a significant role in identifying the parties or their digital capacity (see a Dutch project). Post-contractually notaries could be involved in the means of payment or the conformity of the goods.

In most countries where notaries exercise their function, both the verification of identity and legal capacity, and the regulatory compliance of the business, are conducted by the notary, as an independent third party unrelated to the signatories, overseeing the propriety of the contractual process. In real estate matters, for example, notaries are involved both to give certainty to transactions entailing a significant amount of money, and for transactions where the value or price paid is relatively small, since their involvement is based on the object (real estate), not on the value.

A similar rationale could be considered for electronic commerce, since in this area there is a coexistence of movable assets and rights or services possibly entailing a significant economic amount. Such dealings should not be subject to any lesser diligence or security in their key elements: subjects, object, and form.

5.1. Generating trust regarding the identity of the contractual parties

One of the essential characteristics of the notariat is the verification of the identity of the parties appearing before the notary upon the conclusion of an act of legal business.

In electronic commerce, this could be applied to both the company and the consumer.

There are in fact already some interesting initiatives, such as the Dutch notariat's notarisID project, to which we will return later, or that of the notariat of Quebec, in which certain notaries are authorised to act as identity verification agents to guarantee that the transactions in which the parties are involved are performed by those claimed. In Spain, for example, notaries can also issue electronic certificates and legitimate electronic signatures.

With regard to the identification of the companies or professionals offering their services or products, this could help generate a positive and valuable online reputation with regard to them, resulting in trust both in them and in their business. In terms of the identification of consumers, it could help prevent companies from selling products or providing services to individuals who, for whatever reason, might wish to receive or acquire them without being legally entitled, such as those under legal age, or persons whose capacity has been modified by the courts.

5.2. Generating trust regarding the object

Trust with regard to means of payment applies to the physical security of the payment method, the legal certainty of the transaction and the degree of trust held in the purchaser or vendor, which is intrinsically tied to the credibility of said party in commercial dealings, whether to offer services or products, or to pay for them.

The European Banking Authority (EBA) submitted proposals to establish what it refers to as strong customer authentication (SCA) in connection with Directive 2015/2366, of 25 November 2015, in order to perform payment services in the internal market, also known as PSD2 (Payment Services Directive 2), which

subjects practically all payments to an additional authentication requirement, such as two-factor authentication.

These days, most electronic payments are performed by means of credit cards or solutions such as PayPal, but we should not overlook the growing number of transactions using BitCoin and other crypto-currencies

However, trust can also be extended to the digital object transferred, since a third party, unrelated to and independent of the contractual parties, could act as the custodian of a digital object that does not conform with the contract, and as a result, in the event of any disputes there is a guarantee that it remains unaltered, which could provide a high level of trust in the transaction, promoting the effective application of the consumer protection mechanisms set out in European Consumer Law.

This role is typically ascribed in the marketplace to what are known as "digital notaries". In modern electronic commerce, there is no similar figure to the analogue notary, since what is referred to as digital notarisation is a conceptual transposition of the Anglo-Saxon system which does not correspond to the continental or Latin notarial structure. In fact, if any similar system exists then this is on a private and normally partial basis, such as trusted third parties, in the sense of those called on to act only by one of the parties, and there is therefore room in the marketplace for operations by a group that has gained the trust and respect of consumers, of companies and public authorities.

5.3. Generating trust in the field of data protection

One of the fundamental fears of purchasers when performing an electronic commerce transaction is that their data could be intercepted and reused by a third party, whether for fraud via the Internet, for sale to databases for online marketing purposes, or identity theft.

This fear includes both the theft of data for wrongful purposes, and hacking attacks that company databases could suffer as a result of inadequate protection, and includes bank and identity details, passwords, and security codes, but also the increasingly frequent biometric identification used, such as fingerprints, voice, iris, or facial recognition. This last point is, and will increasingly be, fundamental with regard to the securing and protection of data, since while a password or PIN code can easily be changed, biometric identification is immutable.

Data are today a common element in the counter-performance given for products for applications, and even on occasion the only counter-performance received by the offeror, since both in themselves and as a part of a database or process derived from big data, they can be used in the marketplace. In fact, the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content (COM (2015) 634 final) express

mention of payment by means of the handover or assignment of data.

Given all the above, the suppliers of products or services via electronic channels need means and resources to generate online trust, to ensure that the payer perceives the transaction to be secure. This online trust must, in order to fulfil its function, come prior to the conclusion of the legal business, thereby minimising the temptation for recourse to reparative justice with regard to electronic commerce. It must also, though, extend to the preservation of data, with companies being able to benefit from the extremely high level of security surrounding the technological infrastructure of Europe's notariats.

Important data for these purposes could for example be preserved in an authentic copy of the original, allowing a timestamp to be applied to this, verifying the precise date and the specific content of the individual data set. This authentic copy could then subsequently be used to demonstrate the existence of the contract, of any electronic signature that might have been used, and even to evaluate conformity with the object of the contract, which is the central theme of the Proposals for Directives.

II. The presence of notaries in the pre-contractual phase of e-commerce

Notarial oversight of pre-contractual acceptance of Standard Contract Terms and Conditions in online consumer contracts of goods and services.

1. Previous

Up to date, notaries have effectively exercised their competences within the field of real estate and real property acquisitions. Nonetheless, the significant participation of notaries in such markets does not hamper, but rather encourages the debate on whether it would be advisable and convenient that notaries could bring along legal certainty –an integral part of their functions- to a market out of their traditional realms.

This is the so-called “European Digital Single Market”, already defined as *“one in which the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence”.*

2. The Digital Single Market Strategy

The Commission of the European Union has placed the Digital Single Market at the heart of its Strategy, which will be further developed during the term of President Juncker (COM (2015) 192 final). By implementing this “Strategy”, the freedoms of the EU Single Market are meant to be extended to the digital sector, fostering growth and employment in Europe. The belief, then, is that its implementation will be capable of generating *"up to 250 billion euros of*

additional growth in Europe in the course of the mandate of the next Commission, thereby creating hundreds of thousands of new jobs, notably for younger job-seekers, and a vibrant knowledge-based society".

3. Fulfilment of consumer protection standards

In order to accomplish this objective, the Commission considers it as essential to remove the key differences between the online and offline worlds, and to *"break down barriers to cross-border online activity"*, including explicitly "*differences in contract and copyright law between Member States*".

Consequently, harmonizing EU standards regarding consumer protection in online trade have become one of the Commission's key initiatives aimed at facilitating –especially for SMEs- cross-border online trade. Doing so will build up trust in both cross-border purchases and sales, simply because *"one of the reasons why consumers and smaller companies do not engage more in cross-border e-commerce is because the rules that apply to these transactions can be complex, unclear and may differ between Member States"*.

4. A homogeneous EU legal framework for consumer protection

In this context, within the implementation of this initiative, the introduction of a coherent EU legal framework for consumer protection becomes particularly significant, having far-reaching consequences. On the whole, markets will function in a more smoothly and orderly manner. Secondly, offerors in any Member State will be fully aware of the standards they need to comply with (see Art. 4 Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council) before making their offer. Finally, consumers will be perfectly aware of their rights before entering into a contract realising that they enjoy the same rights wherever they purchase goods or services within the EU.

This strategic goal is basically underpinned by Article 38 of the Charter of Fundamental Rights of the European Union, which states that "*Union policies shall ensure a high level of consumer protection".* This principle is mirrored in the Title XV of the Treaty of the Functioning of the European Union (TFEU), specifically dedicated to "Consumer protection". In particular, Article 169 establishes that "*1. In order to promote the interests of consumers and to ensure a high level of consumer protection, the Union shall contribute to […] promoting their right to information, education and to organise themselves in order to safeguard their interests."*

Further, article 169.2 TFEU reads: *"2. The Union shall contribute to the attainment of the objectives referred to in paragraph 1 through: (a) measures adopted pursuant to Article 114 in the context of the completion of the internal market".*

At this point the reference to Article 114 TFEU is of utmost importance, as it asserts that the European Parliament and the Council *"shall adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market"*. It also states that the Commission, in its proposals, for the approximation of legislation on *"consumer protection will take as a base a high level of protection"* and that *"within their respective powers, the European Parliament and the Council will also seek to achieve this objective"*.

