Argentina - Cybersecurity

TABLE OF CONTENTS

June 2019

1. GOVERNING TEXTS

1.1. Legislation

Currently, Argentina does not have general or omnibus legislation on cybersecurity. However, in the past few years several regulations have been enacted on sectoral matters (i.e. personal data, financial entities or internet service suppliers, public sector) which reflects the increasing importance this matter has for the Government in office.

As for sectoral legislation, the following are applicable:

- Personal Data Protection Act, Act No. 25.326 of 2000 ('the Act');
- the Argentinian data protection authority's ('AAIP') Resolution No. 47/2018 establishing Recommended Security Measures for the Processing and Conservation of Personal Data (only available in Spanish here) ('the Resolution');
- the Argentine Central Bank's ('BCRA') Communication 6354 (only available in Spanish here), as amended by Communication 6375 (only available in Spanish here) and Communication 6271 (only available in Spanish here);
- Digital Signature Act, Act No.25.506 of 2001 (only available in Spanish here) ('the Digital Signature Act'), as amended by Decree No. 182/2019 on Digital Signatures (only available in Spanish here); and
- Act No. 25.690 on Internet Service Providers (only available in Spanish here).

Each of the above seek to reflect the importance of cybersecurity, to establish standards or obligations to protect and safeguard sensitive data and institutional systems, and to prevent cybersecurity incidents.

1.2. Regulatory authority

In Argentina, there are several administrative authorities dedicated to cybersecurity. To date, these authorities have mainly issued regulations directed to the public sector, and currently only approach the private sector for mutual collaboration. Nonetheless, these authorities may eventually develop a regulatory framework on cybersecurity and could issue specific regulation directed to the private sector. These authorities are located within the Modernization Ministry and, so far, none of them have corrective powers but mainly collaboration tasks. These authorities include:

- the Undersecretariat of Technology and Cybersecurity ('the Undersecretariat'), is the main cybersecurity authority. The Undersecretariat aims to, among others, assist the Ministry in the development of a specific regulatory framework that would allow for the identification and the protection of the critical infrastructure of the national public sector, and of the civil organisations and private sector that require it, as outlined in Decree No. 898/2016 (only available in Spanish here);
- the Cybersecurity Committee, which has been assigned to, among other things, promote the enactment of a regulatory framework on cybersecurity and the drafting of an action plan in the implementation of the National Cybersecurity Strategy, in accordance with Decree No. 577/2017 (only available in Spanish here);
- the National Administration of Critical Information Infrastructure and Cybersecurity ('ICIC'), which aims to assist the public sector in all cybersecurity matters, protect the critical infrastructure, develop the public sector's abilities to detect, uphold, reply to and recover incidents, and to draft, in collaboration with the private sector, digital security policies, as outlined in Administrative Decision No. 232/2016 (only available in Spanish here). The ICIC depends on the Undersecretariat for Information and Cybersecurity's Critical Infrastructure Protection; and
- the National Office of Information Technology ('ONTI'), which has as its main responsibility to intervene in the drafting of policies and enactment of the development and technological innovation for the State's transformation and modernisation promoting the integration of new technologies, its compatibility and interoperability in accordance with the objectives and strategies defined in the State's Modernisation Plan, as established in Administrative Decision No. 232/2016.

Other administrative authorities that have issued regulations on cybersecurity which directly affect the private sector include:

- the AAPI, which, among other things, controls the fulfillment of the regulation on integrity and data security from data controllers (records, registers or data banks), requests information relating to backgrounds, documents, programmes or other elements related to personal data processing, and impos-

es administrative sanctions; and
- the BCRA, which, among other things, regulates the financial system, contributes to the proper functioning of the capital market, and imposes sanctions as established in Law No. 21.526 on Financial Entities (only available in Spanish here) ('the Financial Entities Law').

