Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top-ranked lawyers

TMT

Argentina
Lisandro Frene, Juan Pablo M Cardinal and Damián Navarro
Richards, Cardinal, Tützer, Zabala & Zaefferer

chambers.com

2020

ARGENTINA

Law and Practice

Contributed by:
Lisandro Frene, Juan Pablo M Cardinal and Damián Navarro
***Richards, Cardinal, Tützer, Zabala & Zaefferer** see p.13*

Contents

Contributed by: Lisandro Frene, Juan Pablo M Cardinal and Damián Navarro
Richards, Cardinal, Tützer, Zabala & Zaefferer

1. Cloud Computing

Laws and Regulations

From 2016 onwards, cloud services started to be expressly addressed in certain regulations (particularly those concerning contracts with public entities) and implicitly acknowledged in regulations for specific industries within the private sector (ie, provision of IT services for financial entities, data outsourcing, data hosting and processing of personal data, etc).

Cloud computing agreements are standard practice in Argentina and are also admitted by Argentine legislation. In public sector contracts, cloud technology is expressly mentioned in the recent Cloud First regulations, which not only admit cloud technology but also state that such technologies are "reliable and cost-efficient" and that "cloud solutions shall be preferred by public sector entities before any other technological solutions" (ONTI Regulation 2/2018). Examples of such regulations are as follows.

- Regulation 2/2018 of the National Office of Information Technology, also known as ONTI, which recognises that "the use of the cloud allows for minimising maintenance costs and expenses, while providing scalability and reliability";
- Regulation 12/2017 of the Information Systems Agency of the Government of the City of Buenos Aires (which approved the Cloud Computing Regulatory Framework that shall be observed by all dependencies of the Executive Power of the City of Buenos Aires). Annex I expressly acknowledges "the possibility of processing data outside the government, even outside the national territory (as) a characteristic of cloud computing" and also recognises that "the implementation of the cloud has as its main objective to reduce infrastructure costs and provide flexible and measurable computing resources, as well as to minimise the costs of access to information, allowing to reduce unnecessary costs";
- Decree 875/2016 of the Province of Buenos Aires was the first Argentine regulation to mentioned "cloud computing" and the express possibility of hiring such service by the public sector.

Although the aforementioned regulations are applicable only to the public sector, they served to set the legal grounds for cloud services in the private sector on a massive scale. Indeed, within the private sector regulatory framework, while "the cloud" is not expressly accounted for as such, it is admitted in several regulations that allow and regulate transactions with the main features of cloud services. The most relevant example of this is probably Regulation 60/2016 issued by the Argentine Agency of Access to Public Information (AAPI), in charge of enforcing Argentine Personal Data Protection Act 25,326 (PDPA). Complementing Section 25 of the PDPA – which broadly acknowledges the provision of data processing services – Regulation AAPI 60/2016 provides a template agreement with model clauses for the provision of data processing services outside Argentina, in countries without "adequate legislation" in data protection. This provision is inherent and fully applicable to cloud services. Provided that the requirements of this legislation are met, no notification, permission or approval from the AAPI or any other authority is legally required for data outsourcing.

This framework – basic in the hiring of cloud services – was welcomed by almost all the industry, since it regulates international data transfers aligned with EU legislation (ie, EU Directive 87/2010) and, positively, it legislated for criteria that were previously contained in mere AAPI opinions, without the binding force of legal provision, providing certainty and legal security in this sector.

Furthermore, in November 2018 the AAPI issued Regulation 159/2018, which set forth Guidelines and Basic Contents of Binding Corporate Rules for the international transfer of personal data among companies of the same economic group. The guidelines attempt alignment with Section 47 of the GDPR, and establish (in a generic way) issues such as basic conditions for the legality of the transfer, procedures to ensure the data subjects' rights, joint liability of the parties, applicable jurisdiction in case of controversies and the AAPI auditing rights. These binding corporate rules appear as an option to the model clauses set forth by AAPI Regulation 60/2016 for the international transfer of personal data.

Specific Industries with Greater Regulation

In addition to the aforementioned data protection requirements, other industry-specific requirements are applicable for international data transfer in certain areas, such as the financial sector, social security, health, and corporate sector.

