Did You Really Send It? Email Evidence in Litigation and Arbitration in Argentina

By: Lisandro A. Allende and Arturo E. Fontana

Lisandro Allende and Arturo Fontana are with the firm Allende • Ferrante | Abogados in Buenos Aires, Argentina.

Mr. Allende is a partner who practices in corporate law, mergers and acquisitions, international trade and customs law, contracts and real estate, arbitration and civil and commercial litigation, insolvency and restructuring of corporate liabilities, and foreign investments.

Mr. Fontana is an associate who practices in arbitration and civil and commercial litigation, succession, family estate reorganization, insolvency and restructuring of corporate liabilities, and bankruptcy and reorganization proceedings.

EVERY second an estimated 2.4 million emails are sent. The number of email users worldwide is 3.7 billion, and the amount of emails sent per day is around 269 billion.[1]

The practical advantages of these technologies are obvious: they are time-saving, cost-effective and reliable. Most of our communications, whether professional or personal, are not held

[1] Statistics, extrapolations and counting by the Radicati Group from February 2017. Available at http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf.

in paper or physical support but in an intangible record.

Since the application of every new technology comes with inevitable controversies, it has been necessary to legislate on these innovations in order to prevent conflicts and provide adequate answers to those in need of justice.

Because of its timeless quality and general, ample wording, the 19th Century Argentine Civil and Commercial Codes have been used to rule over a wide range of matters involving postal or electronic mails, with almost no legal improvements since their enactments (1862 and 1869, respectively). But in recent times, with the massive popularity of new forms of communications, it has become necessary to pass a law that includes not only facsimile or electronic mails, but also all kind of new technologies widely used.

In response to those needs, the newly unified Civil and Commercial Code[2] ("CCC") regulates all types of electronic communications and applies to all kind of information in the form of a data message, in accordance with the first article of the UNCITRAL Model Law on Electronic Commerce.[3]

I. CCC provisions

The CCC provides practical solutions involving the admissibility of evidence based on emails in both arbitration and litigation procedures.

It is worth to point out that in matters concerning signature and its evidential value, the CCC follows the UNCITRAL Model Law on Electronic Commerce and the Civil Code of Québec.[4]

UNCITRAL Model Law Electronic Commerce has influenced legislation in more than thirty countries, including the CCC, as set out in its preface.[5] Although not expressly stated, the CCC also closely follows the United Nations Convention on the Use of Electronic Communications in International Contracts.[6]

As noted above, the CCC takes into account all methods of written communications. Hence, emails are

[2] Entered into force on August 1, 2015.

[3] Date of adoption: June 12, 1996, additional article 5 Bis adopted in 1998.

[4] The civil code in force in the province of Québec, Canada, which came into effect on January 1, 1994.

[5] Paragraph 44 of the preface: "… *in regards to the notion of signature and evidentiary value, it's been held in special consideration the Model Law on Electronic Commerce formulated by UNCITRAL, the Code of Quebec and the attempts of reform to the French Civil Code regulating evidence*."

[6] Adopted November 23, 2005. Entry into force March 2, 2013.

a type of evidence that can be admitted in arbitration and in court in the same way as any other methods of documentary evidence. However, the letter of the law establishes several limitations regarding confidentiality, as a way of protecting privacy.

A positive aspect of the Argentine legal system is that it allows all types of evidence, even if it is not expressly permitted by law. These principles are referred to as "freedom of proof." Any written communication, regardless of its form of creation or transmission, is admissible as evidence as long as it has been lawfully acquired and is not confidential.

For the purposes of this article, evidence is referred to as information intended to prove a fact from which a conclusion may logically be drawn as to the existence of that fact. Evidence is a crucial tool for the judiciary as it is used to determine matters of controversy. It may consist of proof by testimony of witnesses, writings or records. In adjudicating a matter, judges prefer direct evidence like documents or witness assertions; that is why in many cases intangible electronic evidence is challenged on its admissibility.

Legal limitations on admissibility are not based on mistrust of the technology, but are justified by the constitutional right to privacy. The law requires that the use of confidential emails as evidence in arbitration or in litigation be authorized by the addressee, following the maxim "*nemo tenetur armare adversarium contra se,*" meaning that nobody is bound to arm his adversary against himself.