Lastly, Article 115 of the TFEU enables the Council to *act "unanimously in accordance with a special legislative procedure and after consulting the European Parliament and the Economic and Social Committee"* and "*issue directives for the approximation of such laws, regulations or administrative provisions of the Member States as directly affect the establishment or functioning of the internal market."*

5. Some concerns about the inefficient functioning of the internal market and the Directive 2011/83.

Accordingly, the Commission, in the aforementioned European Digital Single Market (DSM) "Strategy" clearly voices some concerns about the inefficient functioning of the internal market. This DSM-Strategy draws on a previous analysis initially launched by the EU Commission in 2005 with the Review of the Consumer Acquis, which was subsequently followed by the Green Paper 8 February 2007 raising some important issues. All these initiatives finally crystallised in the Directive 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council ("CRD"). This piece of EU legislation is considered as a "maximum harmonisation" Directive, and therefore, its provisions need to be fully transposed into national legislation by Member States without increasing or levelling down the degree of consumer protection granted therein, unless otherwise expressly provided for in this Directive (Art. 4 CRD).

This Directive provides the only legal framework concerning consumer rights and offerors' responsibilities that shall apply to any contract concluded between a trader and a consumer in the EU within its scope of application as set out by Article 3 CRD. In essence, it lays down the standard binding rules for the common aspects of distance and off-premises contracts in this market, which necessarily entails a high level of consumer protection (Art. 169 TFEU).

This fully harmonised regulatory frame brought considerable benefits for consumers, as wherever they are in the EU or wherever they buy from, it makes no difference: their

essential rights are the same[1]. Offerors benefit greatly from harmonisation as they only have to fulfil the legal obligations imposed by the CRD (or rather, the supposedly identical national rules transposing it), instead of complying with the 28 differing regulatory frameworks of each single Member State. This simplification of key regulatory aspects considerably increases legal certainty for both consumers and offerors.

The main scope of the Directive focuses on the retail distribution channel with the greatest potential for growth at present: the Internet. Conceived as a "cross-border space" in which the European internal market can be fully realised, the wide scope of the directive is meant to overcome the limitations stemming from the fragmentation of the rules and the existence of diverging regulatory frameworks in the Member States, which ultimately led to a considerable withdrawal of cross-border transactions, on both the supply and demand sides.

In particular, the Directive sets the focus on the main issues undermining consumer confidence, as well as on several factors deterring traders from engaging in cross-border electronic commerce. Among those causes for concern, the lack of information or insufficient legal awareness of online trade rights and responsibilities prior to the conclusion of the contract prevented both traders and consumers from engaging in cross-border online trade in the EU, while severely undermining confidence on online transactions.

In this regard, in accordance with article 169 TFEU, the Directive regulates in detail the content and scope of the statutory duty requiring traders to provide consumers with pre-contractual information. However, this requirement is regulated far more thoroughly when the transaction is completed remotely or off the business premises of the trader, mostly through the Internet.

With this Directive, the European Commission aims to achieve a true internal market, a foundational principle of the EU, through two different but complementary pathways: firstly, by imposing certain legal constraints on commercial practices performed by providers of consumer goods and services who shall comply with pre-contractual information duties; and secondly, by establishing suitable mechanisms for public monitoring, oversight, and enforcement.

It may therefore be worth concluding that, in this way, the Directive seeks to attain an objective of public interest. All of this is without prejudice to the fact that the specific regulatory constraints established by the national laws transposing the Directive also become part of the regulatory framework applicable to the contract within the context of the specific contractual relations between the offeror and the consumers or users.

6. Downsides of this regulatory framework

[1] Green Paper terminology echoing the Commission in its Communication "A citizens' agenda - Delivering results for Europe": "Wherever you are in the EU or wherever you buy from it makes no difference: your essential rights are the same" COM(2006) 211 final.

The inadequacy of mechanisms to enforce and monitor compliance with its provisions is one the main downsides of this regulatory framework. While the Directive seeks to attain an objective of common interest, i.e. the realisation of a true internal market in the EU, compliance with consumer contract law depends on whether the parties will voluntarily abide by the rules or, whether they would enforce them ex post by claiming a breach of a statutory provision, either before the administrative authorities or, where applicable, before the courts.

The foregoing reveals the following shortcomings: a) there are no effective mechanisms in place to ensure that the contract offer complies *ex ante* with the specific legal obligations imposed by the CRD, and, b) there are no effective mechanisms in place to monitor and enforce compliance on part of the offeror when trading with consumers. These weaknesses become especially important in the context of online transactions, where the offer and trade itself are conducted through the Internet.

The directive understands that these shortcomings may be remedied by the Member States, at least partially, through the enactment of national legislation (falling outside the scope of EU institutions' competence).

7. Notaries could play a valuable role in the satisfactory functioning of the Digital Single Market: A Spanish proposal - The Notarial Seal of Conformity of the Standard Contract Terms

Considering that in countries within the civil law tradition, notaries are accorded with the status of public office holder formally fulfilling the requirements of impartiality and independence; and considering that notaries have been granted with the competence to verify that private contracts are lawfully concluded by private stakeholders and fully comply with the imperative provisions and public policies of national laws; it might be worth assessing whether they could play a valuable role in the satisfactory functioning of the Digital Single Market, and more specifically, in the course of the pre-contractual phase of online transactions.

Notaries could be the public authority vested with the competence, when awarding contracts, to guarantee that the parties to a contract effectively comply with the imperative provisions and public policies.

In this regard, notaries are particularly suited to fulfil the role of ensuring that, during the pre-contractual phase, consumers will receive sufficient information and impartial legal advice on the economic and legal consequences they will face, should they agree on the terms and conditions of the contract.

Furthermore, notaries might be in the position to perform an essential function as gatekeepers –or ex-ante surveyors- within the prominent realm of the provision of consumer goods and services in online transactions. Thus, notaries may contribute to achieve

compliance with common EU standards to ensure a high level of consumer protection as established by Directive 2011/83.

Likewise, notaries may verify that the offer of online good and services will take place in accordance with the Standard Contract Terms and Conditions set out in advance. Usually, on their websites, offerors make these standard contract terms readily available to consumers wishing to acquire their goods and services. At present, these terms are not examined by any authority prior to their publication on the offeror's webpage. No authority verifies whether they meet the high standards of EU consumer protection or not. There are no public mechanisms to enforce "ex ante" compliance as regards the fulfilment of legal obligations within the sphere of online trade of goods and services. In summary, the fundamental right to consumer protection, as a fundamental principle of the Treaty and EU legal order, might be seriously compromised in the pre-contractual phase of online trade as a consequence of all these shortcomings. Further, compliance with standard contract terms merely relies on the inherent responsibility of the offerors (who would fulfil their legal obligations willingly), on the pre-contractual due-diligence of consumers (who would exercise their rights in a timely and responsible manner) and, finally, on the unsatisfactory ex-post enforcement mechanisms before the courts, in the unlikely event that consumers may seek legal redress after they have suffered some damage as a result of a potential breach of their rights (all this assuming they can afford the legal costs).

Should notaries be entrusted with examining the Standard Contract Terms and Conditions of online consumer contracts prior to its publication on the offeror's website, and should they confirm that these terms actually comply with Art. 6 CRD, consumer confidence will be reinforced leading to the conviction that the consumer right to be informed in the pre-contractual phase has been successfully fulfilled. Most importantly, this assessment ex ante would promote voluntary compliance – similarly to soft law- with the common EU standards (these provisions also concern competition) applying equally to all offerors and protecting all consumers on equal terms.

Should the ex-ante examination have a positive outcome, a "Notary Seal of Conformity" (NSC) that may be put on those Standard Contract Terms that have successfully passed the test of Art. 6 CRD. This NSC would come with the additional advantage of serving as a "seal of quality" for the law-abiding offerors.

Thus, even if consumers do not read the clauses of the contract, which typically occurs, they will still have the conviction that the offeror has fulfilled its duties, whenever they spot this seal, as it would mean that a notary has already put Standard Contract Terms against to the test of Art. 6 CRD, thereby guaranteeing that consumer rights of information for distance and off-premises contracts have been properly protected.

Of course, any request on behalf of an offeror to add the NSC to their Standard Contract Terms shall be made on a voluntary basis.

The "Notary Seal of Conformity" would entail the following effects:

- It would mean that the offeror has complied with the consumer/user protection rules envisaged in Art. 6 Directive 2011/83.

- The Standard Contract Terms with the NSC could be hosted on the national notaries' website, so that they could be consulted and downloaded by parties with vested interests, as well as by those public authorities using a secure verification code (SVC).

- When spotting the NSC, consumers will understand that their rights conferred upon them by Art. 6 CRD have been efficiently protected.

- Likewise, consumers will trust that the General Terms and Conditions filed in this database are in force and fully comply with the consumer rights set out in Art. 6 CRD.

The thorough and sound legal training of notaries ensures that they will perform this function guaranteeing and safeguarding consumer rights effectively. This will surely encourage consumers to conclude cross-border online transactions, irrespective of the Member State where the offeror may have its premises.