Financial sector

In regard to the financial sector, data was requested to be maintained in-country until November 2017, when the Argentine Central Bank issued Communication A 6354, as amended by Communication A 6375, allowing banks to hire cloud services and data outsourcing abroad, as long as the many requirements therein established are complied with by both the Argentine financial institution and the foreign data processor (ie, cloud provider).

Pursuant to the aforementioned regulation, financial institutions intending to perform international data transfer and outsourcing activities shall notify this through a communication to the Financial Institutions Bureau (*Secretaría de Entidades*

Financieras y Cambiarias) at least 60 days before initiating such activities, including in such communication certain mandatory information and a copy of the outsourcing agreement in pdf format. The obligation to comply with the terms of this regulation shall be expressly indicated in the agreement between the financial institution and the foreign outsourcing services/IT provider. Furthermore, foreign data processors providing services to Argentine financial institutions shall perform internal audits every year, considering in such audit the compliance with this new regulation; they should also submit a copy of the audit to the External Audit Unit of the Argentine Financial Institutions Bureau, which is a subdivision of the Argentine Central Bank.

The aforementioned regulation requires the cloud services provider to address different "scenarios of IT services", classified according to the kind of data to be transferred to the IT provider and the risk thereof derived, and imposes several "technical and operative requirements" for each scenario, with which both the financial institution and the IT/cloud provider shall comply.

Social security
In November 2018, Argentina's Social Security National Administration (ANSES) issued Regulation 204/2018 and approved a Personal Data Protection Policy applicable to all the data collected by ANSES, saved in its databases. In this regard, Section 10 of its Exhibit I determines: "the personal data processed by the ANSES is stored on its own servers, located within the territory of the Argentine Republic. ANSES does not perform international data transfer, nor does it hire data hosting services from third parties, with the exception of the database related to the evaluation of the performance of its personnel that is hosted on servers located in Spain, a country that provides an adequate level of protection in terms of current regulations." The aforementioned provision restricts the possibility of ANSES using cloud services, which necessarily implies international data transfer. Furthermore, such provision contradicts other provisions of the Argentine legal framework regulating personal data processing.

Health
Argentine Medical Records Act 26,529 allows clinical records to be computerised. In this regard, Section 13 provides: "the content of the medical record can be made in digital format, provided that all means are arbitrated so that the integrity, authenticity, inalterability, durability and recoverability of the data contained therein, is well preserved. To that end, the use of restricted access, with identification passwords and non-rewritable storage media, control of field modification or any other appropriate technique to ensure its integrity shall be adopted".

Corporate
Argentine Companies Act 19,550, through its Section 61 – amended by Act 27.444 of June 2018 – allows companies to keep their corporate and accounting books by digital means, as in the case of the simplified corporations. This provision, however, encounters an important operational obstacle with the provisions of Regulation 6/2017 of the Public Registry, in that its Section 53 determines that the server where the digital files are hosted must be kept at the company's registered offices, thereby precluding the outsourcing of cloud computing services from providers. This legal obstacle is expected to be overcome in the near future, hopefully in 2020. Notwithstanding this, on October 2019 the National Securities Commission issued Regulation 813/2019 whereby it extended the permission of digital bookkeeping to companies authorised for public offering, under the surveillance of the Commission.

2. Blockchain

Risk and Liability
Blockchain is neither regulated in Argentina, nor is there case law specifically addressing this particular technology. Thus, legal challenges related to blockchain are so far considering general legal principles and the specific restrictions of the industry or area of law where blockchain is applied. Legal issues such as risk and liability, intellectual property, data privacy, service level and jurisdiction shall be analysed under the aforementioned approach.

While the adoption of blockchain in the private sector is booming, at a federal level, government is promoting public/private consortia to foster usage of blockchain, with federal government taking the lead in co-ordinating efforts among governmental agencies, trade associations and private parties.

Among the main risks and liability, the following shall be considered.