1.3. Regulatory authority guidance

There is no guidance from the regulatory authorities. However, on 28 May 2019, the Government Secretariat of Modernisation issued Resolution 829/2019 (only available in Spanish here), which provides the framework for the National Cybersecurity Strategy. Resolution 829/2019 states that the National Cybersecurity Strategy will direct the development of concrete actions, plans and politics for the benefit of the Argentinean Nation.

In particular, the National Cybersecurity Strategy is structured along the following objectives:

- awareness in the safe use of cyberspace;
- training and education on the safe use of cyberspace;
- development of a regulatory framework;
- strengthening of prevention, detection and answering abilities;
- protection and recovery of the public sector's information system;
- promotion of the cybersecurity industry;
- international cooperation; and
- protection of the infrastructure of national critical information.

The National Cybersecurity Strategy will be carried out by the Cybersecurity Committee, which shall ensure the safe use of cyberspace among the Public Administration, national, provincial or municipal authorities, private sector, non-governmental organisations and academic entities. It should be noted that Resolution 829/2019 also creates an executive unit within the Cybersecurity Committee that will coordinate the functioning of the National Cybersecurity Strategy and will provide administrative assistance to the Cybersecurity Committee.

2. SCOPE OF APPLICATION

2.1. Network and Information Systems

Sections 6 and 7 of the CBA's Ordinated Text of the Rules on Minimum Operational Requirements of the Area of Information Systems – Information Technology (only available in Spanish here) establishes the minimum requirements that an information system should comply with, for e.g. in relation to functional structure, methodological standards, and a specific informatic security policy.

2.2. Critical Information Infrastructure Operators

According to Section 1.3 of Communication 6375, critical or sensitive information must be protected to prevent its unauthorised use. Section 6.2.4 of Communication 6375 also indicates that all electronic devices that were functional for the storage of critical information and that are no longer used, must be physically destroyed before being shattered.

2.3. Operator of Essential Services

Not applicable.

2.4. Cloud Computing Services

According to Communication 6375, financial entities may hire cloud services. For that purpose, such suppliers must comply with general and specific security requirements listed under Section 7 of Communication 6375, such as implementing a 'unified access point' located in Argentina under each entity's administration, which would allow them to constantly control the activities undertaken by information technology services. It should be noted that all requirements are described within seven categories (each of them with a specific requirement chart), namely, information security government, training and awareness; access control; follow-up and integrity; control and monitoring; incident management; and operational continuity.

As for corporate documents, several rules have been issued to allow for the digitalisation of corporate and account books (i.e. Act 27.349 on Support for Entrepreneurship Capital (only available in Spanish here)). However, progress on digitalisation is withheld because of operating difficulties. Specifically, Section 53 of the General Inspection of Justice's ('IGJ') General Decision 6/2017 (only available in Spanish here) demands that:

- the server in which the corporate files are stored is located in the corporate headquarters in Argentina;
- the corporation save two copies of every digital file in two locations other than the corporate headquarters (at least one of them should be digital); and
- the corporation inform the IGJ of the location of the two copies and to keep this information updated. Evidently, the aforementioned criteria obstruct the possibility of hiring cloud services to store corporate documentation and to replace the traditional records.

Finally, regarding the health sector, Act 26.529 (only available in Spanish here) specifies that medical records may be drafted in magnetic support if certain measures are taken to ensure the preservation of their integrity, authenticity, unchangeability and durability, and the timely recoverability of storage data. Also, access should be restricted with identification keys or any other technique to ensure the integrity of the medical record.

2.5. Digital Service Providers

According to Act 25.690, internet service providers have the obligation to offer protection software to prevent access to specific sites at the time of supplying internet services, regardless of whether the contract was concluded by telephonic or written means.