Accordingly, the notaries may collaborate with the European Commission in the implementation of "Digital Single Market Strategy" in the conviction that their active involvement will have a positive impact on the digital internal market. Actually, by performing their monitoring role, notaries will contribute to build up trust in offerors and consumers, which will ultimately increase online trade of goods and services throughout the EU.

Notaries have made a substantial investment in technology in order to provide their services via online within the Digital Single Market. For this proposal, this could entail, broadly speaking, that notaries will receive and examine the offerors' proposed Standard Contract Terms electronically to verify its compliance with Art. 6. Further, once this process of legal compliance has been completed, notaries from the offeror's Member State will stamp the "Notary Seal of Conformity" on the legal document, which will subsequently be posted on the specific section of the website designated for this purpose, making the sealed Standard Contract Terms readily available for any consumer wishing to examine them.

Of course, once the NSC has been set, the Standard Contract Terms may be sent to the offeror with a Secure Verification Code (SVC) so that it could be posted on their own website. Alternatively, a link could similarly be placed on the offeror's website leading to the official website of the national Notariat and more specifically, to the section hosting Standard Contract Terms. In this manner, consumers will be able to download the Standard Contract Terms with the NSC in a secure and reliable manner, since the authenticity of the seal will be guaranteed in

all cases by the SVC issued by the Notary, either from the offeror's website or the Notariat hosting website.

The Standard Contract Terms will be available in the language of the offeror's State and in the language of the countries where the offer is directed, as required by CRD.

Additionally, the national Notariat hosting the Standard Contract Terms with the NSC could issue a multilingual Certificate, at the request of the offeror, in accordance with the approved template, i.e. by the CNUE or the EU Commission, signifying that the Standard Contract Terms comply with the Art. 6 CRD. This Certificate will be added to the Standard Contract Terms that have been issued with the NSC.

According this proposal, for the process of granting an NSC, the competent notary have to verify compliance of the Standard Contract Terms with Art. 6 CRD and then grants the NSC. As a general rule, since Art. 6 CRD is a binding provision of general application in all EU Member States, the offeror, given the choice, would usually submit his Standard Contract Terms to an authorised notary from the State where he has his habitual residence. In principle, it would be enough if only one notary may verify the Standard Contract Terms of the offeror. That notary could be either the competent notary of the Member State where the offeror has his habitual residence, or even the competent notary of the Member State where the offeror has a subsidiary, a branch or any other establishment set up in accordance with EU law. Further, the competent notary could also be designated among of those from the Member State where the offeror makes his online offer, that is, from the Member State where the consumer has his habitual residence.

At this point, as regards the choice of applicable law against which the designated notary will have to test that the Standard Contract Terms complies with Art. 6 CRD, it might be worth mentioning that Art. 6 Rome I Regulation states that when one of the parties in the contract is a consumer, the contract "*shall be governed by the law of the country where the consumer has his habitual residence*". This means that the test of compliance would be carried out according to the national law transposing Art. 6 CRD in the consumer forum, while there is no reason why the notary could be designated in any other Member State, as before mentioned. In any case, the outcome of the compliance test may be similar in both cases, whether the notary is appointed in the Member State of the consumer or in the Member State of the offeror, since, in principle, the national acts transposing Directive 2011/83 may have the same contents.

Considering that Art. 6 CRD specifically impose imperative pre-contractual information duties upon the offerors ("*unwaivable rights for consumers"*); considering that notaries may assume the supervision of compliance of the Standard Contract Terms submitted by the offeror in accordance with Art. 6 CRD, it might

be worth concluding that their professional liability would be limited: notaries shall only verify that offerors have complied with the duties imposed upon them by Art. 6 CRD. In a nutshell, notaries shall only supervise compliance with the duties derived from this specific provision, excluding the supervision of any other legal obligation arising from the Unfair Contract Terms Directive 93/13, or any other EU consumer applicable laws.

At this time, it might be worth remembering that Art. 4 CRD provides that: *"Member States shall not maintain or introduce, in their national law, provisions diverging from those laid down in this Directive, including more or less stringent provisions to ensure a different level of consumer protection, unless otherwise provided for in this Directive."* Accordingly, the requirements contained in Art. 6 CRD are imperative, being their content basically the same on all the Member States and its interpretation ultimately subject to the jurisdiction of the Court of Justice of the European Union, whose case law is equally binding on all Member States.

According of this proposal, all the costs resulting from requesting the supervision as regards compliance of the Standard Contract Terms of with Art 6 CRD will be borne by the offeror, including all the expenses incurred in granting the NSC as well as all the website fees to host the Standard Contract Terms on the Notariat website and allowing for consumers to effectively access and download all relevant documents in this regard.

All the costs resulting from obtaining the multilingual Certificate of the Standard Contract Terms accompanying the NSC could be equally borne by the offeror, including hosting website fees on behalf of the Notariat website, as well as any expenses incurred in allowing effective access to documents and downloads by consumers using the pertinent SCV.

All in all, considered, the notaries might find worth considering the desirability of encouraging further reflection and in-depth discussion on their effective involvement in both the pre-contractual and the contractual phase of the online trade of goods and services.

This is an initiative easy to implement in those countries within the civil law tradition where public notaries already exist. In those countries where there is not a similar authority, their functions could be performed by any public officer designated by the Member State adequately suited to carry out this role.

In any event, it should be borne in mind that once the Standard Contract Terms have been provided with the NSC, its validity might not only extend its effects to all EU citizens engaging in online trade, but also to any consumer wishing to acquire goods and services from an EU offeror, regardless of their country of origin or habitual residence. Consequently, any consumer from overseas acquiring EU goods and services online could similarly be able to obtain an electronic copy of the Standard Contract Terms, proving

effective even beyond the EU borders. Needless to say, any consumer irrespective of their residence may understand the meaning of acquiring goods and services from an EU offeror meeting the legal requirements certified by the NSC, and consequently, would rather prefer to enter into a contract with a trader holding this seal of quality, as it represents a higher level of consumer protection. After all, the NSC is a seal of quality certifying that the Standard Contract Terms issued by EU offeror comply with the pre-contractual rights of consumers in the online contracting of goods and services as required by Art. 6 CRD.

Final mention should be made of a number of the benefits that the NSC could deliver:

For the offeror: Public oversight through the NSC would serve to alleviate the burden imposed upon offerors to comply with the legal requirements regarding each individual consumer as established by Art. 6 CRD.

The Notary, as a trusted third party, guarantees that the content of the clauses complies with Art. 6 CRD. Through a NSC, the offeror:

a. Conveys greater trust to potential purchasers.

b. Enhances its brand image, offer and professionalism.

c. Becomes a distinctive offeror, as belonging to the group of "the law-abiding offerors".

For the European Digital Single Market: The rise in the levels of compliance with the legal obligations established by Art. 6 CRD will ultimately contribute to foster competition and improve the functioning of the market competition as a whole.

For consumers: The legal position of consumers will be improved as a result of achieving higher rates of compliance with Art. CRD. At present, consumers do not usually read the clauses of the contracts they enter into, but instead, they react later when their rights have been damaged. On a number of occasions, their lack of legal awareness prevents them from taking further legal action. On other occasions, consumers seek collective redress, deteriorating consumer confidence and leading ultimately to a decline in consumption rates.

In this regard, by performing their surveillance role, notaries will help to increase compliance rates with the legal obligations arising from Art. 6 CRD upon the offeror, actively contributing to the enhancement of the European Single Digital Market. Additionally, consumers will rely on notaries as guarantors of their rights conferred upon them by Art. 6 CRD. If consumers notice that the Standard Contract Terms set out by the offeror have been subsequently assessed by notaries and awarded the NSA, consumers will be more willing to trade online. Further, consumers will be provided with an instrument enabling them to distinguish between law-abiding offerors having been granted the NSC, and those that lack this endorsement.

For notaries: Notaries will be regarded as the ultimate guarantors of compliance with Art. 6

CRD as well as protectors of consumer rights, since their role will be connected with the strengthening of the Digital Single Market and the development of EU Digital Single Market Strategy.

III. The notariat and e-commerce subjects

1. The position of the notariat as regards e-commerce subjects

One of the essential elements in any legal business is the proper identification of the subjects who are party to it, the verification of their capacity, their legitimate standing in order to act, and the existence of sufficient powers of attorney or entitlements. All these circumstances apply directly to notarial operations in the physical world, and have over the years been undertaken by the continental notariat, with considerable success and extremely low levels of litigation.

The commencement of similar operations within the digital market is a matter of complex debate, since notaries essentially and fundamentally act directly and in person, and the consideration of actions performed by an indirect and electronic rather than face-to-face method must not lose sight of this concept.

However, if the proposal is for notaries to act within the digital environment, it would make sense to consider whether there is any way of intervening in the identification and capacity of subjects operating within digital commerce, with regard both to users and to companies.