- Firstly, risks relating to security and confidentiality are probably among the main contingencies that potential blockchain users should think about. In Argentina, both of these features are mandatory for the data processor under PDPA. In spite of the decentralised nature of its nodes, as with any other IT system, blockchain systems may suffer hackers' attacks (in fact, 51% of public blockchains have suffered attacks). Such attacks may trigger blockchain vendors and/or managers' liability – especially in permissioned blockchains – both from the contractual law perspective and derived from breach of the aforementioned security duties under the PDPA.

- Secondly, determining who shall be held liable, and against which party a claim shall be made, is another important legal challenge to consider, particularly in a non-permissioned blockchain, where all participants have similar rights. The question might vary in a permissioned blockchain, but still it remains uncertain whether the "super user" or manager of the system could be considered liable for any malfunctioning, security breaches and other damages or participants' claims.

"Smart contracts" is another non-regulated area, where the general principles of law will come into play to resolve implementation issues. Nevertheless, issues such as enforceability, and the binding nature or procedural recognition as evidence are yet to be discussed. As in many other jurisdictions, it is likely that theories and/or solutions applicable to software programming, etc, will come into play.

Intellectual Property

Ownership of the intellectual property of all or part of a blockchain environment is a key factor to be considered by blockchain vendors. This ownership may include the software and business processes, the developments added after its release and the underlying data. In addition, queries should be raised about whether such personal data may be considered IP or even "property" at all, and whether vendors may claim ownership over it, where such personal data belongs to users (even with pseudonymisation).

In spite of the novelty of blockchain, some of these IP issues have arisen already with existing software platforms and/or shared software systems.

Data Privacy

Data privacy is a crucial issue in the use of blockchain technology, especially in a country such as Argentina, which follows the European Union in data protection legislation; the current PDPA was based on the former EU Directive 95/46, and the bill to replace the PDPA is intended to be aligned with the GDPR.

The question of who shall be considered the personal data controller – especially in a non-permissioned blockchain – and the one responsible for complying with the PDPA, and for granting data subject's rights (ie, ARCO rights) and other personal data regulations is a key factor. In a permissioned blockchain – limiting who can join the blockchain network to "trusted" nodes and encrypting the data on the blockchain – the super-user may be considered the data controller, with the liabilities therein attributable. However, none of these matters have yet been addressed by Argentine law or case law.

Another potential issue from a data privacy perspective is to consider the consequences of the user's decision to stop using the service under blockchain when he or she does not hold a copy of the data on the ledger. For such cases, there needs to be provisions and processes in place that ensure the vendor hands over all the data subject's (user's) information and a complete record of all the transactions on the blockchain that are linked to the user's name.

Security issues prescribed by Argentine data protection law should also be analysed under a balanced "privacy versus transparency" approach, especially considering such data protection security provision as set forth by sections 9 and 10 of the PDPA, and also AAPI Regulation 47/2018. The fact that in a public blockchain system anyone can access any data subject's personal data, especially health and/or other sensitive data, poses serious privacy challenges, under both the PDPA and the Argentine Medical Records and Patient's Right Act 25,629. In turn, compliance with security measures within the financial service industry is particularly delicate, as this industry has specific recent and detailed security legal requirements that need to be complied with (ie, BCRA Communication 6375).

Service Levels

From a service level perspective, the challenge is likely to be striking a proper balance between the provider's adherence to standard contracts with limited warranties and liabilities on one side, and the customers' unwillingness to agree to such restrictions on the other. In addition to this type of contractual negotiation – typical of the IT industry – other legal restrictions need to be considered, such as those imposed by mandatory laws that may be applicable. In Argentina, this concerns the Consumers Defence Act 24,240, the PDPA 25,326 and the Medical Records and Patients' Act 26,529, all of which grant rights that cannot be waived by the parties involved.

Jurisdictional Issues

Being a decentralised system in which nodes exist around the planet, determining the correct set of rules to apply in a controversy constitutes a key legal challenge for blockchain. As a matter of fact, disputes derived from blockchain transactions might potentially arise in the jurisdiction(s) of the country of each node in the chain. This circumstance faces blockchain layers with the challenge of needing to comply with many different legal regimes simultaneously. In the event that a fraudulent or erroneous transaction is made, pinpointing its location within the blockchain could be challenging.