In addition, the Digital Signature Act provides the framework for electronic and digital signatures, digital documents and their juridical efficiency. This was later complemented by Administrative Decision No. 927/2014 (only available in Spanish here) ('the Decision') and the Decision's annexes (only available in Spanish here), which set out, among other things, requirements for applicants of digital certifications relating to the content of digital certifications and operational and technological standards of the digital signature infrastructure. These requirements cover the following:

- the security plan, which includes security policies and proceedings and which must fulfil the guidelines of the International Organization for Standardization's ISO/IEC 27002;
- the cease of action plan;
- the business continuity plan, which includes a response to incidents and disaster recovery plan;
- the description of the technologic platform, which states that applicants must

enact proceedings that ensure reliability; and
- the lifecycle of the certifier's cryptographic keys, which provides that cryptographic keys must be created by the certifier, have a minimum of bits, and be created and stored in devices with security level 3 under FIPS PUB 140-2. Moreover, applicants must implement proceedings for recovering such keys, and provide a description of the tests made by qualified third parties on the security of the hardware and software component used.

2.6. Other

Not applicable.

---

3. REQUIREMENTS

3.1. Security measures

Communication 6354 establishes specific requirements for the performance of data processing, IT services and data outsourcing services. It establishes the need to frequently review and update the security policy and complementing documents in accordance with, among other things:

- the risk assessment and the complexity of the financial entity;
- the classification of information assets according to their criticality and sensitivity;
- the security strategy;
- access, identification, authentication and security standards;
- control and monitoring; and
- security records.

In addition, the Resolution provides non-binding recommendations on security measures for the treatment and processing of personal data in computerised means. These recommendations focus on tasks and specialties that data controllers may follow under a cybersecurity incident scenario, including:

- implementing a complaint process to allow users to alert security events;

- having a capable incident management system to show registration date, relevant documentation, people involved and assets affected;
- establishing responsibilities and procedures, such as developing a procedure for management in case of cybersecurity incidents and appointing a person responsible for the communication;
- preparing a report of the incident, which should be sent attached along with an incident notification to incidente.seguridad@aaip.gob.ar, with the following minimum content:
    - the nature of the breach;
    - categories of personal data affected;
    - identification of affected users;
    - measures taken by the person responsible to mitigate the incident; and
    - measures applied to avoid future incidents.

The Digital Signature Act defines the term 'technically reliable' as the quality of the set of computing equipment, software, communication and security protocols and the administrative proceedings related that fulfil the following requirements:

- safeguard against the possibility of intrusion and/or unauthorised use;
- ensure the availability, reliability, confidentiality and correct functioning;
- be fit for the performance of its specific functions;
- fulfil the appropriate rules of security, according to international standards in the matter; and
- fulfil the technical and auditing standard set by the application authority.

3.2. Notification of cybersecurity incidents

There is no general legal obligation to notify the regulatory authority.

As stated in section 3.1 of the note, according to recommendations of the Regulation, a cybersecurity incident should be reported to the AAIP with the following minimum content:

- the nature of the breach;
- categories of personal data affected;
- identification of affected users;

- measures taken by the person responsible to mitigate the incident; and
- measures applied to avoid future incidents.

This report must be attached with the incident notification to the AAIP to the following email address: incidente.seguridad@aaip.gob.ar.

Also, according to Section 3.1.5.1 of Communication 6357, the 'area of information asset protection' must register financial entities' incidents and weaknesses in security matters and be immediately informed through the proper information channels, with the purpose of analysing its causes and enforcing improvements on the information controls to prevent their future occurrence.

3.3. Registration with a regulatory authority

Registration with a regulatory authority is not required. However, the National Programme of Critical Information and Cybersecurity Infrastructures, created by Resolution 580/2011 (only available in Spanish here), and under the direction of ICIC, seeks, among other things, to collaborate with the private sector in drafting policies on safeguarding digital security, drafting annual briefs on the status of cybersecurity, and promoting awareness of the risks in digital media. It should be noted that this programme is not mandatory. Adherence to the programme is optional for the private sector through the submission of the adherence form, as approved by Provision 3/2011 (only available in Spanish here).

