Argentina

Enrique M. Stile and Diego Fernandez
Marval, O'Farrell and Mairal
Buenos Aires, Argentina

Introduction

This chapter will analyze the regulatory efforts Argentina has made regarding issues of the Internet, and how it compares to regulatory schemes imposed by other nations and international bodies. Among the topics it will explore are e-commerce, digital signatures, protection of personal data and privacy online, cybercrimes and Internet service providers’ (Internet service providers) responsibilities, freedom of speech online, and how the new Civil and Commercial Code, in force since August 2015, addresses issues of the Internet.

The chapter will explore issues of the Internet in the context of employment relationships; more specifically, what the scope of power an employer has with relation to the use of the Internet and its employees. Among the issues analyzed in such context will be the use of emails by an employee for both personal and professional use, and the treatment of such in relation to privacy expectations. The chapter also will address issues of social media networks, and how Argentine courts have decided on such issues. Lastly, the chapter will analyze the current situation regarding active unions.

E-Commerce in Argentina

What Is E-Commerce?

E-commerce is any type of commercial activity conducted through an electronic network, usually the Internet. These commercial activities include but are not limited to the buying and selling of goods or services, forming contracts, or the transferring of funds or data. E-commerce is usually divided into two categories — complete e-commerce and incomplete e-commerce.

The former refers to transactions in which the promotion, buying, and payment of the product occur within the electronic system. Distribution can occur within the electronic network or not, depending on the product or service. Incomplete e-commerce refers to transactions that begin on an electronic network, but the completion or payment of such transactions occurs outside the electronic system. Like other Latin American countries, the overwhelming majority of Argentina’s e-commerce is incomplete.
From another perspective, e-commerce also can be divided into four categories: business to business; business to consumer; business to government; and government to citizen. For the purposes of this section, e-commerce will refer to any commercial transaction conducted through an electronic network regardless of which parties are involved.

**Regulation of E-Commerce in Argentina**

While Argentina does not have a comprehensive regulatory scheme in place to govern e-commerce, there are some norms in place that address the issue: Law Number 24,240\(^1\) (the “Consumer Protection Law”); Resolution Number 412/1999, passed by the Ministry of Economy and Public Works and Services;\(^2\) and Resolution Number 104/2005, passed by the Ministry of Economy.\(^3\) The new Civil and Commercial Code also has incorporated the recognition of electronic documents and digital signatures.

The Consumer Protection Law was intended to protect consumers in the current commercial market, whereby the protections granted by the Law have been said to apply to consumers dealing in the e-commerce market. The Law extends its protection to any consumer, which it defines as being any natural or legal entity that buys or consumes goods or services, of which it is the end or final user. Therefore, the Law does not protect commercial transactions that are engaged with the purpose of carrying out other commercial transactions, or to benefit a third-party consumer.

The Consumer Protection Law includes regulations that are imposed on commercial providers. Commercial providers are mandated to divulge all pertinent information regarding the goods or services they are offering, and this information must be made available free of charge to consumers. Commercial providers are not to discriminate as to with which consumers they engage in business, and commercial providers are forbidden from discriminating against foreigners in regards to pricing or quality of the goods or services.

The Law offers detailed information as to what constitutes a valid contract of sale, the method in which acceptance can be given, the period of 10 days within which the consumer is allowed to revoke acceptance, and the implied warranties for which commercial providers are responsible. The Law states that, when the terms of an agreement are inconclusive, the agreement must be interpreted to benefit the consumer.

While the protections for consumers are fair, an issue arises when attempting to apply the protections in the realm of e-commerce. In theory, the same protections apply to consumers on the electronic market; however, in practice, the protections can be difficult to enforce. In e-commerce, transactions are often fast-paced,

---

\(^1\) Law Number 24,240, published on 13 October 1993.
\(^2\) Regulation Number 412/1999, published on 9 April 1999.
\(^3\) Regulation Number 104/2005, published on 27 June 2005.
increasing the possibility of deception. Issues also arise in regard to the formulation of contracts and what constitutes a legally enforceable agreement.

Resolution Number 412/1999 was passed to approve the recommendations formulated by the Work Group on Electronic Commerce. The Resolution was, for the most part, aspirational in nature. The Resolution called for the implementation of a national database or method of tracking the growth of national e-commerce activity. It also recommended that the Argentine government develop mechanisms to facilitate cooperation with international organizations that seek to regulate e-commerce.

The Resolution also called for the establishment of mechanisms designed to protect the personal data of consumers engaged in e-commerce, as well as methods to ensure the validity of digital signatures. The Resolution called for the expansion of legislation designed to protect intellectual property rights of individuals or legal entities in the digital market. The Resolution also called for Argentina to adhere to the international agreements proposed by the World Intellectual Property Organization (WIPO), regarding the treatment of intellectual property online. Additionally, the Resolution stated that a mechanism should be enacted to facilitate the relationship between the government and the private market. This proposition was suggested to facilitate the issue of taxation and customs surrounding e-commerce. The Resolution was a step in the right direction; however, it did not offer concrete regulations of e-commerce. While some of the suggested provisions were adopted, for the most part, the provisions remained as suggested guidelines.