In the absence of contractual provisions, the Supreme Court of Argentina case law calls for asserting Argentine jurisdictions whether or not there is performance, of any materiality or kind, in Argentina (CSJN, 20/10/98, Exportadora Buenos Aires S.A.

c. Holiday Inn's Worldwide Inc. Fallos 321:2894), for which setting up proper jurisdiction clauses will be a must, and will clearly help to provide users with legal certainty about which laws and courts should be applicable in a controversy derived from blockchain transactions.

However, this may be challenging with multiple customers' transactions – the essence of a decentralised environment like blockchain – when certain local "public order" regulations are mandatory. In Argentina, this is the case with the Consumers Defence Act 24,240, the PDPA 25,326 and the Medical Records and Patients' Act 26,529, all of which grant rights that cannot be waived by the parties involved, including mandatory local (Argentine) jurisdiction and applicable law.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

Big Data

Modern technological concepts such as "big data", "artificial intelligence" (AI) and "machine learning" have scarcely been mentioned in recent Argentine legislation, and none of them have been regulated as such. Thus, assessment and counselling about these topics is so far provided for based on general principles of law – in particular, tort law and contractual, IP and privacy regulations.

In respect of big data, in 2017, Regulation 11/2017 created the Big Data Observatory, an entity within the IT & Communications Bureau. Although its specific tasks are to be defined by further regulation, it aims to "study the regulatory framework of personal data use", "foster and create big data technological platforms", "promote good big data practices" and "propose for new regulations". As of January 2020, Regulation 11/2017 remains without further regulations and none of the aforementioned regulatory frameworks have been passed.

Furthermore, internet service providers (ISPs) are key actors in the processing of big data and, to date, their liability is still unregulated, in spite of several bills on the matter. While the generic right of access and deletion of incorrect data is addressed in the PDPA, there are neither takedown nor counter-notice/respond legal proceedings. This question is currently de facto regulated pursuant to case law precedents.

In recent years, hundreds of cases have been brought to courts against search engines and/or social media providers where plaintiffs request their data to be erased or blocked, based on "revenge porn", disinformation, hate speech, slander, non-authorised use of image, privacy, etc. In the absence of legislation, each controversy is decided on a case-by-case basis, according to Federal Supreme Court guidelines. Based on such case law, a bill (S-1865/2015) on ISP liability is being considered in Congress with a view to enforcing a negligence system (as opposed to strict liability) on ISPs. If enacted, this bill would be the first regulation concerning ISP liability and, in general terms, would limit such liability.

Without specific legislation currently in place, ISPs' duties and liabilities with regard to processing big data is judged based on tort principles (the Civil and Commercial Code) and privacy law (PDPA), including matters such as database ownership, purpose and final usage (ie, misuse) of analytics made with big data, treatment of sensitive data, etc.

More advanced issues are yet to be seen. Examples of insurance derived from improper processing of big data – or claims derived thereof – are currently rarely available or very expensive to access.

Machine Learning

In the absence of legislation regarding machine learning and artificial intelligence, there is legal uncertainty in Argentina about these matters.

In terms of artificial intelligence, relevant elements include liability and insurance, data protection, intellectual property, jurisdiction, and even fundamental rights.

It is worth noting that, in November 2018, Decree 996/2018 was issued, by which the Argentine federal government set forth the basis for an Argentine Digital Agenda (Agenda Digital Argentina) aiming to establish guidelines for a technological legal framework and digital institutional strategy to be implemented throughout the country. These guidelines mention artificial intelligence as well as other technological concepts such as cybersecurity, "digital inclusion", access to IT services, biotechnology, "digital government", e-commerce and technological neutrality, among many others. Given the terms of the Decree, its broad guidelines and potential scope, further specific regulations accompanying it were expected. In this context, the Secretariat of Modernisation of the Chief of Cabinets, by Regulation 5/2019 of January 2019, created Argentina's Digital Agenda Unit, with the aim of "accelerating the digital transformation of the country"; the unit shall be dissolved once its aim is fulfilled, whatever takes place before.

