ARTICLE:

THE LEGAL REGULATION OF ELECTRONIC EVIDENCE: A PENDING NECESSITY[1]

By **Eduardo de Urbano Castrillo**

Electronic evidence, a term that has become more commonly accepted than others, such as "digital evidence" or "technological evidence", is now firmly established in forensic practice and doctrinal considerations, and there is an increasing degree of consensus as regards the concept and its application in practice. Nonetheless, there has been a pressing need for the regulation of such evidence. The recent Spanish Act, governing the "Use of Information and Communications Technology in the Administration of Justice" attempts to provide such regulation, although it does so in a somewhat timid manner. The objective of this article is to contribute some reflections or suggestions that might serve to complement the legislation, which are, in an indirect manner, covered by this act governing electronic evidence.[2]

Introduction

For some years now, the question of new technology, and particularly its application in the administration of justice, has been a much discussed issue. There has been relentless, if somewhat slow moving, progress in this respect.[3] There is an increasing volume of jurisprudence and some regulation of electronic evidence, although, in our opinion, its treatment is fragmented and insufficient.

The preamble to the new act governing the "Use of New Information and Communications Technologies in the Administration of Justice" acknowledges the need for specific regulation, which would go beyond what is set out in Act 11/2007 of 22 June, which refers to the electronic access of citizens to public services. The preamble reiterates the imperative need for rules governing such technologies in the administration of justice and the importance of this for the modernisation of the legal system.

An examination of the new act referring to electronic evidence suggests that, while an opportunity has been missed, all is not lost. Alhough the legislation fails to provide specific regulation, it does offer guidelines of interest and evident utility that improve upon the previous situation. Furthermore, these guidelines may well be complemented if they are dealt with by the forthcoming Criminal Proceedings Act. For this reason, we dare to propose specific legal regulation of electronic evidence, subsequent to briefly outlining the most important characteristics of such evidence.

A new legislative initiative

Within the framework of this issue of electronic evidence, the Spanish government has drawn up Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (Act for the Regulation of the Use of Information and Communications Technology in the Administration of Justice), which was recently passed by the Spanish parliament. It unquestionably represents a further step along the road towards the information society that forms part of the period in which we live, and the public administration has a great role to play and much work to do with respect to the objectives of this society.

The new legislation finds its justification in the framework of the necessary modernisation of the administration of justice, with the objective of

1 *This is an updated and revised version of the article published in Spanish in the May 2011 edition of the legal journal "La Ley Penal" (Wolters Kluwer-La Ley).*

2 *The legislation in question is Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (Act 18/2011, of July 5, which governs the "use of information and communications technologies in the administration of justice"), published on 6 July 2011.*

3 *In Eduardo de Urbano Castrillo and Vicente Magro Servet, La Prueba Tecnológica en la Ley de Enjuiciamiento Civil (Aranzadi-Thomson, 2003), we had already looked at the procedural implications of new information technologies and, in particular, with respect to electronic evidence.*

It is particularly striking that there is no specific treatment of the peculiarities of electronic evidence, which is undoubtedly a prime element of the "electronic file", a term which is being promoted as a replacement for the traditional "court record"

safeguarding the right of citizens to effective judicial protection (articles 1 and 2). To this end, it is maintained that, in this context of modernisation, one of the most pertinent elements is the introduction of new technology into judicial offices, and that the generalised and compulsory use of such technology will serve to enhance administration in judicial offices, modernise the way they operate and increase efficiency levels. Three specific "objectives" are outlined in the premable (item I paragraph 2):

> La presente Ley regula el uso de las nuevas tecnologías en la Administración de Justicia. Los principales objetivos de esta norma, son: primero, actualizar el contenido del derecho fundamental a un proceso público sin dilaciones indebidas, gracias a la agilización que permite el uso de las tecnologías en las comunicaciones; segundo, generalizar el uso de las nuevas tecnologías para los profesionales de la justicia; tercero, definir en una norma con rango de ley el conjunto de requisitos mínimos de interconexión, interoperabilidad y seguridad necesarios en el desarrollo de los diferentes aplicativos utilizados por los actores del mundo judicial, a fin de garantizar la seguridad en la transmisión de los datos y cuantas otras exigencias se contengan en las leyes procesales.