Likewise, after the enactment of this programme, a registry of security incident response teams was created by Provision 5/2015 (only available in Spanish here) in order to coordinate the actions of the informatic emergency response teams and to act as a repository for information on security incidents, tools, protection and defence techniques, standards and good practices. Even though registration is optional for the private sector, the programme establishes certain requirements that a corporation must fulfill in order to register, such as:

- delivering a certified copy of the corporate bylaws and of the act of appointment of the responsible person;
- delivering a 'constitution letter', based on the Internet Engineering Task Force's Request for Comments No. 2350, that provides information on the

computer security incident response team, the channels of communication, mission and responsibilities.

3.4. Appointment of a 'security' officer

According to Section 3.1.1 of Communication 6357, financial entities must consider within their organisational structure a specific area in charge of protecting its information assets, establishing the mechanisms for the administration and the security control over the logistical and physical access to their technological and information's resources. The person in charge of protecting information assets will manage the enactment and maintenance of the security policy established by the director or the equivalent authority of the entity.

Likewise, though it is only a recommendation, the Regulation, applicable to data controllers of databases and data processors, states the need to define a responsible person in charge of the fulfilment of the security measures.

Finally, it should be noted that a draft data protection bill (only available in Spanish here) ('the Bill') was submitted to the National Congress of Argentina on 19 September 2018. The Bill intends to fully replace the Act and to mirror the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), reflecting international standards and principles. Notable changes included in the Bill concern notifications of security incidents, the obligation to appoint a data protection officer in certain circumstances, protection by design and by default, data portability and opposition's rights. If the Bill were to be enacted, it would be enforced two years after its date of publication in the Official Gazette.

3.5. Other requirements

Not applicable.

---

4. PENALTIES

Currently, regulatory authorities that may apply administrative penalties for non-compliance with cybersecurity regulation are the AAIP (Sections 31 and 32 of the Act) and the BCRA (Section 47 of Law No. 24.144 on Organic Charter of the BCRA) (only available in

Spanish here), notwithstanding the criminal liability that could be applied in the specific case.

According to Section 31 of the Act, the AAIP may apply the following sanctions to data bank users and/or data processors:

- a warning;
- a suspension;
- fines of up to a maximum amount of ARS 100,000 (approx. €1,980); or
- closure of their archive, register or data bank.

As for the administrative penalties that BCRA can apply, these include (Article 41 of the Financial Entities Law):

- a warning;
- fines;
- temporary or permanent prohibition to use bank current accounts;
- temporary or permanent disqualification to act as a promotor, founder, director, manager, member of the supervisory board, syndicate, liquidator, auditor, partner or shareholder; and
- revocation of authorisation to operate.

ABOUT THE AUTHORS

Gustavo Bethular

RCTZZ

Gustavo Bethular is a Partner at Richards, Cardinal, Tützer, Zabala, Zaefferer SC ('RCTZZ'). As part of his practice, Gustavo advises companies from diverse sectors, including from the telecommunications, software, real estate, pharmaceutical, financial services and consultancy sectors. In addition, Gustavo has collaborated with companies in internal and judiciary investigations relating to, among other things, fraud, bribery, harassment, copyright infringement, child pornographhy, smuggling, forgery, hacking and bank fraud.

As an external advisor, Gustavo has been involved in the drafting and reviewing of bills on emails, privacy, network neutrality, cloud computing and informatic crimes. Gustavo has also offered trainings and lectures at several universities and public bodies on topics such as cybercrimes, forensic practices, copyright infringement and cloud computing.

bethular@rctzz.com.ar

RELATED CONTENT

NEWS POST

Russia: Minkomsvyaz announces study on security of IoT

LEGAL RESEARCH

Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No.526/2013 (Cybersecurity Act)

LEGAL RESEARCH

Insurance Markets: Benefits and Challenges Presented by Innovative Uses of Technology (7 June 2019)

NEWS POST

USA: GAO releases report on innovative uses of technology

NEWS POST

EU: Cybersecurity Act published in Official Journal