As regards users, one first group of beneficiaries from notarial intervention would include those under legal age, persons with limited capacity and their representatives, and the interested parties would therefore be those affected themselves, but also their legal representatives, parents or guardians, who would enjoy the guarantee of oversight or supervision. This would furthermore provide a method of granting autonomy to those affected by a judicial modification of their legal capacity, while remaining at all times subject to preventive control of access to certain transactions. For example, the existence of restrictions on a person jeopardising their assets through online betting sites, in the same way that restrictions are applied to physical access to certain gaming arcades or casinos.

Even those who are of legal age and are not subject to any restrictions on their capacity might need or find it desirable to have a system of prior identification for the persons with whom they interact online. For example, an adult may wish to be certain that he or she is interacting with other adults on a social media platform, or that the comments that a person publishes via a public digital platform can be traced, to ensure that in the event of any unlawful comment, the perpetrator can be properly prosecuted.

The second group would be the companies or individuals providing online services. This

could serve to strengthen their brand and gain online reputation, while at the same time fulfilling a possible legal obligation to ensure that the service is provided to parties entitled to request it. For example, that alcohol is sold only to those over legal age.

Meanwhile, though, companies can also generate such trust and security by properly identifying themselves in their communications, website, or social media profiles. How can we know whether a company posting its business on Google is who it says it is? It is true that there are verified accounts, but we are not talking here about major companies with which we are all familiar. We are talking about SMEs. We are talking about legal certainty. And who better, then, that a notary to provide that guarantee, in a secure and immediate manner?

2. Identification and digital capacity

2.1. Identification of the digital business operator

There is at present no public institution or any official, impartial third party capable of guaranteeing in electronic commerce the identity of the company or professional offering the service prior to the legal transaction, with any confirmation actions or claims occurring subsequently.

As a result, proper identification of the digital business operator and the resources available to it in order to perform sales or provide services online, whether via a website, application or social media platform which is to be used for the transaction, could increase the trust of consumers, who would have unquestionable confirmation that the person behind an online offering is who they claim to be. In short, this would be a way of guaranteeing that in all cases consumers would be able to know who the ultimate owner of a website application is.

Such companies or professionals must provide consumers with information in order to comply with all the obligations imposed on them not only in the EU regulations, but also on a supplementary basis in the corresponding national regulations. Likewise, they must be in a position to guarantee the replacement or repair of the product in the event of non-conformity of a purchased product. As a result, the need to know in advance for whom, where, and under which regulations consumers can exercise their rights, could prove fundamental.

Nonetheless, notaries should be kept outside the actual commercial activity of the companies they provide their service to so that they do not lose their standing as an impartial third party. In other words, notaries can assist in digital commerce, but must take particular care not to become digital traders themselves.

2.2. Identification of the digital consumer

One inevitable question that is already being considered is whether identification of the consumer within the digital context is desirable or necessary. The reply seems increasingly clear: yes, it is desirable to provide those acquiring or contracting goods

or services within a digital context with an unequivocal means of identifying themselves in their online transactions.

If the question raised is what form this identification can take, then the answer is clearly open to debate. The first and perhaps most immediate response would be to consider electronic signatures, above all following Regulation (EU) No. 910/2014, of the European Parliament and of the Council, of 23 July 2014 (the eIDAS Regulation), which may provide a valid means of identification of the signatory, just as a fingerprint or some other form of biometric identification could ultimately also do. These methods of electronic identification are progressively being incorporated within National Identity documents, some of which, as in Spain, include an electronic signature, while others are in the process of incorporating this.

In Spain, for example, the traditional National Identity Document is of value in itself not only as accreditation of the identity of the holder, but also other personal details, such as nationality. This concept evolved into the Electronic National Identity Document (or DNIe), which is now the most widespread means of remote electronic identification in Spain, at least in potential terms, since according to official figures from the National Police and the Ministry of the Interior, more than 45 million DNIe cards have been issued, giving some idea of the potential that this document has to popularise electronic signature.

However, the fact that so many electronic identity documents have been issued does not mean that use of them is equally widespread: they were not all issued at once, not all are operational, and not every household has a smart card reader. In fact, the percentage of Spanish users who had used their card on some occasion in 2016 was less than 15 percent for dealings with public authorities, and less than 5 percent for dealings with private enterprises, such as online banking.

As a result, the fact of having an electronic, free, official identity document issued by the public authorities of a country would not, for the moment, seem to provide a guarantee that this form of electronic ID will ultimately fulfil its function.

The second aspect requiring reflection is if there is a need for documents with a more extensive object, providing not only a signature, but certain attributes giving greater knowledge and certainty as to identity, and even a degree of the legal capacity on the part of the person using them, and which can be used on a universal basis. In short, the question is: can a concept of single digital identification combining all different virtual identities be developed?

In response to this question, there needs to be a distinction between the identification of a natural or legal person and the identity or identities that may be used in the digital world in general, and in online and social commerce in particular, since one single person could be identified for different electronic services or

social media platforms with different public or private profiles.

The term "identity" may be defined as a set of inherent features of an individual, characterising them with regard to others. We may here cite three key points of this concept: first, the objective element (the set of features), second, the subjective element (they are combined in a person), and the third, the element of differentiation or cohesion between the subjective and objective aspects.

This element of cohesion is always a natural or legal person. As a result, although one single user might have several profiles, accounts or virtual identities, there is always one natural or legal person behind them, and it may on occasion be desirable for that person to be identified, one such situation being when accessing electronic commerce.

This identification can occur at two points, either when accessing the network, raising the possibility of demanding unequivocal identification every time a subject accesses the Internet, or on individual access to certain social media networks, when acquiring certain products or contracting services, including any website or service that could generate a particularly significant relationship in economic or personal terms, such as online gambling websites, the sale or purchase of goods, social media networks, forums, etc.

As a result, if the response is positive, we should reflect on who could or should issue such digital IDs or identity documents, and whether we as notaries would in such circumstances be in a position to issue them.

2.3. Digital legal capacity

One question intrinsically tied to the above is whether a concept of digital capacity could ultimately be developed, by means of which the electronic identification certificate would include not only the identity of the holder, but other objective data serving to ascertain an element of capacity on the part of the contracting party, such as being of legal age, or having no restrictions imposed on contractual entitlements.

In order to further this idea, we will make reference to the notarisID concept developed by the Dutch notariat. First we need to clarify its operational scope and the effects that it can generate. A confirmation of the capacity of a person can never be performed in general and a priori except in court proceedings for incapacitation under court guardianship, and as a result the issuance of a digital ID would not constitute a general notarial attestation as to a person's capacity, but rather confirmation of the absence of any judicial limitation on that capacity.

The logical question that at least we as notaries should ask is: could a system like this ultimately, and indirectly, result in a notarial judgment of capacity? The response, although complex, must be in the negative.

The reason being that, if the business to be undertaken lies within the sphere of public documents, it is a notary who confirms the individual's identity, whether they are of legal

age, who reaches a judgment as to capacity, to ascertain that there are no limitations on capacity, that the individual is not acting under coercion or through error, is able to understand the effects of granting consent, that the individual's will is genuinely expressed in the document, etc. This notarial judgment of the capacity of a person is highly sensitive and complex, and cannot be recorded as an item of data in a token or on a smartcard.

Nonetheless, in purely private actions, such as those resulting from electronic commerce, the Notary is not there to verify the capacity of the person and instead the parties themselves must ensure this. Here, such digital ID systems, which serve to supplement ordinary diligence, could have a role to play.

3. The Dutch project: notarisID

In the Netherlands, they have begun to develop an online personal identification system by means of notarial certificates, by the name of notarisID, established as a means of identification fully compliant with the provisions of Regulation (EU) No. 910/2014, of the European Parliament and of the Council, of 23 July 2014 (the eIDAS Regulation).

The aim of this project is that those requesting the provision of services in the private sector and from public authorities should have an electronic means of identification allowing them unequivocally to conclude dealings in a digital manner.

It should be mentioned, in order to contextualise the project and the possible implications of the concept, that this would under no circumstances substitute traditional notarial identification for those dealings that so require, such as real estate transactions or the incorporation of commercial companies.

This form of identification is equivalent to an electronic identity certificate issued by the Dutch Government (DigiID), and is therefore an alternative to this. It should furthermore be borne in mind, as mentioned above, that some countries, such as Spain, already have an electronic identity document.

Nonetheless, it reveals certain peculiarities to be reflected on, the first of these being that these certificates are not issued by a public authority, the Social Security, or the police, but by the Dutch notariat. The reason for this is that notaries have positioned themselves as the ideal guarantors of trust as regards the identification of individuals, and aim to extend this certainty to online identification: it is notaries who issue the certificate having physically identified the user at their office, referring this to the notarisID application that the user has on their mobile phone, which can be used from that point onwards together with a PIN chosen by the users themselves.