Resolution Number 104/2005 also deals with e-commerce. This is perhaps the most influential of the regulations discussed here because, unlike the others, this Resolution regulates transactions entered into using the Internet. More importantly, this Resolution states that any infringements that occur in Internet-derived transactions will be addressed in accordance to the Consumer Protection Law. The Resolution adopted the agreement reached by MERCOSUR in 2004.

Article 2 of the Resolution establishes the duties of online commercial providers. It sets out the requirement to divulge any pertinent information as to the product or service being offered, including, but not limited to, the conditions of delivery, the cancellation process, the return process (and who bears the cost), the final cost of the product, the warnings regarding the products (if possibly harmful to consumers), and the process by which to modify the purchase agreement.

Article 3 of the Resolution also states that online commercial providers must provide consumers with information regarding their physical and/or electronic location. A customer service phone number or email address must also be provided, along with any information regarding the duration and extent of any

---

4 Regulation Number 412/1999, article 1.
5 MERCOSUR is a sub-regional international organization created to promote free trade, and the fluidity of goods in the region. Argentina is one of the five member states; the others are Brazil, Uruguay, Paraguay, and Venezuela.
warranty. Additionally, article 4 makes it clear that the consumers’ silence in respect to an offer will not necessarily constitute an acceptance.

Therefore, online commercial providers are required to have mechanisms to detect and inform online consumers of possible errors with their transactions prior to the finalization of such transactions. Consumers also are to be provided with the information of the consumer protection department on the website of the online commercial provider.

Finally, article 6 of the Resolution mandates the cooperation in sharing of information regarding items covered by the Resolution with other members of the MERCOSUR. The Argentine Supreme Court has made some interesting and important decisions regarding e-commerce. However, issues such as electronic payment methods, the formulation of contracts, and jurisdictional questions are still to be addressed and regulated.

**Digital Signatures**

**Civil Code**

The Civil Code, in force until July 2015 and first enacted in 1869, recognized documents as being instruments with content. When the Civil Code was created, the instrument referred to was usually paper. In fact, article 978 only recognized agreements in written documents, and article 1,012 required the agreement to be on paper accompanied by a signature for private matters. Given these limitations, it was a challenge to recognize electronic or digital agreements using the Civil Code as it was written.6

**Laws Governing Digital Signatures**

The first attempt to incorporate the concept of electronic or digital documents into the Argentine legal framework was in 1996, with Law Number 24,624.7 The Law allowed for documents relating to the national public administration to be archived and stored in an electronic or optical manner. While the Law was a step in the right direction, it only recognized electronic documents in the public sector as valid.

It was not until 2001 with the passing of the Digital Signatures Law (Law Number 25,506)8 that the recognition of electronic and digital documents became valid in the private sector. The Law defined a digital document as the digital representation of acts or events, regardless of the medium used for its installation or file storage. The Law thus established the functional equivalence between a digital document and a written document on paper. Article 6 of the Law explicitly states that a digital document fulfills its equivalent to a written document.

---

6 This was overcome by the new Civil and Commercial Code.
7 Law Number 24,624, published on 29 December 1995.
The Law makes a distinction between electronic and digital signatures. A digital signature according to the Law is the application of a mathematical procedure to a digital document that requires information only known to the signer, which is what most parts of the world also consider to be a digital signature.

The Law also states that a digital signature must be subject to third-party verification, which will verify both the authenticity of the signature, as well as detect any subsequent alterations that might have been made after the signing of either party. This authority is called the Certifying Authority, and it is in charge of issuing the digital signature certificates to the parties. On the other hand, an electronic signature refers to a set of data that is integrated, linked, or associated with other data as a means of conveying a signature by a signee.

The functional equivalence of a digital signature is stated by article 3 of the Law, in which it states that a digital signature will satisfy the requirement of a written signature when mandated by law. Therefore, article 1,012 of the Civil Code would be satisfied by a digital signature. However, while a digital signature will be valid under the Law, an electronic signature lacks the necessary requirements to be legally binding as it is. Any individual alleging the validity of an electronic signature will have the burden of demonstrating its authenticity.

In order for a digital signature to be valid under the Digital Signatures Law, it must meet certain requirements. It must be accompanied by a digital certificate that must be digitally signed and approved by a third party. This third party must be a licensed Certifying Authority that will confirm the identities of the parties, verify the authenticity of the documents, and keep records of the encryption processes used for the digital signature. Certifying Authorities are basically notaries of the virtual world. Foreign certificates, which in principle have no effect under Argentine law, can be validated if:

- The foreign certificate complies with the conditions established by the Law and regulations and a reciprocity agreement signed between Argentina and the country of origin of the foreign certificate is in effect; or
- Such certificates are recognized by an Argentine Certifying Authority, to ensure their validity and effectiveness under the Law, and this recognition was validated by the enforcement authority.