In both cases – machine learning and artificial intelligence – IT systems' capacity to make autonomous decisions seems to pose the greatest potential impact in terms of liability. Application of causation principles and determining who shall be considered liable for the fault that causes damages seems a crucial legal

challenge, particularly if a negligence regime (as opposed to strict liability) is applied.

In response to the main legal challenges, when managing a project involving big data, machine learning or artificial intelligence, cybersecurity is a key legal consideration to consider. In this regard, the AAIP Regulation 47/2018 sets a series of "recommended" – ie, not mandatory – security measures for the processing of personal data.

Also, and throughout 2019, further regulations regarding cybersecurity have been issued by the government. In particular: the Federal Government adopted the National Strategy of Cybersecurity – enacted by Regulation 819/2019 of 28 May 2019, by the Secretariat of Modernisation of the Chief of Cabinet of Ministers – guaranteeing an adequate level of cybersecurity on IT systems within the public sector.

Additionally, on 4 November 2019, the National Ministry of Security approved – by Regulation 977/2019 – a Federal Plan of Prevention of Technological Crimes (2019-2023), aiming to establish by 2023 qualified personnel, technology and the necessary regulation to fight against the execution of crimes through means of TIC within the National Territory, and to become aware of the national metrics (ie, to have an accurate measure of the quantity and conditions of the execution of such type of crimes at a national scale). Lastly, the Ministry of Human Rights and Justice approved the creation of a Cybercrimes and Digital Evidence Unit through the issuance of Regulation 1291/2019 of 27 November 2019, this in order to provide member states and officials of the local criminal system with round-the-clock assistance in computer-related crimes.

However, for now, such measures are applicable only within the public sector, not the private sector.

4. Legal Considerations for Internet of Things Projects

Regarding the "Internet of Things" (IoT), in April 2017 the Secretariat of Information and Communication Technology issued Regulation 7-E/2017, calling interested parties to submit opinions, proposals and needs of different players and sectors involved in the development of the IoT, pursuant to a pre-established administrative proceeding. This regulation was issued within the framework of Regulation 8/2016, which created the Internet Services Workgroup with the purpose of "analysing and promoting public policies to develop internet services" and, in particular, to "promote development of the Internet of Things, specifically for the development of public policies related to security, public health and environmental matters".

Decree 996/2018, by which the Argentine Federal Government sets forth the basis for an Argentine Digital Agenda (Agenda Digital Argentina), also mentions the IoT – in addition to many other IT concepts – among the guidelines for a technological legal framework and digital institutional strategy to be implemented in Argentina. In spite of all these legal references, as of January 2019 none of the expected regulations had been enacted and the IoT remains without specific regulation.

In the current legal scenario, when contemplating a project with connected devices in Argentina, analysing it from a data protection perspective is of the essence. The PDPA and Regulations AAPI 60/2016 (regarding international transfer of personal data) and 47/2018 (regarding data security measures) are crucial pieces of legislation, as well as other cloud legal considerations referred to earlier.

It is worth considering that the bill that aims to replace the PDPA in its entirety, in order to update it and align it with international standards and principles established by the EU General Data Protection Regulation (ie, GDPR), includes privacy by design and privacy by default sections almost identical to those in the GDPR. If the bill is finally enacted, they shall be considered in the implementation of IoT projects.

5. Challenges with IT Service Agreements

Entering into an IT Service Agreement with a Local Organisation

IT service agreements are not specifically regulated as such in Argentine law. Articles 1251 to 1279 of the Civil and Commercial Code regulates services agreements, but refer to general services and not particularly to IT services. The general regulation applicable to all private contracts applies; this is as provided for, primarily, in articles 957 to 1122. Among those, Article 958 refers to the freedom of contract or party autonomy, which governs the relation between the parties, although that freedom may be restricted by different mandatory provisions.

While it is not yet clear, as the new Civil and Commercial Code only came into effect in 2015, outsourcing contracts may be impacted, as this may be considered as a "supply agreement" and therefore certain provisions may come into play, such as a maximum term (20 years), as in the absence of a contractual stipulation, provision of services are to be considered to fulfil clients' needs. A first-refusal right may also come into play, as provided by the Civil and Commercial Code, as well as certain restrictions for the unilateral termination of long-term agreements.