The second and important specificity is that the personal data of users are in all cases protected, since first of all it is the users themselves who control the data or attributes included on the certificate, and furthermore the specific data are never handed over or communicated, and instead a simple yes/no response is given to the question asked by the service provider. For example, in order to

ascertain whether a person is or is not of legal age, the system does not return the date and place of birth, but a yes/no response to the question "Is this person of legal age?"

The third, is that the certificate has no cost associated with it for users of the service.

IV. The relationship between blockchain, notaries and e-commerce

1. Notarial trust and digital trust

The "*raison d'être*" of the notariat lies in trust, which is based both on the legal certainty that notaries convey as professionals skilled in resolving complex legal problems, and on the security offered that the consequences of users' legal dealings will be as they expected and wished.

The notarial system is based on the concept of preventive justice, in which notaries advise the interested parties, devise and author public instruments and keep them in their safekeeping in their archives or protocols, guaranteeing their existence, unaltered status, and the legitimate interests of those accessing them. The consequence is to generate trust and legal certainty in the before, the during and the after of legal acts.

Currently, the trust of users and public authorities in the notarial service is unquestionable, but it can likewise not be refuted that the current technological situation allows us to postulate for certain applications or services a type of electronic, mathematical, or digital trust that could interfere or overlap with notarial guarantees.

This digital trust is based on encryption and algorithms, two intrinsically connected concepts. Specifically, encryption is a technique that allows the use of algorithms to conceal information, making it visible only to those able to decrypt it, namely the parties given access to the algorithm used to encipher or encrypt the information. Here we find a clear relationship between analogue and digital trust: certainty of consequence, trust that in the case of a particular event we will obtain a specific response.

This concept would in principle seem to be confined to operations of the mathematical or scientific type, but new encryption techniques, the growing applications of algorithms, and even in the future the combination of both with artificial intelligence, mean that this concept of mathematical trust or logic is gradually finding its way into the sphere of documents, where the information analysed, encrypted or transferred represents data other than a number or a mathematical solution.

In other words, the applications of encryption, of the blockchain or artificial intelligence in the legal sphere, are now becoming a reality, giving rise to a debate as to what type of trust is more efficient, whether the two are complementary, whether one should be superior to the other, while maintaining both, or if the less efficient should disappear in favour of the more efficient. This is a similar

conflict to that which existed only a few years ago when mention was first made of electronic signatures, and the possible collisions with the notarial function.

In fact, Regulation (EU) No. 910/2014, of the European Parliament and of the Council, of 23 July 2014 (eIDAS Regulation) on electronic identification and trust services for electronic transactions in the internal market, directly addresses the concept of electronic trust, although the Regulation does not affect national or EU Law with regard to the execution and validity of contracts or other legal or procedural obligations with regard to form.

It is clear, then, that for the moment the object of the Regulation is not to replace traditional trust with electronic trust in every aspect, including notarial operations, since it likewise does not alter or impact on the regime of public and private instruments, and as a result, with regard to the former we will continue to need authorisation before a competent public official, typically a notary. Meanwhile, the Regulation also adds that in addition it should not affect national form requirements pertaining to public registers, in particular commercial and land registers, which clearly means that the regulations regarding the registration of documents in national registers are likewise unaffected. It is also clear, though, that this electronic trust is now beginning to be accepted in regulatory terms and is being given legal effects, in particular of a procedural nature.

2. Is electronic trust infallible?

If the legal certainty offered by digital trust is so clear, then, could we ask ourselves the question: are there errors in the algorithms?

Trust in the predictability of the result is derived from trust in the actual algorithm used and in the programmer, the efficiency of their programming and the reliability of the data employed and processed, giving us absolute certainty that if the data are correct and the algorithm has been properly programmed, then the result will likewise be correct.

Although the answer should be a positive one, it is irrefutable that there are numerous points at which a failure can occur with regard to an algorithm: faulty data, inappropriate interpretations, or incorrect processes or errors in the source code or in the interface, and even a poor relationship between the data-generating devices could give rise to an illogical result.

It is at this point that we need to consider the compatibility between the two types of trust, since we must trust not only in the algorithm or the blockchain, but also the subject entering, processing, and interpreting the data. In other words, in order for objective trust to take full effect, it may be that subjective trust is required.

3. The compatibility of the two types of trust

Just as the notarial function was supplemented and enriched by the introduction of electronic signatures, these new forms of digital trust may also be

compatible with notarial operations. In fact, they not only may but must be compatible, since analogue trust cannot survive on its own in an increasingly digitised world, while conversely, electronic trust likewise cannot do without analogue or traditional persons or systems of trust, in order for them to take full effect, even if only from a strictly legal perspective.

The threat here is perhaps not so much blockchain but artificial intelligence if, in the future, it is in a position to overlap or even replace qualified professionals. For the moment, this assertion is not yet a realistic threat, since the current technical state of the art only allows applications for simple algorithms where there is no contradiction, paradox, or interrelated decisions.

4. The position of blockchain within the legal system

Electronic trust in the blockchain is one of the types of electronic trust arousing the greatest expectations. For some, it is a great and disruptive step forward in whatever field it may be applied to. For others, it offers absolutely nothing in legal dealings. In any event, its economic and technical significance is unquestionable, since in 2017 the expectation is that 75 percent of financial institutions, and according to IBM 20 percent of the most important among them, will have a blockchain-based solution in everyday use, including contractual applications. The fintech market has taken off, and with it for the moment insurtech and even legaltech.

Blockchain is simply a chain beginning with an initial block, which is connected in an un-modifiable and permanent manner to the next, and so on successively without interruption and with no possibility of any gap between blocks, with each block containing a record including, for each transaction added to the chain, a hash with data as to its existence and the precise date and time.

These blocks, and the chain that supports them, were created to register BitCoin transactions, but the idea soon developed that the transaction registered in a blockchain could have a reference to a digital file added, which could be any document, including a text. And if it could be a text, then it could be a contract or a will which, having been archived or registered in the blockchain can generate an appearance of certainty that the content remains unmodified and that it existed with that specific content on a particular date and at a particular time.

Notaries have access to various key aspects which a blockchain does not itself enjoy, such as oversight of individual legality performed by each notary, recognised status as a public function or authority in many jurisdictions, and civil and even criminal liability on occasion as a result of notarial instruments and protocols. In other words, under the current system the notary is responsible, but we do not know who would be responsible for the functioning of the blockchain, although we could in theory detect responsible parties in the case of a private blockchain.

The value of the document in a blockchain must also be clarified. This remains a private document, and the blockchain does not preserve a copy of it, and so can likewise not stand in for the function of notaries as the custodians of the original instruments signed by the parties. The value of the timestamp generated when the file is included in the blockchain is a different matter, and this could correspond to the non-qualified timestamps referred to in Article 41 of Regulation 910/2014 (eIDAS), which means that it would not be denied legal effect and admissibility as evidence in legal proceedings.

Whatever the case, the fact is that no technology is in itself either good or bad. Blockchain specifically allows for multiple uses, with the common feature of a record contained within a chain of blocks, which may be public or private, but has no effect on the individual registering it, the content registered or how this is done. In other words, this technical resource allows us to guarantee the record, its traceability or acknowledged confirmation, but we cannot presume that what is registered, traced, or acknowledged is accurate, legal and valid.

5. Blockchain and notaries

The problem is that the relationship between blockchain and the legal professions is based on two false premises: first, there is a confusion between the technical resource to provide a particular service, and the provision of the service; and the second, the suggestion of a clash between this technical resource and the service provider.

In truth, blockchain is simply the technical resource that will be used by professionals in fulfilling their function, such as in order to guarantee the integrity of a document, but the resource (blockchain) replaces neither the professional (who, for example, draws up the contract), nor the document itself (which is not incorporated within the blockchain). Now, it may be that this technical resource is more efficient than other methods.

As a consequence of all the above, the impact of encryption in general, and of blockchain in particular, on the notarial profession, needs to be considered. Essentially a potential notarial private blockchain could be an option that could potentially improve the notarial function, while furthermore specifying the point at which the service is provided.

The point prior to signature of the contract is perhaps the least open to improvement, though it may be thought that sending a notary documents recorded in a blockchain to draw up an authentic instrument could provide a greater guarantee of authenticity and unalterable status. At the point when consent is given, one could debate the usage of electronic means of identification based on electronic signature or blockchain, means of payment if electronic money or crypto-currencies such as BitCoin are used, or the use of the blockchain registration of electronic documents a copy of which is held in the

safekeeping of the notary, the typical case being the depositing of digital files.