The encryption process can be one of two types, symmetrical and asymmetrical. In a symmetrical system, there is one mathematical procedure, or code generated by the sender of document. The code is sent in a communication separately from the one containing the digital document to be signed. The receiver uses the code to decipher the message and sign it. In an asymmetrical system, there are two codes generated by the receiver of messages.

One of the two codes is public while the other code is private and known only to the receiver. The sender uses the public code of the receiver to encrypt the message, and the receiver uses his private code to decipher the message and sign the digital document. Both systems are designed to increase the legitimization of
a digital signature, as it ensures that only those intended to have access to documents are the ones who are really signing it. Currently, in Argentina, the asymmetrical system is used with the Certifying Authorities having the duty to dispense the codes to the users.

Exceptions to Digital Signatures

While the digital signature will be valid for most transactions, there are a few exceptions where it will not suffice; for example, causes of death provisions still require a written signature. Judicial acts or decisions regarding family law also still require written signatures. Generally, personal acts require written confirmation, as well as any acts which call for a written signature by law or by the contracting parties.

Law Number 26,685, passed in 2011, allows the use of electronic documents and digital signatures for the administrative and judicial processes of the Supreme Court and further recognized the use of technological solutions as legitimate under the Law. Additionally, in 2014, Argentina made progress by certifying the company Encode SA as a Certifying Authority under Administrative Decision Number 927/2014.

Prior to this, the Digital Signatures Law was applicable to the private sector only in theory because the necessary certifying authorities were not in existence. Even though the administrative decision granted Encode SA its license to become a Certifying Authority, the digital signature is not yet commonly used in the private sector.

Protection of Personal Data and Privacy

Data Protection Law

The most comprehensive statutory regulation passed by the Argentine government regarding the protection of personal data is the Personal Data Protection Law (Law Number 25,326), and Regulatory Decree Number 1558/2001 (the “Data Protection Law”), which has the Data Protection Authority as its controlling authority. Additionally, the Data Protection Authority has recently adopted a new rule in which it sets out guidelines and good practices for software developers.

Purpose of Data Protection Law

The main purpose of the Data Protection Law is to guarantee the complete protection of data contained in files, records, databases, or other technical means, either public or private, if destined “to supply information”, and the rights to good reputation, privacy, and access to information, in accordance with article 43 of the

---

Constitution. In addition, the provisions of the Data Protection Law are applicable to legal entities.

According to the Data Protection Law, a private file, record, or database will be deemed destined “to supply information” if its use exceeds an exclusively personal use and if its purpose is the assignment or transfer of personal data, not taking into account whether such personal data treatment is free of charge. Under the Data Protection Law, “personal data” means any kind of information referring to individuals or legal entities, whether identifiable or not., “Sensitive data” means any personal data revealing racial or ethnic origin, political affiliation, religious, moral, or philosophical convictions, union activity, or information related to health or sexual orientation. “File, record, or database” means any organized collection of personal data, subject to data processing, whether electronic or not.

Protection of Data

The Data Protection Law states that the gathering of personal data cannot be done through dishonest, fraudulent, or illegal means. The regulatory decree states that the determination of good faith and loyalty in the acquiring and use of personal data must be based upon the analysis of the procedure utilized and the information previously provided to the data subject.

The Law also states that collected personal data cannot be used for different or incompatible purposes from those it was intended for, and any personal data that is collected must be accurate and current. Moreover, personal data which is completely or partially inaccurate must be deleted, substituted, or supplemented by the individual or entity responsible for the database if there is knowledge of such inaccuracy or incompleteness. The data subject must be allowed access to the information being stored.

The Law also states that the responsible person or user of the database shall adopt the necessary technical and organizational measures to guarantee the protection and confidentiality of personal data. The registration of personal data in databases which do not comply with such requirements is forbidden. The responsible person and any person who intervenes in any phase of the treatment of personal data have a duty of professional secrecy. The duty will persist even after the relationship with the data subject is terminated. Such duty of secrecy will be exempted if required by a judicial Resolution or for public safety, national defense, or public health reasons.

Consent

The general principle under the Data Protection Law is that any treatment, disclosure, collection, storage, amendment, destruction, and processing of personal data must be specifically consented to by the data subject. Such consent must be given freely, based upon the information previously provided to the data subject and expressed in writing or by equivalent means depending on each case. The data subject, with no retroactive effects, may revoke the consent at any time.
Nonetheless, the Law does mention several exceptions in which informed consent of the data subject is not necessary; for example, when the data is obtained from public sources with unrestricted access, consent is not needed. When the data is collected by the government pursuant to its legal authority or in its capacity as such, consent is not required.

When the information is limited to name, identification number, tax or social security identification numbers, occupation, date of birth, and domicile, consent is not required. Consent also is not needed if the information derives from a contractual, scientific, or professional relationship with the data subject, provided that such data is necessary for the development and compliance with such relationship.

Nor is consent needed if the information is related to transactions made by financial institutions pursuant to Law Number 21,526, which provides for the allowed functions of public and private financial institutions. For example, article 39 provides exceptions for confidentiality obligations that financial institutions have for their clients. Financial institutions are allowed to divulge clients’ personal information without consent if they are asked to do so by a court. A government agency can request information of a client provided that it has a legitimate purpose, such as tax auditing. Lastly, the Central Bank of Argentina can request information as long as it is acting within its scope of functions.