The first is to update the content of the fundamental right to a public process without undue delay; the second is to generalise the use of new technologies amongst legal professionals; and the third is to set out in a regulation, which takes the form of a law, the foundations to ensure their effective and secure use in the judicial field.

The act comprises five titles. The first title deals with the scope and basic principles of the legislation, while the remaining four have more specific content. Because a detailed examination of the new act is not the aim of this article, we shall only mention some of the more pertinent provisions: recognition of the right of professionals in the administration of justice to work using "electronic means" (article 4); electronic files (article 29) provides that all documents used in judicial proceedings "may be" stored by electronic means; for the presentation of documents, all manner of statements, documents "and other means" or instruments presented must follow a digital protocol (article 38); rectification: a time limit of three days is established for the party so required to rectify non-compliance or deficiencies observed in the use of the relevant technologies with respect to the terms laid down by the act (article 43); the new law applies to all legal jurisdictions and will complement existing legislation on the use of this type of technology in the administration of justice (DA 7ª).

Omission of the treatment of electronic evidence

It is particularly striking that there is no specific treatment of the peculiarities of electronic evidence, which is undoubtedly a prime element of the "electronic file", a term which is being promoted as a replacement for the traditional "court record". It is to be wondered whether this is a deliberate or involuntary omission. Obviously it is not the same, but regardless of the answer, the effects are identical: the opportunity to deal specifically with such an essential issue has not been grasped. Nonetheless, it is true that in a general, and therefore in an indirect manner, the matter seems to be implicitly dealt with within what the act refers to as "electronic documents" and "other means and instruments".

In this respect, it is worth citing article 38 of the Act:

> Artículo 38. Presentación de escritos, documentos u otros medios o instrumentos.

1. La presentación de toda clase de escritos, documentos, dictámenes, informes u otros medios o instrumentos se ajustará a lo dispuesto en las leyes procesales, debiendo ir acompañados en todo caso del formulario normalizado a que se refiere el apartado 4 del artículo 36, en el que además se consignará el tipo y número de expediente y año al que se refiera el escrito.

2. En todo caso, la presentación de escritos, documentos y otros medios o instrumentos se ajustará a las siguientes reglas:

   a. Los documentos en papel que, conforme a lo dispuesto en las leyes procesales puedan o deban ser aportados por las partes en cualquier momento del procedimiento, deberán ser incorporados como anexo al documento principal mediante imagen digitalizada de la copia, si fueran públicos, o del original del documento obrante en papel, si se tratara de documentos privados. El archivo de la imagen digitalizada habrá de ir firmado mediante la utilización de los sistemas de firma electrónica previstos en la presente Ley, en las leyes procesales o en otras normas de desarrollo.

   b. Los documentos electrónicos públicos o privados se incorporarán como anexo al documento principal siguiendo los sistemas previstos en esta Ley o en sus normas de desarrollo y conforme a lo previsto en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

   c. En caso de que fueran impugnados por la parte contraria, se procederá conforme a lo dispuesto en las leyes procesales y, en su caso, en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

   d. No se admitirá la aportación en otra forma, salvo en el supuesto de que, por las singularidades características del documento, el sistema no permita su incorporación como anexo para su envío por vía telemática. En estos casos, el usuario hará llegar dicha documentación al destinatario por otros medios en la forma que establezcan las normas procesales, y deberá hacer referencia a los datos identificativos del envío telemático al que no pudo ser adjuntada, presentando el original ante el órgano judicial en el día siguiente hábil a aquel en que se hubiera efectuado el envío telemático. Tales documentos serán depositados y custodiados por quien corresponda en el archivo, de gestión o definitivo, de la oficina judicial, dejando constancia en el expediente judicial electrónico de su existencia únicamente en formato papel.