However, the inherent nature of Blockchain means that it is the point after execution of the instrument that is perhaps most open to improvement through the application of blockchain technology, in particular the circulation of electronic copies the unmodifiable status and integrity of which are based on the existence of a private notarial blockchain, which could even be supranational and European.

6. Blockchain and property registers

One of the legal sectors in which blockchain is achieving the greatest penetration is the increasing number of initiatives to transfer property registers to a blockchain-based system. The justification for the use of blockchain is founded on three different aspects: economic reasons, combating fraud and security of title.

They are all based on the idea that a property with properly configured title, which is also where necessary duly registered, will enjoy faster and simpler access to finance, by eliminating or substantially reducing the creditor's risks. However, as typically occurs in those systems where the point of performance and definition of the legal business takes place before a notary, it is specifically this moment, and none other, that is the key point in establishing the business, with registration being a subsequent, protective step.

Allowing any private document, drawn up by any individual, to have access to the blockchain, and hence public registration, would be tantamount to leaving the State shorn of evidence and information, which would be a substantial step backwards. It should also be recalled that a record is as secure, reliable, and strong as is the title that it reports, and there is little point in having an unmodifiable Register based on electronic trust, if the titles recorded in it are defective, or lack rigour or quality.

The first countries to propose a system of this kind were Honduras and the Republic of Georgia, although the most ambitious project is in Ghana, given its potential expansion to nearly the whole of the African continent, the aim being to register property titles by means of blockchain, supporting the public registration of these titles and their enforcement status by means of smart contracts, serving to improve real estate guarantees for micro-credits and governmental investment contracts. However, there are also initiatives in Europe, since Sweden has likewise announced its intention to work on a concept for the use of blockchain and smart contracts for sales of real estate assets and for the land register.

V. Digital inheritance

1. Digital inheritance in connection with analogue inheritance

One of the cornerstones of holding the right of succession is the concept that the death of a

person constitutes the termination of their legal personality, and the commencement of succession in favour of their heirs. Another such cornerstone is the concept that the inheritance comprises all assets, rights and obligations of a person that do not expire upon death.

The third is the existence of figures in the succession playing different roles and having different effects: the heir is the person who succeeds another in all their goods and rights, assets, and liabilities, as a kind of continuation of the personality of the deceased. A legatee is one who succeeds another with regard to a specific asset or right, as expressly bequeathed by the testator. The executor of the will is responsible for specific actions when a person dies, ensuring that the terms of the will are duly fulfilled.

This same structure of succession, based on Roman foundations, can likewise be transferred to Anglo-Saxon systems of succession, in which the personal representative plays the key role in the procedure.

The phenomenon of succession has progressively become more complex as people's estates have expanded and become more diverse: where new legal objects or types of property or personal relationship which are hard to fit into the pre-existing categories arise, then eventually the question emerges as to how to handle their transfer upon death.

This is precisely what is now happening with new digital relationships and objects, since not only are there few specific regulations in this regard, but furthermore these relationships have such distinctive aspects and characteristics that we must even consider whether or not they lie within the scope of the traditional law of succession. The question we need to begin to ask ourselves, then, is whether or not this is an inheritance that is separate from the ordinary procedure.

It is hard to argue that digital inheritance is a set of individual relationships separate from non-digital inheritance, since however different the principles governing the scope of electronic relationships and their objects might be, this does not offer a decisive reason to fragment the succession of an individual or to relax or modify universal principles of succession, above all since within the digital inheritance itself we come across a diverse range of content, including personal and absolutely personal rights, asset rights with both physical and digital content, succession in legal relationships before third parties, intellectual property rights, etc.

This notwithstanding, it is likewise true that consideration must be given to these specific features, and solutions provided within the law of succession serving to accommodate the digital inheritance within an individual's general inheritance, as simply another part of it: the phenomenon of digital succession should not be handle separately, but instead the traditional structure of succession must be adapted to the digital reality, and those

situations that cannot be accommodated within any of the traditional categories new solutions within this structure must be found.

In short, the transfer to our known concepts of the current reality, in which the boundaries between personal and social relationships are blurred, when speaking of social media, blogs, and digital assets, making it hard to know where one begins and the other ends.

It is no coincidence that one basic principle of the interpretation of law is to prevent it from becoming ossified, by means of corrective interpretation based on the social reality of the era to which the standard must be applied, as required, for example, by Article 3 of the Spanish Civil Code.

2. Digital assets

Digital assets, as with the general concepts of the succession or inheritance of property, in the objective sense, are complex because of the diverse relationships, assets and rights that comprise the digital estate.

These digital assets, rights and relationships may, like all other analogue assets, rights, and relationships, belong to natural or legal persons. This chapter will focus on the situations derived from the death of a natural person, since if the social media profile, email, or digital files belong to a legal person, the system to be applied would be that corresponding to the winding-up, liquidation and termination of the personality of said entity.

The focus on digital inheritance must therefore be diverse, providing a solution both to the transfer of digital content and the legitimation of successors with regard to those service providers with which the deceased had established relationships.

2.1. The transfer of digital files

Digital files created by the deceased, of whatever type they might be (photographs, video, audio, documents, etc.) would be subject to transfer by inheritance, following the general rules for the transfer of movable assets, and would even on occasion require the application of any specific aspects that might arise in accordance with intellectual property regulations.

These files are no different from analogue files, except in the storage medium, aside from one significant and distinctive duration: they can be easily duplicated without undermining the quality of the original, unlike the case of handwritten documents or photographs that have already been developed, where a distinction can be made between the original and the copy, raising the unresolved question of whether there is scope for a multiple bequest to several individuals simultaneously of one single digital object, since the same item can be bequeathed concurrently without any significant differences arising.

It would therefore be desirable for the testator, when making the request, to specify whether he or she authorises multiple copies or reproductions in order to allow the heir,

who, unless otherwise provided by the testator, is responsible for handing over the bequest, to retain a copy of the files, or otherwise. Having said this, it must be borne in mind that multiple reproduction may be limited by copyright or may be subject to other limitations upon acquisition that, even though it might be possible, would not permit copying and distribution, in accordance with the inherent intellectual property regulations.

Those digital files that have been acquired outright by the deceased and can be transferred upon death subject to no limitations other than those resulting from the file itself or the service by means of which they were acquired, such as the establishment of a limited number of reproductions, a time period for use, reproduction on a physical storage medium, all within a particular spatial context. It is important to specify in this regard that not all assets acquired by an individual as a digital consumer are subject to outright ownership, since certain general terms and conditions of sale cover not the acquisition of ownership, but instead a right of use lasting a particular period of time.

A tangential but important question is that the files and documents acquired, and on occasion also those created, could be of economic value, with a cost of acquisition, and even a market value, and if they are included in the inheritance, then consideration would need to be given to this in order to calculate the overall estate, for the purposes of the inheritance tax return and the application of taxation in accordance with the general rules. One could imagine substantial libraries of music or collections of electronic books which could, given their volume, be excluded from the category of household chattels and so be subject to taxation.

As a result, just as a music collection, video library or set of photo albums can be bequeathed, it would be perfectly permissible for a digital photo or music library or a collection of electronic books to be bequeathed in a will.

2.2. The distinction between container and content

The storage medium containing the digital files, if it is a physical object such as a hard drive or mobile device, is subject to ordinary ownership, being considered a movable asset, ownership thereof normally being accredited by means of public and unchallenged possession by the deceased, although this could also be demonstrated by other means, such as documents providing proof of acquisition.

The storage medium, if it can be so named, could also be a virtual hard drive or the cloud, in which case one cannot speak of ordinary ownership, but rather a right of access to the content, resulting from a contractual relationship with the company providing the service.

2.3. Succession in BitCoin and similar concepts

Virtual currencies, crypto-currencies, electronic money, BitCoin, or any other asset

or right equivalent to these unquestionably belongs to the inherited estate.

The questions resulting from their inclusion within the digital inheritance estate are not greatly different from those that would be raised by other digital assets, with two in particular requiring emphasis: the possible lack of transparency regarding the accounts, and the high intrinsic value of said assets.

The first problem is connected with the fact that ownership of the access codes is personal and private, and as a result disclosure in any document other than a notarial will, given the security guarantees and secrecy of the protocol, could give rise to the complete loss of the investment made. It would not be advisable to give the codes allowing for retrieval or transfer of virtual currency to another person. Likewise, it would similarly not be advisable to distribute the codes among several individuals, nor to have recourse to complex data cross-referencing systems.

In fact, even a traditional notarial will, which enjoys notarial protocol protection, could be insufficient depending on the specific case, as it is accessible to all heirs entitled to a copy, and it may therefore be beneficial, as with digital files or social media or email access codes, to refer to another public instrument, access to which would be restricted, and which would record the private data giving access to the virtual wallet. This other instrument could be a will without revocation, a notarial affidavit, an act recorded in the protocol, or even a notarial deposit.