With regard to sensitive data, the Law provides for a more restrictive set of regulations. It states that no person may be obliged to supply such information, and the sensitive data may only be collected if authorized by law, and for a public interest purpose. Such data also may be collected for statistical or scientific purposes, provided that the data subject cannot be identified. Setting up files, records, or databases which either directly or indirectly reveal sensitive data is forbidden. Data related to criminal precedents may be collected solely by the relevant competent authorities, and within the scope of the applicable legislation.

Assignment of Personal Data

Personal data can only be assigned for the compliance of purposes directly related to the legitimate interest of the assignor and assignee and if made with the previous consent of the data subject. Such consent may be revoked. Additionally, the owner must be informed of the purpose of the assignment as well as of the identity of the assignee.

Consent to the assignment may not be required if it is so provided by law; in those cases when the use of personal data is not subject to the data subject’s consent (see text, above); if it is made between governmental agencies pursuant to their legal authority; and when personal data is related to the health of individuals, and its disclosure is necessary for public health reasons. The

---

identity of the individual must be preserved; and if, due to the process used, the
data subject may not be identified (dissociated information).

The assignee of the personal data shall be subject to the same legal obligations
as the assignor and both shall be jointly and severally liable for any obligations
vis-à-vis the Data Protection Authority and the data subject. The assignee may
be total or partially exempted from liability provided that he can prove that the
cause of the damage could not be attributed to him or her.

International Transfer of Personal Data

Transfer of personal data to other countries or to international organizations is
forbidden if such countries or organizations do not grant an appropriate level of
protection according to the Data Protection Authority’s criteria. This prohibition
ceases if the data subject expressly consents to the international transfer.

The above restriction does not apply to international judicial collaboration; some
cases in connection with medical treatments; banking or stock exchange
transactions in accordance with applicable legislation; transfer of data pursuant
to international treaties; and transfer of data between governmental intelligence
agencies for purposes of fighting against organized crime, terrorism, and drug-
dealing.

Rights of Data Subject

In principle, the data subject has the right to access to any database containing
personal data owned by him, request information in connection with his data,
and demand the correction, deletion, update, or confidential treatment of his or
her personal data. Noncompliance with such obligations by the party responsible
or user of the files, records, or databases within 10 days entitles the data to be
subject to judicial claims and to give notice of such failure to the Data Protection
Authority.

The right to access must include the data subject’s rights to know whether the
data subject’s information is in the file, record or database; to know all the
information regarding the data subject included in the file, record, or database;
to request information regarding the sources through which the personal data
was collected; to request to be informed of the purposes of the collection; to
know the intended use imagined for the personal data; and to know whether the
file is registered according to the Data Protection Law.

Sanctions and Remedies Available under Data Protection Law

Notwithstanding other sanctions and/or indemnification for damages derived
from other applicable laws, the Data Protection Authority may apply the
following penalties in the event of violation of the Data Protection Law:

• Observation;
• Suspension;
• Fines between AR $1,000 and AR $100,000;
• Business closure; or
• Cancellation of the file, record, or database.

The Data Protection Authority also has declared that any responsible person and any person who intervenes in any phase of the treatment of databases must keep an updated “Security Document.” The information to be included in this “Security Document” will vary according to the personal data being processed in each case. Three security levels exist, namely:

• Basic level of security — Applied to personal data in general;
• Medium security level — Applied to databases owned by entities fulfilling a public or private function that must maintain their confidentiality due to an express legal provision; and
• Critical security level — Applied to databases that manage sensitive data.

Article 31 of the Data Protection Law stipulates what an individual or entity that violates the Data Protection Law will be sanctioned or fined. The range of administrative sanctions and fines is as follows:

• Moderate — Fine of AR $1,000 to AR $25,000;
• Severe — Suspension of one to 30 days and/or a fine of AR $25,00 to AR $80,000; and

Very severe — Suspension of 31 to 365 days and/or fine of AR $80,001 to AR $100,000.

Examples of non-compliance within each of the categories are as follows:

• Moderate — Not respecting the gratuity principle (data subjects should be able to exercise their rights free of charge, such as access, deletion, and amendment); not providing in a timely manner any information or documentation required to the Data Protection Authority; and not registering and/or renewing the corresponding data base;
• Severe — Collecting personal data without having the subject’s prior express and informed consent; not taking appropriate measures when the subject requests access, deletion, and amendment; retaining personal data for a longer period than necessary; not removing the data subject’s email from a database upon request; and obstructing the Data Protection Authority’s inspection and audit’s procedures; and
• Very severe — Not registering a database upon request from the Data Protection Authority; declaring false information when registering a database; not ceasing a non-compliant treatment of personal data upon request from the data subject and/or the Data Protection Authority; collecting data by misleading or fraudulent activities; and transferring personal data overseas to a country without a proper level of protection or without consent from the data subject.