      Cuando se deban incorporar documentos sobre los cuales existan sospechas de falsedad, deberá aportarse en todo caso además el documento original, al que se le dará el tratamiento contemplado en el párrafo anterior.

   e. En los casos en que se deban aportar al procedimiento medios o instrumentos de prueba que por su propia naturaleza no sean susceptibles de digitalización, serán depositados y custodiados por quien corresponda en el archivo de gestión o definitivo de la oficina judicial, dejando constancia en el expediente judicial electrónico de su existencia.

Article 37. Submissions, documents and other means or instruments.

1. The presentation of all kinds of statements, documents, opinions, reports and other means or instruments will be in line with that set out in the provisions of the procedural laws and they must always be accompanied by the standard form referred to in paragraph 4 of Article 35. This standard form must also contain the type, number and year of the file referred to in the statement.

2. In all cases, the presentation of statements, documents and other means or instruments shall comply with the following rules:

   a) The document, in paper or electronic format, which, in accordance with that laid down in the procedural laws, can or must be submitted by the parties at any time during the procedure, must be submitted in the form of an annex to

the main document by means of a digital image of the simple copy, in the case of public documents, or the original in paper format, in the case of private documents. Their fidelity with the original documents must be guaranteed through the use of the electronic signature systems set out in this Act and the procedural laws and such documents must comply with the rules of each authority with responsibility for the computerised telecommunications system of each jurisdiction.

b) In cases where such documents are contested by the opposing party, the procedure will be in accordance with the provisions of the procedural laws and, where appropriate, those of Act 59/2003 of December 19 with reference to the Electronic Signature.

c) The same procedure will apply to the presentation of all types of documents in court appearances and hearings.

d) Submission will not be permitted in any other manner unless it can be shown that, owing to the singular characteristics of the document, the system does not allow for its addition as an annex to the main document for subsequent telematic sending. In such cases, the user will ensure the transmission of the document in question to its addressee by other means, in accordance with that set out in the procedural laws, and must include the relevant reference data of the telematic sending of the document to which it could not be attached. The original of the document must be submitted to the judicial body on the first working day subsequent to that on which the telematic sending of the document would have taken place. Such documents will be deposited and kept by the corresponding official in the judicial office and a note must be made in the electronic judicial file of its existence only in paper form.

In all cases where there are doubts regarding the authenticity of documents submitted, the original of the document must also be submitted, subject to the same conditions set out in the preceding paragraph above.

e) In cases where means of proof cannot be digitalised, such means of proof shall be deposited and kept by the corresponding official, in the live or definitive file of the judicial office, and a note of its existence must be recorded in the electronic case file.

We are not of the opinion that the references outlined above are inappropriate, but it will be agreed that it would be preferable to have a regulation, however brief, on the procedural aspect of evidence of this type, given that it is increasingly submitted and does not enjoy even minimal regulation at present.

Meanwhile, the work of interpretation and analogous application of the general rules governing evidence, complemented by the specific legislation in existence and the relevant case law that is appearing, must continue. With the objective, therefore, of complementing the new legislation, we offer some ideas to offset its shortcomings in the following specific proposal.

Regulatory proposal

In our opinion, the three areas that should be dealt with explicitly in a law referring to electronic evidence are: general characteristics, specific issues and main forms of electronic evidence. We outline some reflections on these points below, which might be of interest for future regulation.

General characteristics

Subsequent to defining the term "electronic evidence", the requisites for its validity must be established, along with the manner of its inclusion in the procedure, practice of the evidence and assessment.

By "electronic evidence", we understand evidence that might accredit facts relevant to the process through means of reproduction of words, sounds and images created by modern information technology instruments and presented in an appropriate electronic format. All electronic evidence is created and displayed in computer or binary language that includes two elements: first, the material element or hardware and second, its content, provided by determined computer software.