The legal aspects to be considered when drafting and negotiating an IT service agreement in Argentine are: changes to services and price, complying with regulation that governs the parties (eg, banking regulation), intellectual property rights, data privacy, limitation of liability, etc. The regulation of these aspects is quite similar to the regulation applicable in the majority of the civil law and common law main jurisdiction.

However, some legal aspects that have to be taken into account are regulated in Argentina in a different way than other main jurisdictions, including the following: price adjustment provision, currency, labour law, choice of law and pre-formulated or boilerplate contracts. These aspects will be addressed below.

Relevant Rules or Mandatory Laws

Price adjustment

Although high inflation has beset Argentina over the years, price adjustment due to inflation is forbidden (Act 23,928). This prohibition has been somewhat repealed or at least mitigated in some transactions or operations (eg, loans secured by mortgages granted by banks), but it is still in force in private contracts. However, despite the prohibition, price adjustment clauses are usually included in private agreements, at least when price is fixed in local currency; the adjustment mechanism should be carefully crafted to try to prevent it from falling within the prohibition.

Currency

In the scope of Article 958 of the Civil and Commercial Code (freedom of contract or party autonomy), the parties to an agreement may freely set the terms of the contract, which includes the currency. Thus, they can fix the price in the local currency (Argentine pesos) or a foreign currency (probably US dollars). However, according to Article 765 of the Civil and Commercial Code, even if the price is fixed in a foreign currency, debtors may cancel the debt by paying with Argentine pesos. Collecting payment in this currency may be uneconomic if the government, as it has done in the past, sets exchange control mechanisms (eg, a foreign exchange deadlock) which leads to an official foreign exchange rate artificially lower than other unofficial rates that reflect the real market value of the currency.

Although it is debatable whether or not aforementioned Article 765 is a public order provision, most of the case law has considered it is not and that thus the parties to a contract may freely agree that Article 765 does not apply, and that the debtor shall cancel the debt in a foreign currency.

FX restrictions

Since September 2019, Argentine's Executive Power and, mainly, the Argentine Central bank has issued a series of regulations that may hinder the acquisition of foreign currency and payment/submission to entities outside Argentina (ie, an IT provider located outside abroad). Presidential Decree 609/2019 and Argentine Central Bank communications 6770, 6787, 6815 and others set out foreign exchange controls pursuant to which some of the aforementioned payments and submissions of monies to foreign entities require previous authorisation from the Argentine Central Bank.

Labour law

According to Article 30 of the Argentine Employment Contract Act 20,744, a company (client) that hires a provider to render services related to the company's business (eg, outsourcing of payroll) may be considered jointly liable with the provider for the fulfilment of the provider's employment and social security obligations with respect to the employees involved in the services. This risk is usually addressed with labour indemnity provisions in the service agreement and, ideally, with the client controlling that the provider complies with its labour obligations with respect to its personnel (eg, that it is duly registered, that salaries and social security obligations are duly paid, etc).

Choice of law

Under Argentine Private International Law (conflict of laws), if the contract cannot be characterised as an "international contract" (eg, because both parties are Argentine companies, or the contract is mainly performed in Argentina, etc), the parties may not choose a foreign law to govern their agreement. Only in international contracts may the parties (under Argentine private international law) freely choose the applicable law. In addition, under the same Argentine Private International Law, if the contract is not international, arbitration can only take place in Argentina (designating Argentina, most likely Buenos Aires, as the seat). Arbitration is common as a dispute resolution alternative in Argentina.

Boilerplate or pre-formulated contracts

Articles 984 to 989 of the Civil and Commercial Code provide for the regulation for boilerplate or pre-formulated standard contracts, which are contracts – different from consumer contracts – in which one party agrees to general provisions drafted by the other party without having participated in the drafting. This regime includes some interpretative rules against the party who has drafted the agreement that need to be considered (eg, the clauses that alter or distort the obligations of the party which has drafted the agreement are void). They should be taken into account considering that many contracts are executed using these types of agreements.