(Release 5 – 2016)
In addition, the Criminal Code has been amended by the Data Protection Law to punish with imprisonment those who knowingly supply false information in a personal data file; gain access to databases illegally; or disclose personal data protected by law.

Software Developers and Privacy

The Data Protection Authority adopted Rule Number 18/2005,¹² which sets out guidelines for software developers who in most cases are not familiar with the principles of data protection of the Data Protection Law. The guidelines emphasize that software applications have the ability to collect, treat, and process personal data; therefore, it is important to make sure that the application is in compliance with the terms and obligations under the Data Protection Law.

In order to protect privacy and personal data during the software developing process, the Rule recommends that software developers should take into account privacy in the process of developing an application; develop the applications using “privacy by design”, considering any privacy and data protection implications from day one; establish a clear privacy policy with easy access; activate the privacy options by default; allow users to control and choose their privacy options; limit the quantity of data collected; protect the data collected and choose someone within the organization to be responsible for privacy compliance; and use privacy-enhancing technologies to protect users’ personal data by minimizing or eliminating data collection.

Furthermore, the guidelines highlight the importance of placing a clearly visible and transparent privacy policy informing users about the personal data collected, the purpose of the collection and how it is used, and who will have access to the data (including any third parties). The guidelines address the specific problems of mobile apps echoing the difficulties that the size of the screen poses in terms of proper display of privacy policies.

To that end, it suggests that developers should be creative to show users what their privacy practices are, e.g. in the use of graphics, colors, and sound, to try to get their attention. Lastly, the Guidelines refer to apps designed to be used by children. In that connection, they suggest limiting the collection of data from children as much as possible; contemplating stricter security measures; avoiding the sharing of personal information of children; and, when necessary, obtaining parental consent.

Cyber Crimes and Internet Service Provider Responsibilities

Areas such as the responsibilities of Internet service providers or Internet intermediaries are not explicitly addressed by Argentine law. Nonetheless, in 2008, Argentina made great improvements when it passed legislation and amended the Criminal Code.

Problems with Regulating Cybercrimes

While some progress has been made in the area, cybercrime is still a challenge. A lack of a comprehensive and specific regulatory scheme is needed. Another obstacle that makes cybercrimes hard to govern is that many of these crimes are international in nature, meaning they are committed in one country, but affect people or entities in another country.

This raises issues of jurisdiction, applicable law, and authority. The lack of an international agreement to govern these cybercrimes also is an obstacle to the proper regulation of cybercrimes. Additionally, the ability of the infringer to hide in anonymity when committing crimes also presents an obstacle in regulating and prosecuting cybercrimes. Lastly, the rapid advancement of technology also presents an obstacle, as legislation cannot keep up with the advances being made.

Cybercrime Law

Prior to the Cybercrime Law (Law Number 26,388),13 Argentina was considered a favorable venue for cybercriminals because one of the most important principles of Argentina’s criminal law is that, for a crime to exist and be punished, the illegal conduct must be expressly and specifically codified. A lack of codified laws governing cybercrimes allowed cybercriminals to escape prosecution.

Prior to 2008, many cybercriminals committed cybercrimes in Argentina that affected other nations and went unpunished. Argentina could not prosecute the crimes and could not extradite the criminals without a regulatory framework governing cybercrimes. The Cybercrime Law codified various areas of crimes that were pervasive online. The Cybercrime Law modified the Criminal Code and made the following cyber actions punishable crimes:

- Informatics damages;
- Informatics fraud;
- Tampering with evidence;
- Child pornography;
- Privacy crimes;
- Crimes against national security and interruption of public communications; and
- Falsifying electronic documents.

Informatics damages were added to the Criminal Code as article 183. This made it illegal for someone to destroy, alter, or make unavailable or useless another’s data, documents, programs, or informatics systems. Article 183 is very general but is meant to include crimes such as the destruction, illicit use, or alterations of data systems, or online informatics systems. The unsolicited introduction of a
computer program or virus into an online system also is illegal under article 183, as well as any tampering with a website belonging to another.

Informatics fraud makes it a crime to alter an online system with the purpose of defrauding someone else. It also extended the protections against ordinary fraud to cover fraud conducted through electronic means. Similarly, while the prohibition against tampering with evidence was already a crime, the Cybercrime Law extends the prohibition to any evidence, regardless of format.

The child pornography crime is perhaps the most comprehensive regulation put in place. The Law amended the Criminal Code to include in article 128 the prohibition of child pornography by any means. The Law made it illegal to produce, finance, distribute, facilitate, offer, or divulge content displaying a minor under 18 years old in sexual activity or displaying their genitals. Additionally, it is illegal to promote or organize by any means live activity that would include minors acting in a sexual manner. These crimes carry prison sentences ranging from six months to four years. The Cybercrime Law also incorporates the violation of electronic correspondence and punishes the exposure of secrets obtained illegally by means such as hacking. For the most part, unauthorized access to a database is a punishable crime under the Cybercrime Law. The illicit interruption of public communications includes electronic communications as well. Lastly, the falsifying of electronic or digital documents also was made illegal.