The "validity requisites" for the admissibility and assessment of electronic evidence include, in addition

to the general requisites for all evidence – relevance, necessity and legality – requirements specific to this type of evidence. In order to pass the admissibility test, the authenticity of the document must be verified, leaving the critical examination of its informative content for the assessment stage. There must be control of the technological aspect (hardware) and the reliability of the computer program and process (software) used to create the electronic format. At this time of the procedure, there is no prejudgement – except in cases of flagrant inadequacy or illegality – of questions such as identity, integrity and authenticity of the document. These questions are dealt with in the hearing itself.

With respect to "inclusion in the procedure", once the evidence has been admitted, the electronic format will be submitted to the court and kept under the responsibility of the judicial secretary. Care will be taken to ensure its good conservation and proper registration, and details will be taken of the operations required for its future use. The chain of custody of this type of evidence is of particular importance, given that it is not unalterable or difficult to manipulate. On the contrary, the term virtual evidence is a consequence of its essential alterability at any time. Therefore, we do not consider it acceptable that such evidence remains in the custody of the police or any other party. It should be at the disposition of the court, duly registered and safeguarded in a secure location.

The "practice" of such evidence should be carried out through its examination, and the process for such examination will have distinctive characteristics, in that it will most probably need to be displayed or listened to. It should be made clear that such evidence will be examined at the hearing or court appearance, and the necessary infrastructure must be in place for this purpose. The party submitting the evidence should ensure its viability, with all guarantees, which includes previously furnishing the other party, if necessary, with a copy of the format containing the evidence to facilitate the questioning of or objection to the same. The rules set out for judicial recognition in the Spanish Code of Civil Procedure could be supplementary to the application of articles 299 1 5º and articles 353 to 359 of the Code.

Finally, the "assessment" of electronic evidence constitutes another matter of special interest, due to the specific nature of this type of evidence. In this respect, we limit ourselves to outlining the main aspects to be borne in mind. The nature of documentary evidence obliges provisions on this type of evidence to be followed analogously insofar as possible, and special emphasis should be placed on the criterion of "due circumspection" with the specific rules set out in current legislation – and legislation governing the electronic signature or the content of the act governing the use of information technologies. The hardware and software, as defining structural elements of the evidence, must both be examined. Great attention must be placed on possible manipulation and maximum emphasis should be placed on the specification of grounds for justification. It will also be necessary to have information technology expertise at hand in order to avoid dependence on any possible personal knowledge of the judge presiding over the case. The judicial body should take account of the conclusions of any digital evidence specialist with the greatest care possible, especially bearing in mind that this is a field of continuing technical innovation.

Finally, to complete the list of basic issues to be taken into account for the assessment of electronic evidence, let us mention the use of article 4 of the Code of Civil Procedure (LECiv) as a supplementary protective rule. This text contains the most comprehensive current regulation with respect to evidence in general. It is also of interest to point out the use of analogy with respect to the most similar methods of proof dealt with by LECiv. An example of this would be provisions governing the searching of a place of residence for the purposes of acquiring electronic evidence.

Special issues

In this section, we examine a number of issues, the regulation of which would undoubtedly facilitate the use of electronic evidence and would be justified by the specific nature of new technologies. In our opinion, the issues requiring individual attention include: access to the document, public electronic documents, unsigned documents and the treatment of electronic originals and copies. We offer the following very brief observations on each of these points.

Access to the document

On the basis that article 24.2 of the Spanish Constitution (CE) does not permit that a defendant be obliged to testify, it is not possible to oblige the owner of information uncovered to facilitate access to such information, since this would be tantamount to asking

him to cooperate in his presumed incrimination. This presents obvious difficulties, because very often the information is protected with passwords and keys or even encrypted to prevent the reading and examination of the data. Given this situation, the law could include the provision that in the warrant authorising the interception of electronic communication, such authorisation would include the right to gain access to its content through whatever technology that might enable the password to be obtained or enable the text written in code to be decrypted.[4]

Public electronic documents

Both public documents and private documents signed by notaries, which include documents ranging from electronic national identity documents to documents referred to in article 27 of the Spanish Commercial Code, administrative documents, Social Security and Inland Revenue documents and, of course, title deeds digitally signed by notaries, have an obvious legal status, although they would be subject to examination as to whether they comply with the requisites that would give them the privileged status of evidence.