In such cases, the party concerned could adapt access to the data by specifying who is entitled to a copy or to retrieval of the deposit. Nonetheless, the fact is that the heir will always have an interest in ascertaining and investigating the true assets of the deceased, for example in order to guarantee the enforced share or to pay creditors resulting from the inheritance. It is therefore difficult to restrict or conceal from the heir a particular part of the inherited assets, by limiting the right to copies.

Whatever the case, whether or not there is a will, the first aspect is to locate the investment. Someone needs to be aware of the existence of, for example, the BitCoins, and to hand over the access code to the heir, if he or she does not already have this.

The heir succeeds the legal position of the owner of the virtual currency, and may therefore maintain the virtual monies as such, or proceed to convert them into conventional cash via the applicable channels in each case (sale, conversion, etc.) in the same way that the owner could. If there are several heirs, then they will need to agree as to how to proceed.

The second difficulty in accessions results from the fluctuation in the value of virtual currencies. It may be that, in the near future, the part of the virtual money or means of payment comprising the inheritance of an individual could be very substantial, requiring

valuation, calculation, declaration and taxation in accordance with the general rules. The problem, as with other assets the value of which can drastically and rapidly rise or fall, is the value to be adopted.

2.4. The position of intrinsically personal relationships

Rights of personality need to be excluded from this phenomenon of digital succession, except from action to obtain restoration of material or moral damages occasioned to the right of reputation, privacy or personal image, for example.

Lifelong rights and fundamentally personal digital relationships must likewise be excluded, since it would not seem that one can upon death transfer any contract or service in which the personality of the deceased played a decisive role in establishing or maintaining it, or where the personality of the deceased is publicly expressed and identifiable. This point is a very important one when focusing what is included within the digital inheritance, and how.

To consider the example of the succession of a person's email account: to begin with, there could be details in the deceased's email that would be necessary in order to exercise rights before third parties, along with important documents and digital files sent or received by the deceased. Meanwhile, data protection and the secrecy of communications would prevent access being granted to this information, since this may entail access to the information of third parties that was disclosed to the deceased, but not to his or her heirs.

Email is not, though, the only example that one could include within this category: the relationship established by the user, for example, with a social media platform begins with a sign-up agreement and the downloading of the application or usage of the corresponding account via a browser, but from the point at which the user begins to make use of the service, there is a divergence between the relationship with the service provider behind which the social media network lies (which is personal, but perhaps not absolutely personal), and the relationship with other users (which is absolutely personal). For example, in Twitter the relationship according to the terms accepted upon registration is "personal, worldwide, unremunerated and non-transferable".

As a result, the question should perhaps not focus so much on directly excluding these relationships from the content of the digital inheritance, but rather in positioning them within a special regime of post-mortem administration of said content, attributing to those who have the status of heir a title of sufficient legitimation in order to allow them to act with regard to the service providers who control access to the content in question.

This title of legitimation would entail the possibility of access to the content, but what the heirs could under no circumstances do is to publish new material passing themselves off as the deceased, not only because of issues

regarding the supplanting of identity, but specifically because the relationships with other users interacting within the network may indeed be deemed absolutely personal.

3. Legitimation before service providers

The current reality is that digital inheritance, with regard to this matter, is fragmented for three reasons: first, because these service providers may normally have their centres of operations in different countries with their own different systems and structures for succession and legitimation.

This first problem should be addressed through regulation, at least within Europe and at a basic level, in order expressly to include digital inheritance within ordinary inheritance, and to grant the heirs or legatees certainty as to how they should act.

To this end, through the initiative of the notariat of Malta the RODAIS (Regulation Of Digital Assets within Inheritance and Succession scenarios) Project is being developed, beginning with a comparative study of the companies providing online services in order to bridge the gap in digital inheritance and national legislation, for the purpose of creating a guide and a good practice document, which should be passed on to international service providers operating in Europe, such as Facebook, Google, Apple and Spotify.

The second reason is that each service provider has a specific operational policy in the event of the death of the holder, which is accepted by users themselves (whether they are aware of this not) when they agree to the contractual terms and general conditions that are accepted upon creation of an online account.

In this regard, a channel for clear understanding of the succession implications that the private designation of an individual as successor, agent or legal representative upon the death of the holder could have should be provided, clearly advising users of the conflicts and potential problems that could arise with regard to the figure of the heir.

The third reason is that such service providers typically choose not to apply the traditional succession concepts of heir or legatee, relaxing the requirements for access to the content and the account of the deceased, and allowing individuals who need not be heirs to access content that could prove to be absolutely personal.

Nonetheless, this does not mean that indiscriminate access would be permitted. At Google Mail, for example, they admit that they are "*aware that many people ultimately pass away without leaving behind clear instructions as to how to administer their online accounts*," and accept applications, following a specific analysis of each case, for access to be allowed on the part of an authorised representative of the user, even with supplementary security measures, for example having received at least one email from the account in question.

This solution, like other specific approaches adopted by other services, as a security measure to confirm evidence of a relationship

with the deceased, might be appropriate, but the fact is that people typically send hundreds of emails to dozens of different addresses, which might or might not include our heir.

The same applies to the terms of social media platforms. On Twitter, for example, there are specific standards regarding how to serve notice of a deceased user in order to deactivate the account, establishing criteria that bear little or no relationship to succession regulations, since an authorised person is allowed to act as the representative of the estate of the deceased, or a direct relative of the deceased, without any particularly greater formality, or sufficient proof of their status as heir. Nonetheless, it is specified that access to the account cannot be granted to anyone, irrespective of their relationship with the deceased.

Facebook similarly has provisions in place in the event of death. It specifically offers the option of completely closing the account and eliminating the profile, requiring proof not only of the death but also status as an immediate relative of the deceased, and access to certain personal details regarding the person, such as the email address used by the deceased to log on to the social network. The other option is to maintain the account with commemorative status, in order to allow friends and relatives to leave messages there after the death.

An attempt should be made in this regard to ensure that these terms and conditions respect the domestic succession regulations of each country, and the basic European standards we referred to earlier, by means of the formalisation of these general conditions, to provide single and unequivocal solutions based on the structures of succession law.

Of course, the document of legitimation should be a notarial instrument, as in the case of an ordinary will. A separate question is: should it be the traditional will, or should other types of succession be allowed?

4. Notarial testaments and online testaments

As already suggested, the traditional analogue notarial will and testament is not easily adaptive: it would not be convenient to update it every time there is a change to electronic contact details, passwords, account numbers, or every time a user register with a social media platform.

Again, though, the fact that the notarial will and testament may require an appropriate solution for this social reality does not mean that the regime governing titles of succession would need to be completely changed. Perhaps, there could be mixed documents, or two complementary documents, or some other channel that would allow the traditional will to coexist with the required adaptability of that part of the document dealing with digital matters.

Nonetheless, there must be awareness that there are digital matters that the notariat does not as yet cover. For some of these situations there are digital services provided by private companies that are positioning themselves to occupy this space. There needs to be

reflection on whether a notarial instrument should continue to fill this gap, and if so, how it should do this.

In short, this is the debate as to whether there exists a digital or online will, whether this should exist, and what characteristics it should have.

ACADEMIC COORDINATION:

CESARE LICINI

Cesare Licini is a notary in (Italy). He graduated in law from the Catholic University of the Sacred Heart in Milan (1977). He has had numerous responsibilities at European and international level. In particular, Cesare Licini is a member of the Steering Committee of the International Union of Notaries (UINL). He was Vice-President of the UINL's European Affairs Commission (CAE) from 2004 to 2007 and Chair of the CNUE's Anti-Money Laundering working group from 2011 to 2017. He is also a UINL and CNUE delegate in the Financial Action Task Force on money laundering (FATF). Mr Licini has published widely and participated in numerous national and international congresses and conferences.

MODERATION:

CATALINA GUERRERO

Catalina Guerrero is head of section of the International Department of Agencia Efe, the first agency in Spanish and fourth in the world. Her professional performance is now focused on the Euroefe.euractiv.es project, which she joined in January 2016 to follow the current affairs of the European Union (EU) from a Spanish and multimedia perspective.

She previously spent nine years as the editor of EFE's Integrated Culture department (National and International), where she closely followed the intellectual trends of Europe and the rest of the world. She came to Culture after an enriching eight-year stint in Paris, where she was the EFE correspondent from 1999 to 2007.

In her early professional years she was involved in radio. With a degree in Journalism from Madrid's Universidad Complutense in 1992, she also holds diplomas as a Professional Expert on Culture, Civilisation and Islamic Religion from the Spanish Open University (UNED) (2007) and on the European Union (2016) from the Madrid Diplomatic School.