Internet Service Provider Responsibility

Strict Liability

In 2012, Division J of the National Court of Appeals in Civil Matters applied a standard of strict liability in an action against Google and Yahoo. In this case,\textsuperscript{14} an Argentine model had sued both entities because her name was being related and linked to sexually explicit content in the search results. The Court of Appeals rejected the reasoning of the lower court which had ruled that search engines could only be responsible after having actual knowledge of an infringement, by judicial notification.

The Court of Appeals ruled that a search engine is not merely a facilitator, but rather a promoter of the content being displayed, because the algorithms used to run the search and display the search results are developed by the search engines. Thus, the Court of Appeals found it appropriate to impose a standard of strict liability and found the defendants responsible, and ordered Google to pay AR $75,000 and Yahoo to pay AR $15,000 in damages.

Standard of Fault

In 2013,\textsuperscript{15} with very similar facts to the case above, Division I of the Court of Appeals in Civil Matters, applying a standard of fault analysis, found that

\textsuperscript{14} Krum, Andrea Paola v. Yahoo de Argentina S.R.L, et al. (2012).
\textsuperscript{15} L.B v. Google, Inc. (2013).
Google was not liable for the infringing content of a third party. Here, the Court of Appeals reasoned that search engines are merely intermediaries who provide access to content but are not able to alter such content on their own.

In addition, the Court of Appeals reasoned that while search engines have mechanisms to filter results, the burden of monitoring all content should not be placed on them but instead it should rest on the plaintiff. Lastly, the Court of Appeals stated that the plaintiff had failed to show that Google had failed to remove or block the content after having actual knowledge of its existence.

**Supreme Court Decision**

In 2014, the Argentine Supreme Court issued a decision on search engine liability regarding the actions and content of a third party that the search engines did not generate or control. The facts of this case are similar to those of the cases decided by the Court of Appeals in that an Argentine model also sued Google and Yahoo for linking her image and name to third-party websites displaying sexually explicit content.

The District Court had ruled in favor of the model, while the Court of Appeals reversed the decision in favor of Google, both using a standard of fault analysis. The Supreme Court agreed to use a standard of fault and found the search engines not liable for the infringing actions of third parties.

The Supreme Court acknowledged that the case required the court to balance rights of reputation and image, against the rights of free speech of another. Using the standard of fault analysis, the court reasoned that holding liable a search engine who merely displays third-party content would be like holding a library liable for having harmful books in their catalogs. The Supreme Court stated that a search engine should not carry the burden of monitoring all the content it displays. Nonetheless, the court did state that search engines could be found responsible for the content of a third party under certain circumstances.

Thus, if the search engines had actual knowledge of the illicit content and failed to take remedial action, liability could be imposed on them. The court continued to state that actual knowledge could be established in two ways. If the infringing nature of the content was obvious or evidently infringing, then an out-of-court notification would suffice, while if the content is not obviously infringing, then a court notification would be necessary to establish actual knowledge.

In this case the court decided that, upon having actual knowledge of the infringing content, the search engines acted diligently to remove it. On the issue of using thumbnail images of the plaintiff in search results, the Supreme Court ruled that it was not necessary to have the plaintiff’s consent, and therefore it would not violate Intellectual Property Law (Law Number 11.723), which holds that prior consent is required to use another’s image.

---

The court stated that the use of thumbnail images was identical to the displaying of third-party links in search results. The only difference was that the thumbnails were a visualization of the third-party content, as opposed to a link.

Post-Supreme Court Decisions

Since the decision of the Supreme Court was rendered, there have been similar cases decided by other Courts of Appeals. In some cases, the allegedly infringing parties were not search engines, but instead electronic platforms (websites). The judges presiding over these cases have not all agreed, finding the websites liable on some occasions and not on others.

In May 2015, the Court of Appeals in Criminal Matters decided a case involving the unauthorized posting by third parties on the websites www.taringa.net, www.portalplanetasedna.com.ar, and www.tipete.com of links that redirected users to files containing literary works by the well-known writer Jorge Luis Borges. The plaintiff was the owner of the intellectual property, and was suing the websites for violating intellectual property rights. The Court of Appeals, using a standard of fault analysis, found the websites not liable for the postings of third parties on their electronic platforms.

The Court reasoned that the websites were mere intermediaries and were not owners of the content posted by their users. The Court formed the analogy that holding the websites responsible would be like holding the owner of an Internet café responsible for the illicit Internet navigation of its customers. In other words, the Court viewed the websites as neutral hosts. Nonetheless, the Court did state that, upon receiving actual knowledge of any illicit content, the Internet intermediaries would need to take corrective action, which the defendant did, according to the record. Therefore, the Court of Appeals in Criminal Matters rejected the plaintiff’s claims.

In contrast to this decision, in May 2015, the National Court of Appeals in Civil and Commercial Matters Divisions I and III ruled against nationally known websites in a suit brought by Nike International Ltd., for violation of the Trade Mark Law. In 2004, Nike sought legal action against DeRemate for violating its rights under Argentine trade mark laws by allowing its users to offer Nike counterfeit products on its platform www.deremate.com.ar. However, negotiations were sought and the parties came to an agreement that stated that DeRemate would remove illicit Nike products when notified.