Third parties are not allowed to use emails or any form of correspondence without the consent of the addressee. When this type of evidence is provided by someone who neither is the originator nor the addressee, magistrates are required to take into account how this person gained access to the mails and reject those obtained in an illegal way.

This legislation protects confidentiality in accordance with the Argentine Federal Constitution and Criminal Code, which consider it contrary to the law to intercept or access electronic communications, mails, phone calls or computer data and that prohibit the publication of illegally obtained data.

Today, most business communications are conducted via electronic device. In order to prevent unauthorized use of private emails, it is advisable to use legal notices asserting its confidential status or stating that the text is protected by the attorney-client privilege. The author of a letter, email or any kind of electronic communication has the prerogative to decide whether the content is confidential or unrestricted.

Digital evidence is not a format directly readable by humans. Additional tools are required to include digital documents as evidence, such as printing it on paper, showing it on a computer screen or other output readable by sight that can reflect the data accurately.

For this reason, it is essential to take every preventive measure regarding the preservation and disclosure of electronically stored evidence, taking into consideration the method of storing data and the precautions needed to prevent its loss. Thus, when serving as defense counsel, it is prudent to request appropriate judicial measures to avoid tampering with the evidence, up to and including obtaining a court order to seize and investigate digital devices, if necessary.

Despite the aforementioned legal regulations and all technical measures available there is still a chance that electronic records have been tampered with. That is why it is important to improve governmental efforts regarding the reliability of this type of evidence, which may be strengthened by introducing new security techniques.

II. Digital Signature Act

The arrival of new technology brought into existence a new kind of document called the electronic record. This form of intangible document has clear benefits compared to standard documents. For instance, electronic records can be preserved in the same quality for a long time through encryption processes, thus reducing the chance of their contents being altered.

Email has become the predominant and preferred form of communication in all aspects of business and social interaction. Since negotiations, transactions, closings and performance of contracts are accomplished through email, it has become necessary to pass legislation contemplating a secure way of creating and signing electronic documents. As a way to fulfill those needs, the Digital Signature Act [7] ("DSA") was sanctioned in 2001 in Argentina.

The DSA draws a clear distinction between a digital signature and an electronic signature.

A digital signature is a type of electronic signature created with mathematical algorithms assuring that the message has been performed by his/her signatory and has not been altered in transit. Such information is permanently embedded into the document, which will show if someone has tried to tamper with it after signature. Hence, a digital signature provides more security than a traditional

[7] National law No. 25, 506, December 11, 2001.

electronic signature as it links the document to the author. This is the digital equivalent of a handwritten signature and can thus be used to validate the authenticity and integrity of any digital document.

The DSA defines "electronic signature" as any author identification and verification mechanism used in an electronic system that lacks any of the legal requirements to be considered a digital signature.

Every digital signature is unique to both the document and the signer, and it binds them together, making it almost impossible to deny having signed a document. By contrast, an electronic signature can be contested in court.

The DSA seeks to solve the problem of tampering and impersonation in digital communications, providing added assurances regarding the origin and identity of an electronic document.

In a similar way, the CCC states that documents with digital signatures are considered signed as long as they guarantee the authorship and integrity of the instrument.

However, if an email lacks a digital signature, there are other resources useful to litigators and judges, including the internet protocol address, or IP address, that identifies which computer sent an email, combined with reports from the internet server provider (ISP). The information provided by the ISP can attest not only date and time, but also the identity of the originator and addressee, and furthermore, can bind an account to a person if that same account has been used for online shopping, bank transactions or it is associated to a credit card. In any case, an IP witness expert's report would be needed.

The evidential value of emails grows extensively when offered with other types of proof, because most electronic communications filed as evidence in arbitration or litigation lack digital signature. Therefore, the role of the judge becomes crucial, as he will ultimately decide on the evidential value of each piece of evidence.

Manipulation, alteration or corruption of electronic records is always a possibility, thereby posing a serious challenge to collect and preserve the evidence. For that reason, when submitting electronic evidence, it is critical to offer computer forensics evidence as well.

Computer forensics is a branch of forensic science concerning legal evidence found in computers and digital storage mediums. In our judicial system computer forensics are useful to courts because they can explain and attest the current state of a data storage format, such as a CD or any computer system.

Even though the DSA has been in effect for almost sixteen years, at the moment electronic signatures, digital signatures and other forms of

encryption are not widely popular in Argentina, due mainly to the lack of trust in technology and state bureaucracy involved.