We believe that it is primarily a matter of confirming two questions: (a) that the validity of the document is governed by what is set out in the relevant legislation, and (b) that, with prima facie evidence or justification of weight, it can be claimed that the document has been manipulated, falsified or fraudulently produced. As regards the first question, it is necessary to accredit the identity of the parties, the time and date of the creation of the document or the creation of the copy by the authorised public notary.[5] The above includes cases in which the notary is the recipient of an electronically emitted document, in which case, he will seal, sign and ratify such document and record its nature and origin. With respect to the second question, there is no reason to prevent the checking of the alleged illegality of a public electronic document, provided that reasonable grounds for doing so can be offered.

Unsigned document

It is a fact of experience that most electronic documents generated by modern technologies do not bear an electronic signature. In these cases, the Italian doctrine speaks of an "explicit exclusion of the privilege of evidentiary effect attributable to a computer document without a qualified electronic or digital signature".[6] Nonetheless, the validity of such a document is not in doubt, though it should be made clear that such validity is subject to the accreditation of its authenticity in the event that it is contested by the other party.

Original and copies

The distinction between originals and copies of electronic documents is a matter of importance, and also a complex one, given the versatility of electronic formats. On the one hand, the absence of the public notary and on the other, the ease with which digital reality can be transformed into material reality – the virtual document versus the printed document – makes this a particularly complex technical issue. Complex to a degree that some authors state plainly and clearly that in this case, it is impossible to differentiate between an original document and a copy.

However, the importance lies not in the printed document, but rather in the master or original document. To identify this original, it is of fundamental importance to examine the date on which it was created – the earliest date possible – and for this purpose, the technical means needed to obtain this information must be available. This is due to the fact that in respect of the electronic document, the data relating to its creation is of fundamental importance for the detection of subsequent manipulation. This requires a material examination of such document, the location of the hardware and an interpretation of the logical elements of the system used to draw up the document.

The issue is further complicated by the different ways in which the document can be presented, not just relating to the device on which it is stored – for instance, a memory stick – but also because it may be accompanied by audio or visual content, the addition of which would have required different operations during which alterations to the original document might have been effected. Computer graphics enables the product to be "enhanced" but also facilitates additions or deletions with a clear objective of deception (e.g., the deletion of unattractive "realities" or their presentation in a manner different to that of the original). These simple considerations serve as warnings which are relevant to this particular type of evidence, and they confirm the need to have recourse to the expertise of a

4 *José-Ernesto Fernández Pinós, Valoración procesal de la prueba informática 10/7/2006, Agència Catalana de Protecció de Dades (http://www.apd.cat).*

5 *Juan Bolás Alfonso, 'Firma electrónica, comercio electrónico y fe pública notarial' Revista Jurídica del Notariado, No 36, 2000 pp 31-64.*

6 *Francesco Ferrari, 'Il Codice dell'Amministrazione digitale e le norme dedicate al documento informatico', Rivista di Diritto Processuale, June 2007, vol. 62 no. 2, pp 415-432.*

digital evidence specialist, in the majority of cases with a certain degree of sophistication, to help the judicial body to arrive at its judgement in respect of authenticity.

Main forms of electronic evidence

It will undoubtedly be of great assistance to include regulation of some of the most commonly used forms of electronic evidence,[7] such as e-mails, web sites, intervention of computers, videographic evidence and such like. Another possibility would be to opt for mere regulatory references by type or category of evidence, computer evidence, audiovisual evidence or to distinguish between electronic evidence provided by the parties and official public electronic evidence. It might also be useful to have some regulation governing information technology expertise for legal purposes.