By 2008, Nike sought further action, claiming that DeRemate was in breach of the agreement and that illicit Nike goods were still being sold on the website. Therefore, Nike requested that DeRemate be ordered to cease any use of Nike, including its use as a keyword under the Google Ad Word program, and compensate Nike for damages.

19 Nike International Ltd. v. Compañía de Medios Digitales CMD SA (2015).
In 2007, under similar facts, Nike sought action against CMD, which owns and operates the website www.masoportunidades.com.ar on which counterfeit Nike products were being offered. Both DeRemate and CMD maintained that they were not responsible because they were neutral virtual markets which allowed third-party users to convene and carry out interactions. They rejected the notion that they were an online store: They denied owning any of the products sold on their websites, and they denied any participation in the transactions. The Court of Appeals disagreed with the defendants in both cases.

The Court found both DeRemate and CMD to be active participants in the illicit postings of the third parties on their websites. The Court found DeRemate to have an active role because it had contracted search engines to retrieve its website using the keyword Nike and provided a payment method that facilitated the illicit transactions. CMD also was found to have an active role because it promoted the products of its users and took five per cent of every transaction. Both were ordered to pay damages, implement filters to prevent illicit postings, and remove any illicit products from their websites upon receiving notification.

**Freedom of Speech on Internet**

**In General**

Argentine law does not specifically address the issue of freedom of speech on the Internet. Instead, guarantees from existing freedom-of-speech law are applied to regulate online behavior. However, there are four current attempts to pass regulations to better protect and regulate online behavior.

The most laws are derived from the American Convention on Human Rights, also known as the Pacto de San Jose de Costa Rica. Law Number 23,05420 adopted the freedom of speech provisions suggested by the American Convention on Human Rights. The Law guarantees to protect all forms of speech, regardless of method of expression. It explicitly forbids any type of censorship. However, it does not guarantee immunity from legal actions brought on certain actions that are forbidden by law.

Such actions must be clearly codified and adopted by law. Examples of areas where free speech could lead to legal action against the person are matters of national security, public health, public order, and defamation. The Law acknowledges that censorship may be appropriate when the morality of a child is in danger, such as in child pornography. In 2005, Law Number 26,03221 formally acknowledged that the right to access of information through the Internet is a right protected under freedom of speech.

---

20 Law Number 23.054, published on 19 March 1984.
Yahoo and Anti-Semitism

In 2000, the Federal Court on Civil, Commercial, and Contentious Matters of San Martin decided a landmark case in *Kirovsky, Jorge Osvaldo*, regarding the prohibition of sale of anti-Semitic products online. The products were posted by third parties, while Yahoo was being used to bring up the search results. The Court was asked to determine whether the posting of Nazi products online was prohibited by Argentine anti-discrimination law.

The Federal Court, in a controversial decision, stated that, while offensive, the posting of Nazi products online by third parties did not make Yahoo liable as its actions were protected under freedom of expression. The Court furthered stated that, if it found Yahoo liable, it also must find libraries that offer Hitler’s book *Mein Kampf* liable.

New Civil and Commercial Code

In 2014, the new Civil and Commercial Code became law as Law Number 26,994 and was promulgated under Decree Number 1775/2014. The Civil and Commercial Code came into effect on 1 August 2015. Among the many changes the Civil and Commercial Code brings is the clarity it will provide to issues relating to the increased use of electronic means to engage in commercial activity.

The Civil and Commercial Code formally incorporates the validity of digital signatures in article 288, which states that, in matters conducted via electronic means that require an individual’s signature, a digital signature will suffice. However, it states that the signature must convey the identity of the person signing, leaving little room for doubt.

The Code also deals with the issue of long-distance contracting in article 1105. Among the methods the Civil and Commercial Code recognizes are contracts formed via telecommunications or electronic means. Article 1106 indicates that, when a written contract is required by law, an electronic document will suffice for the written contract requirement.

Article 1107 furthers states that the burden of informing the other party of all pertinent information in relation to the contract will by default rest with the provider of goods. In other words, it is the provider who will be deemed responsible for informing the other party of the necessary method of acceptance and who bears the risk of damages.

Article 1108 refers to the time between when an offer is made and acceptance can be made. The article states that an electronic offer should include the time frame within which acceptance is required. If such time frame is not included in the offer, the other party has the option to accept the offer so long as it has the offer in their possession.

---


23 Law Number 26,994, published on 7 October 2014.
With regard to applicable law governing contract disputes that might arise in contracts formed in one jurisdiction and accepted in another, the Civil and Commercial Code states in article 1109 that the contract laws of the jurisdiction in which the consumer receives the offer provisions or where it was intended to be received will govern contract disputes. Additionally, the consumer will hold an irrevocable period of 10 days in which they could withdraw their acceptance of a contract entered into from a distance, as stated by article 1110.