But this situation is slowly changing with the unstoppable spread of electronic documents, not only in international commerce but in everyday life. As electronic evidence will play an ever-increasing role in litigation, lawyers and magistrates will have to learn how to use this technology efficiently and take advantage of its multiple benefits.

III. Case Law

Due to the flexibility of evidence available in arbitration and litigation in Argentina, digital evidence has been accepted for decades. The use of digital evidence has increased in the past few years, as courts have allowed the use of emails, digital photographs, word processing documents stored in computers, instant messages histories, spreadsheets or files saved from accounting programs, internet browser histories, databases, contents of computer memory, GPS tracks, digital video and audio files.

It is well established by Argentine courts that emails and other similar ways of communicating held in electronic records should be admitted as evidence. Magistrates are expected to take these pieces of evidence into account, though always with the precaution that they have to be consistent with other evidence available, such as witness and expert testimony and printed documents.

Since computer data compilations must by law be treated like any other record, judges must understand how this technology works in order to be able to assess its reliability.

As the CCC entered into force less than two years ago and applies only to facts that occurred thereafter, there is almost no appellate case law applying its provisions. Hence, precedents cited below apply old provisions of the Civil and the Commercial Codes.

These Codes regulations were rooted in judicial decisions ruling over matters concerning postal mail, but also telegraph and facsimile. In a way, many torts involving emails (Simple Mail Transfer Protocol or SMTP) are similar to those with postal mail, and have been considered as such.[8]

Electronic messages are thus considered to have the same evidentiary quality as a fax message, both considered as being

[8] "G. D. E. v. C. S.A.", National Trial Court of Commerce no. 18, October 23, 2001, RCyS 2001-VI, 173 - RCyS 2001, 1049 - La Ley 2002-B, 3, AR/JUR/1423/2001.

comparable to any other type of written proof, like postal mail.[9]

Regarding the matter of privacy, courts have held: "As long as the correspondence has not been received by the recipient, it belongs to the sender, but once received, it belongs to the recipient, without prejudice to the moral right of the sender as the author. Interference, interception, exhibition or the registration of letters affect the secrecy and the right to privacy."[10]

> "The usage of emails that are not owned and that were not addressed to the email address of the offeror, is not acceptable, as the protection of the privacy of users of the system should be maintained, in order to avoid a flagrant breach of privacy. Given that in the area of criminal law it has been said that electronic mail is private correspondence protected by the Constitution of the State of Argentina, the only way in which it could be entered in the private sphere would be by order of a competent judge, since that is the authority referred to in the Constitution."[11]

When dealing with the admissibility of emails as evidence, a distinction has been made between those with digital signatures and those without them (following the DSA), giving superior status to mails with digital signatures.[12]

It is understood that an email with a digital signature is equivalent to any written document with signature and its content is bound to the author. Even if the emails are not digitally signed they can be submitted as evidence, with the same status as other written documents.[13]

Furthermore, it has been ruled that the password used in an ATM should be considered as a type of electronic signature, if it is linked to a signed document.[14]

---

[9] "Unión del Sur Calzados S.A. v. Salbarregui, Nicolás", National Appellate Court on Commercial Matters, Panel E, November 28, 2008; "Zachara, Ivone E. et al v. Banco Itaú Buen Ayre SA", National Appellate Court on Civil Matters, Panel C, February 9, 2007.

[10] National Appellate Court on Civil Matters, Panel H, July 11, 1997, LL 1998-C, 247.

[11] "Vázquez, Walter M. v. Pomenarec, Diego", National Appellate Court on Commercial Matters, Panel A., La Ley Online AR/JUR/15523/(2009).

[12] "Bunker Diseños S.A. v. IBM Argentina S.A.", National Appellate Court on Commercial Matters, Panel D, February 3, 2010.

[13] "Ketra S.R.L. v. Omda S.A.", National Appellate Court on Commercial Matters, Panel F, September 13, 2012.

[14] "Bieniauskas, Carlos v. Banco de la Ciudad de Buenos Aires", National Appellate Court on Commercial Matters, Panel D, May 13, 2008.