SPEAKERS:

PILAR DEL CASTILLO

Former Minister of Education and Culture from 2000 to 2004, **Pilar del Castillo** was elected to the European Parliament for the first time in 2004. She belongs to the Partido Popular (People's Party), which in turn is a member of the European People's Party. She is the European Parliament's rapporteur on the European Electronic Communications Code. She has also been, among others, the rapporteur of the Telecoms Single Market Regulation; the Directive on Security of Networks and Information Systems for the ITRE committee; the Regulation on the Body of European Regulators in Electronic Communications (BEREC); the report on Cloud

Computing Strategy for Europe and the Report “A Digital Agenda for Europe: 2015.eu”, to name just some examples.

Del Castillo is the Chair of the European Internet Forum (EIF), Vice-President of the European Energy Forum, member of the Board of Knowledge4Innovation (K4I) and member of the Transatlantic Policy Network. Del Castillo is Professor in Political Science and Administration. She obtained a PhD in Law from Complutense Univeresity. Before, she had attended Ohio State University on a Fulbright scholarship, graduating with a Master’s degree in Political Science. She was the Executive President of the Centro de Investigaciones Sociológicas (Sociology Research Centre) from 1996 to 2000.

ÖRJAN BRINKMAN

Örjan Brinkman was born in 1956. He graduated with a teaching diploma in 1978 and served as a pre-primary and municipality principal until 1988 and later worked as Head of Development and County Manager in TBV adult education (until 1996), Marketing Manager and expert on labour market and education in the Women´s Forum foundation (until 2002), Director of Administration in culture and education in the municipality of Sodertalje, Principal in primary and secondary education in Vittra until 2006 and Secretary General of The Swedish Disability Federation until 2012.

He was also a member of the Monitoring Committee and the Working Committee of The European Social Fund I Sweden until 2011 and of the Swedish Government’s Disability Delegation in 2011.

Today he is active in a number of confidential assignments relating to his current position. He is a member of the Board of Agriculture’s consumer advisory group, the Chemicals Agency’s advisory council, President in Väddö Södertörn – College foundation, Member of the Dialogue Forum – Dental and Pharmaceutical Benefits Agency, President of The Swedish Consumers Association and Råd & Rön Consumer Magazine, President of BEUC – The European Consumer Organisation.

PETER BISCHOFF-EVERDING

Peter Bischoff-Everding is a lawyer by training and holds a Ph.D. from Hamburg law school in competition law. He started his professional career as associate lawyer in a law firm in Berlin before he joined the legal department of the German Ministry of Economy.

Since 2004, Peter has been European Commission official, working first in the Enterprise and Industry Directorate-General in the area of free movement of goods and under the WTO rules concerning technical barriers to trade.

He was then responsible for legal and regulatory issues in the unit in charge of EU policy and legislation in the medical devices and cosmetics sectors. From October 2012 to September 2016, Peter was deputy Head of Unit in the Health and Consumers Directorate-General in charge of consumer product and service safety.

Since October 2016, Peter has been deputy Head of Unit in the field of Consumer and Marketing Law which is part of the Directorate-General for Justice and Consumers. His unit manages the cross-cutting EU consumer law body and is currently preparing a possible legislative proposal to further modernise the rules of EU consumer law.

ANTONIO GHIO

Dr. Antonio Ghio is a partner at Fenech & Fenech Advocates and heads its ICT & IP Law Departments. For the past twelve years his work has solely revolved around ICT law issues, trying to find solutions to the constant struggle existing between law and technology, both inside and outside of the courtrooms.

Ghio also lectures in ICT law and Cyber Crime at the University of Malta and held the position of Chairman of the Malta Communications Authority after having served as a member of the Board of Directors for the last five years.

He has an LL.D from the University of Malta where he specialised in legal aspects of Internet security and online privacy as well as an LL.M from Strathclyde University where he specialised in offshore electronic commerce.

Ghio is a founding member and current President of the Malta Information Technology Law Association – MITLA. He is a regular speaker on ICT law issues in conferences both locally and abroad and has a regular column on ICT law issues in the Sunday Times of Malta as well as a personal blog on ICT Law issues at ictlawmalta.blogspot.com.

TAMÁS PARTI

Dr Tamás Parti, civil law notary in Budapest, President of the Budapest Chamber of Civil Law Notaries, member of the General Council of the UINL (International Union of Notaries), President of the CNUE's Futurology Forum and Chair of the Committee for Technological Adaptation of the Hungarian Chamber of Civil Law Notaries. Furthermore, he is a lecturer in the Department of Civil Procedure at the Faculty of Law and Political Sciences of Eötvös Loránd University in Budapest (ELTE) and examiner in the legal profession examinations [Bar examinations] in Hungary. His PhD field of research is the study of the effects of contemporary social and technological processes on fundamental rights – an aspect of this research is the study of the effects of technological progress on the notarial profession.

LORENZO PRATS ALBENTOSA

Chair of civil Law, Autonomous University of Barcelona, since 2008 (previously, University Complutense-Madrid, 2007, University of Cantabria, 2002, University of Valencia, 1984). Arbitrator since 2007. Member of the Cabinet of the Ministry of Justice, Spanish government (2004-2007). Law practitioner (since 1986). Education: University of Valencia (Spain): Law Degree & PhD; Bologna University (IT): PhD researcher; visiting professor: Cambridge University (UK), Chicago University (USA), London School of Economics (UK).

ALEXANDRE LIBORIO DIAS PEREIRA

Alexandre Liborio Dias Pereira (LL.B, LL.M, LL.D Coimbra), born in July 1970, is a full-time law professor at the University of Coimbra. He teaches Contracts, Computer Law, Copyright and Business Law, and supervises postgraduate research. He is also

part-time adjunct professor at the Coimbra Business School and invited lecturer of the Summer School on European Private Law at the University of Salzburg (Austria). He has also served as visiting full-time law professor at the University of Macau (China), and has been FCT sabbatical fellow at the Max-Planck Institute, Munich (Germany). He has presented communications worldwide and published more than one hundred scientific works in Portugal and abroad. His research focuses on the legal environment of the EU digital single market.

JOSÉ CARMELO LLOPIS BENLLOCH

José Carmelo Llopis Benlloch was born in Valencia (Spain) in 1978. After graduating in 2001 from the Faculty of Law at the University of Valencia, he became notary in the class of 2005-2008.

In 2013 he became a mediator at the Solutio Litis Foundation of the Notarial College of Valencia.

Since 2014, he has been writing weekly about technological and notarial issues on his blog and participating in committees and working groups at a local (IT Committee), national (Jurisprudence Group) and international level (CNUE New Technologies working group).

In 2016, he was co-author of two ebooks relating to Digital Inheritance and Electronic Evidences, and he spoke about New Technologies at conferences in Spain, like NotarTIC, and abroad, such as the 5th World Notarial University in Rome organised by the UINL.

Also, in 2016 he was honoured to be the Spanish national rapporteur for Topic II concerning electronic notarial acts and paperless processes at the 28th International Congress of the Notariat in Paris.

REMCO VAN DER KUIJP

Remco van der Kuijp is a Dutch Civil Law Notary (2006) and a member of the Board of the Royal Dutch Society for Notaries (KNB). He is treasurer and as a Board member responsible for ICT projects and pension rights. He is involved in the development of Notary-ID, a new project of the Dutch notariat. Furthermore, he has a keen interest in blockchain and online business development for notaries.

CRISTIAN BUŞOI

Mr **Cristian Bușoi** has been a member of the European Parliament since 2007 and is currently active in the Committee on Industry, Research and Energy, the Committee on the Internal Market and Consumer Protection, the Delegation to the EU - Ukraine Parliamentary Committee and the Delegation for the EURONEST Parliamentary Assembly. In 2016, he was the only MEP awarded the MEP Award for Healthcare and was distinguished by the European Organisation “Eurordis” with a trophy recognising his support for patients suffering from rare diseases.

Prior to this, Cristian Buşoi was President of Romania’s National Health Insurance House (2013 - 2014) and member of the Romanian Parliament (2004 - 2007), where he was part of the Health and Family Committee.

Mr. Buşoi has been a member of the National Liberal Party for 20 years and currently holds the position of President of PNL Bucharest. In the PNL he has also served as Secretary General, First Vice-President and member of the Permanent Political Bureau.

Cristian Bușoi graduated from Carol Davila University of Medicine and Pharmacy in Bucharest, Carol I National Defence College and the Law School of Titu Maiorescu University. In 2010 he obtained his Ph.D. in Public Health and Health Management from the University of Medicine and Pharmacy Victor Babes Timisoara.