Personal data

Regarding data storage locations and other personal data protection regulations that may (and generally will) impact provi-

sion of IT services, please refer to sections **1. Cloud Computing** and **6. Key Data Protection Principles**.

Knowledge Economy Promotion Regime
Additionally, the Executive issued Decree No 708/2019, which regulates the Knowledge Economy Promotion Regime created by Law No 27.506 providing substantial tax and labour law benefits to entities using and/or providing IT services, as required by the law. Such benefits include fiscal stability, detraction from employers' social contributions in regard to employees, transferable tax credit bond, reduction on income tax rate, exclusion of withholding and/or collection VAT regime. The benefits apply to a wide range of broadly defined IT activities.

To gain the aforementioned benefits, registration is mandatory and shall be filed before the National Register of Beneficiaries of the Knowledge Economy Promotion Regime, which will operate within the scope of the National Directorate for Knowledge-Based Services which comes under the jurisdiction of the Secretary of Small and Medium Enterprise Entrepreneurs. However, through Regulation 30/20 of the Ministry of Productive Development, the new federal government recently suspended – for an indefinite term – said registration, for which the benefits of this Regime are currently de facto suspended. Meanwhile, the newly elected President submitted to Congress a new bill aiming to substantially amend the Knowledge Economy Promotion Regime. Said bill is still in Congress and it is still to be seen, if it is enacted, the scope of the aforementioned amendment, including when and how the Regime will come into force again.

6. Key Data Protection Principles

Core Rules Regarding Data Protection
Processing of some sort of personal data is involved in almost all TMT projects, therefore knowing the applicable data protection regime is crucial for a solid legal assessment.

In Argentina, Personal Data Protection is acknowledged in the National Constitution and in the Argentine National Civil and Commercial Code (Section 1770); it is regulated at a federal level by Argentine Data Protection Act No 25,326 (PDPA) and by more than 70 regulations issued by the Argentine Agency of Access to Public Information (AAPI), in charge of enforcing the PDPA, pursuant to presidential decrees 899/2017 and 746/2017. The AAPI – which replaced the former Argentine Data Protection Authority (*Dirección Nacional de Protección de Datos Personales*) – is an autonomous public entity recently created within the National Chief of Cabinet (the highest authority of the National Government Ministries).

In December 2018, Argentina adhered to the Council of Europe 1981 Convention of Individuals with Regard to Automatic Processing of Personal Data, incorporated into local law by Act No 27.483, the first binding international instrument for member states in protection of fundamental freedoms, and in particular the right to respect for privacy.

Other more specific data protection-related laws and sectoral regulations are also applicable, such as: regulations about an individual's rights to his or her own image and voice (Act 11,723, Section 31, and Argentine Civil and Commercial Code, Section 53); the right to intimacy (Argentine Civil and Commercial Code, Section 52); health data and consent for medical treatment (Argentine Civil and Commercial Code, Section 52, and Argentine Medical Records and Patient's Right Act 25,629, as amended by Act 26,742); financial entities' data treatment (Argentina Central Bank issued Communication A 6354), etc.

The PDPA is mandatory legislation applicable to data treatment of Argentine residents, regardless of where such treatment is performed. PDPA rights cannot be waived by data subjects, as it is considered a "public order" law.

On 19 September 2018, the Executive Branch submitted to the National Congress a bill that aims to replace the PDPA in its entirety in order to update it and align it with international standards and principles established by the EU General Data Protection Regulation (GDPR). Among the many provisions established by the draft are regulated issues such as: extraterritoriality, notifications of security incidents, new rights such as data portability and opposition, protection by design and by default, risk impact assessments and the obligation to appoint a Data Protection Officer in certain circumstances. If enacted, the same would come into force after two years of its publication in the *Official Gazette*. During this period, the current PDPA regulations would remain in force.

Distinction Between Companies/Individuals
Under the PDPA, so far there is no distinction made between companies and individuals, as the rights granted therein are applicable to the personal data of individuals and legal entities.