E-mail

The e-mail has become the leading means of inter-personal communication of our age. It does however, present important problems, as has been mentioned. It is not difficult to manipulate and it can be easily altered. "Its manipulation is inexpensive and within the reach of anybody", and most importantly of all, "such manipulation is, in most cases, impossible to detect".[8] This type of evidence can present diverse difficulties, such as: arguments as to whether it was sent or received, if a document with an electronic signature was signed with free will, and, of course, whether the message had been manipulated or not. This is particularly the case with attached documents, which may have been drawn up by third parties and not by the sender. Therefore, with respect to e-mails, great importance lies in the accreditation of the identity of the sender and receiver, the completeness and authenticity of their contents, the meticulous examination of the diligence of the parties and due judicial control, which implies not being satisfied with the mere submission of the computer formats containing such information.

Web sites

Unquestionably, web pages increasingly form part of the electronic evidence submitted for the purpose of accrediting a very large number of offences, and they contain essential data. In this respect, the two matters of greatest interest, in our opinion, are: to identify the party responsible for the content and to test such content. In principle, the party responsible for the content of a website is the real domain holder, which would often coincide with the legal domain holder, but not always. In addition, the web page may have information posted by third parties. We are thinking of a blog or of those who introduce information in web pages.

In consequence, the supposed evidence provided by a web page would need to be considered in connection with the domain holder of the page and the actual author of the content and all due care should be taken to establish the real facts. In particular, it is of prime importance to locate the logs which would enable the tracing of the most recent changes to the home page, and, with the greatest possible speed, to obtain, in the form of an electronic photograph, electronic notarial certification of a specific page at a specific time, i.e., at an exact time and date.

Surveillance and the interception of electronic communications

Entering into the processing of this evidence, in the manner of entering and searching a residence – here we are faced by what is usually described as an "electronic residence" – requires judicial authorisation with the application of the principle of proportionality, which means prior application of the principle of necessity – that is, the measure is absolutely necessary because there is no less onerous alternative – and the juicio de idoneidad (principle of appropriateness) – because the action would reasonably lead to the obtaining of elements of fundamental importance to the procedure – and such measures must be taken with respect to the guarantees demanded by case law for the entering and search of places of residence.

In addition, possible traps laid by the user must be avoided to prevent claims of unauthorised access. It is also important to ensure the preservation of the integrity and identity of the material seized, for the purpose of resolving complaints related to the chain of custody. Due care must also be exercised in the task of obtaining data. This can be carried out by means of an exact copy (a duplicate) of the content of the hard drive and other computer elements (pen drives and other removable memory units), which must always be carried with the due accreditation of the judicial secretary.

7 *The amount and variety of evidence makes it of considerable use to examine works such as Stephen Mason, general editor, Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010) and Stephen Mason, general editor, International Electronic Evidence (British Institute of International and Comparative Law, 2008).*

8 *Mario E. Clemente Meoro and Santiago Cavanillas Múgica, Responsabilidad Civil y Contratos en Internet: su regulación en la ley de servicios de la sociedad de la información y de comercio electrónic (Comares, 2003).*

Video conference

In recent times, the use of video conferencing has ceased to be limited to the business world and large companies, and has become increasingly employed in the administration of justice. Video conferencing is useful in order to avail of the statements of witnesses or technical experts, when such form of communication is considered necessary for reasons of utility, security or public order. The two-way communication and synchronisation of sound and image should be ensured. It should be made clear that if problems are detected that impede or seriously hinder comprehension of the message and the participation of the parties, the evidence will be invalid. Therefore, judicial control of this evidence should exercise care in establishing the identity of the video conference participants, ensure appropriate sound and picture quality and ensure that the right of the parties to question and cross-examine witnesses can be exercised at all times.

Information technology opinion

In our opinion, it is vital to regulate the areas of expertise implied by this type of evidence in order to ensure that judicial protection in each case does not depend in a hazardous manner on the private knowledge the judge may have of such matters. Therefore, we consider the opinion of suitably qualified digital evidence specialists to be an essential element of electronic evidence, as it is complementary to evidence of this type submitted by the parties. Such opinion serves to shed light on possible manipulation of the evidence and other technical details, such as: the hardware used for the creation of the electronic formats and the content of the software, which is often concealed by some method of encryption.

Eduardo de Urbano Castrillo is a Doctor of Law and a Judge of the Technical Advisory Body of the Supreme Court of Spain