When dealing with clickwrap agreements, the judiciary said that such forms of agreements are equivalent to any other contract, the only difference being the way the offer and the acceptance are presented.[15]

According to Argentine case law, electronic evidence can, in principle, always be admitted. If there is an allegation of misuse or failure of the operating system that can affect the accuracy of such electronic data, then the *onus probandi* is on the party who is challenging it.

Although the recognition of new types of electronic evidence might be regarded as slow, it is good to point out that all over the country magistrates and arbitrators rule in favor of accepting the modern technologies as evidence, which is an indubitable benefit to all the parties involved and contributes to a more efficient judicial system.

IV. Doctrine

Following the same path as the judicial rulings, copious doctrine has formed to apply the laws governing postal mail to new digital media, in view of the numerous similarities between regular mail and other methods of communication like phone calls, chat room logs or multimedia messages.

Even before the era of the information technology, authors approached this subject, providing opinions about telegraph communications and recorded phone calls as evidence in trials. This doctrine remains a fundamental resource in finding ways of solving challenges facing the admissibility of electronic evidence. It also provides accurate and appropriate solutions for new technology improvements.

Since the DSA came into effect, doctrine has developed the theory of "non-repudiation:"

> "The guarantee of non-repudiation between sender and receiver allows repelling the refusal both of having received and of having sent the message. It not only guarantees the identity of the issuer, but also the integrity of the instrument. The law implements this guarantee by incorporating a novel legal effect, by attributing to the digital documents the presumption *iuris tantum* of authorship and authenticity, reversing the burden of proof and thus exceeding the provisions

[15] "AOL Argentina S.R.L. v. Government of the City of Buenos Aires", Appellate Court on Administrative and Tax Matters of the Autonomous City of Buenos Aires, Panel I, July 11, 2006 (Official Records of the Judiciary of the Autonomous City of Buenos Aires; RC J 155/11).

> made in the Civil Code regarding the private instruments made on paper, which require the recognition of the signature as a requirement of authenticity."[16]

This guarantee of non-repudiation asserted has been well received by the magistrates and arbitrators and is extensively used in judicial verdicts and arbitral awards. It is also very convenient for commercial trade, as it gives the much-needed assurance to close contracts using telecommunications.

The doctrine further asserts the multiple benefits of the use of electronic evidence and endorses its admittance in arbitration as well as in civil, commercial and criminal courts.

V. Forecast

For electronic evidence, the CCC is an improvement that can be very valuable for judges and arbitrators. Over time, all parties involved will learn to trust and benefit from this system, leaving behind physical media (when possible) and eventually evolving towards a paperless judicial system.

Even though there are several limitations that prevent unauthorized use of any form of written communication, including documents in electronic format, a valuable aspect of the law is that it can be applied to new forms of written or multimedia communications, such as mobile phone text messages (SMS), Snapchat, Facebook, WhatsApp or any new app, technology or social media available in the future.

Due to this flexibility, it will not be necessary to change the law with every new system for generating, sending and receiving data messages. The CCC as it is can provide useful solutions.

But the most significant improvement introduced by the CCC and the DSA is the equivalence and legal legitimacy of both electronic and handwritten signatures (and paper document/electronic document), with no difference when filed as evidence.

To achieve unconditional admissibility of electronic records as evidence in arbitration and litigation in Argentina, specific criteria have been created to satisfy the conditions of authenticity and reliability, and these criteria should be strengthened with new techniques of security and encryption introduced by advanced technologies, and the necessary understanding and reliance on new technology.

VI. Conclusion

[16] AUGUSTO C. BELLUSCIO AND EDUARDO A. ZANNONI, "CIVIL CODE AND OTHER COMPLEMENTARY LAWS", 1343 (Astrea, First Ed., 2007).

Although the legislation discussed in this article is a step in the right direction, there is more progress to be made in Argentina in the area of electronic evidence. Issues that still call for a solution, include the need of proper training of law enforcement agencies in handling electronic evidence, and correct methods of filing such evidence in an arbitration panel or in a court.

The government should also take measures to ensure that global trade requirements are fulfilled, including the regulation of digital signatures using biometrics methods such as voice recognition, retina or digital prints and other ways of creating electronic signatures that may come in the future.

The assimilation of new technology in the legal system demands a cultural change in arbitrators, judges and lawyers to ensure that the legislation is applied to arbitration and litigation. To support this, we recommend defense counsel keep pace with the rapidly changing digital world and the opportunities this brings in the field of justice.