Any provisions contracting away this irrevocable 10-day withdrawal period will be null and void. A provider is required to inform the consumer of their right to revoke their acceptance, and if they are not made aware, the period of revocability will not begin to run. A consumer wishing to revoke an acceptance is required to inform the provider in writing (either on paper or electronically) or similar means used for the initial contract.

There are a few exceptions where the consumer may not revoke an acceptance to an offer. Article 1116 states that a consumer is barred from revoking an acceptance if the provider was asked to provide the consumer with a specifically personalized product that met specific requirements set by the consumer. While the Civil and Commercial Code does not state the reasoning it is quite clear that a personalized product will not be as marketable to other clients if the initial consumer rescinds on the acceptance of the product. Products that deteriorate fairly quickly also are not revocable by the consumer. Another instance where an acceptance will not be revocable is when the product in question is a digital file, or software, which upon delivery could be downloaded, stored, and used indefinitely. Lastly, products such as newspapers and magazines cannot be revoked by the client, as their value is time-sensitive.

Social Networks in Workplace

Power of Employer

The use of social network tools in Argentina in the workplace is not regulated under a specific law, and the parameters and rules of their use are usually granted by the employers and the particular case law. Nevertheless, it has become a matter of increasing concern for employers.

Employer control should be executed within certain parameters, contemplating the employee’s privacy rights. For instance, an employer could be allowed to monitor how much time an employee uses Internet at work or what sites he visits. On the other hand, if the employer has access to an employee’s social network account, it could be an infringement of the employee’s privacy rights and the employee could file a complaint against the employer.

The Labor Contract Law (Law Number 20,744) governs the majority of labor relationships in Argentina. However, as mentioned above, it does not contain a specific rule about this matter. Considering the boundaries established by a company’s common practice and case law, there are some rules to observe to
comply with the normal standards and minimize risks of dispute with employees. Consequently, an employer may be allowed to monitor the use of work tools, including time consumed with social network tools or sites, but it may not affect an employee’s privacy, including accessing an employee’s own social network accounts without authorization.

The limits of employer control should be previously established. Common practice recommends signing a document in which the employee acknowledges the power of the employer to control the use of social network tools by employees at work. This practice would, in principle, minimize the risk of future claims by an employee concerning invasion of privacy. An employer may control the use of social networks at work within certain limits (i.e., monitor the time consumed by the employee and sites visited, although not to access an employee’s own accounts without authorization). However, it is required to advise an employee about the limits of use and the power of an employer to control use. Usually, a document is signed by an employee at the time of commencement of work.

Use of Email

There is no specific regulation in Argentina as regards electronic communications in the workplace or legal prohibitions that prevent employers from establishing a corporate policy to be observed by employees. The Labor Contract Law is based on the principle of “good faith” that must be observed by both parties throughout the employment term. Therefore, it might be interpreted that the observance of a sensible corporate policy regarding electronic communications falls within the scope of an employee’s duty of good faith.

The Labor Contract Law grants an employer the authority to direct and organize the company business. Furthermore, the Labor Contract Law establishes that an employee should observe the employer’s instructions regarding work to be carried out. A corporate policy on electronic communications in the workplace could be considered among those instructions. In turn, employee compliance with the policy could be regarded as part of the duty of due diligence and cooperation.

Employees should be warned that misuse of communication tools could lead to disciplinary measures or dismissal with cause in the event of continued misuse. The Labor Contract Law enables an employer to apply disciplinary measures, provided they are proportionate to the breach. Furthermore, the Labor Contract Law establishes that employees may be liable for damages caused to employer interests with malice or by willful misconduct.

24 Law Number 20,744, section 63.
25 Law Number 20,744, section 64.
26 Law Number 20,744, section 86.
27 Law Number 20,744, section 84.
28 Law Number 20,744, section 67.
29 Law Number 20,744, section 68.
30 Law Number 20,744, section 87.
Notwithstanding the above, it must be taken into account that the Constitution grants special protection to correspondence and private papers, considering it inviolable.31 In that sense, in Lanata,32 the Criminal and Correctional Court of Appeals held that:

“. . . In relation to the legal protection awarded to correspondence and to private papers, email should be put on a level equal to traditional mail. “Email” possesses even more marked privacy protection characteristics than traditional mail, since for its functioning it is required a server, a user name and an access code, which forbid third parties interference in the data that could be filed in, or issued through, it . . . .”

Therefore, it would be reasonable to understand that the constitutional protection should cover the personal email accounts of employees. However, it should be determined whether the constitutional right also may be applied to email accounts provided by employers to employees as a consequence of the labor relationship between them.

**Conclusion**

Argentina does not have a general and comprehensive regulatory scheme regarding the Internet, although legislative efforts to regulate online activity can be observed over the last years with reasonable success. In that regard, the Consumer Protection Code, the Data Protection Law, the Digital Signatures Law, and the Civil and Commercial Code provide the basic rules regarding e-commerce. Argentina has also advanced in matters of cybercrime and Internet service provider responsibility.

---

31 Constitution, section 18.