It should be noted that the bill that aims to replace the PDPA in its entirety in order to update it and align it with international standards and principles established by the EU GDPR only protects personal data of individuals (aligned with the GDPR in this aspect). So, if the bill is finally enacted, companies' data will be excluded from the Argentine personal data protection legal regime.

General Processing of Data

Data subjects' consent requirement for data collection and/ or treatment is one of the key principles of the PDPA. Furthermore, data subjects' right to access to data and right to correct or erase data has been a constitutional right since 1994; the habeas data proceeding to exercise such right are incorporated in the PDPA.

An exception to the data subject's consent requirement takes place when a data processor receives databases from a data controller for the sole purpose of providing processing services to a data controller, acting on behalf of the latter. The data processor and its duties are regulated in Section 25 of PDPA.

If the data processor is located outside Argentina (ie, data outsourcing, provision of cloud services, etc), the Argentine data controller/exporter and the foreign data processor/importer shall execute a written agreement to provide such services. The requirements of such data transfer agreement depend on whether or not the legislation of the country of the data processor (data importer) provides "adequate levels of data protection".

In case of data transfer to countries whose laws do not provide "adequate data protection", such as the USA, the Argentine entity (data exporter) and the foreign data processor (data importer) shall execute a Data Transfer Agreement pursuant to the template set forth by AAPI Regulation 60/2016. Please refer to **1. Cloud Computing** for further information on data processing and specific industries' data protection regulation.

7. Monitoring and Limiting of Employee Use of Computer Resources

Argentine law establishes certain generic restrictions on monitoring and limiting use by employees of company computer resources. Indeed, workplace privacy has been an increasingly hot topic in recent years in Argentina, mainly due to the advancement of technologies and its impact on data protection. According to Argentine Employment Contract Act 20,744, the employer has the power to exercise personal control on employees within certain limits that safeguard the workers' dignity and privacy (sections 65, 70, 71 and 72). Such standards are not precisely defined and are analysed by courts on a case-by-case basis, aligned with other labour legislation (which is very protective of employees' rights) and the PDPA principles.

As a rule, employees shall give prior consent (preferably in writing) acknowledging that their data may be collected by an employer by way of monitoring their workplace communications. In other words, the basic principle sustained by case law – mainly labour courts – is that the employer cannot access the emails and/or IT files of his or her employee except where the latter has previously authorised it. In practice, this is typically – and validly, according to case law – performed through an employer's privacy policy that (sometimes together with other policies and/or conduct guidelines) the employee is invited to sign when taking up a position. Among other terms, such policy shall state that IT resources shall be used for working purposes only (not for personal or private matters), and that the employer shall have the right to access their content.

Regarding workplace video surveillance, case law has established that the company must notify where the cameras are located, what type of models they are, and whether they can record audio or not; it has been decided that the sound or voice recording is much more intrusive and therefore has greater complications when it is used as evidence at court. Video cameras should not be located in places that disturb the employee's privacy and/or intimacy and/or psychological integrity. Argentine labour courts have consistently rejected certain video-recorded evidence in cases where the cameras were located in staff toilets and/or places where some employee privacy and intimacy is expected.

In addition, video surveillance is considered a data collection proceeding specifically regulated by the AAPI (Regulation 10/2015). Apart from registering the video surveillance database before the National Databases Registry, companies undertaking video surveillance shall have a privacy handbook containing certain mandatory information such as references to places, dates and hours in which surveillance cameras will operate. The collection of any images shall be limited to the security reasons stated, without interfering with the privacy and/or intimacy of data owners. Letters shall be exhibited to the public and to workers expressly indicating: the existence of video cameras, the purpose for video surveillance, the company responsible for the images/data treatment, its domicile and the way in which data subjects may contact such company to exercise their basic rights.

8. Scope of Telecommunications Regime

In Argentina, telecommunication is the emission, transmission or reception of signs, signals, data, images, voice, sounds or information of any kind, by wire, radio, optical or other electromagnetic systems (Act 27.078). The purpose of Act 27.078 is to state as a public interest activity the development and regulation of information technology and communications and associated resources, establishing and ensuring complete network neutrality. The aim is to guarantee the human right to communication,

giving access to information and communication to all residents in social and equitable geographical conditions.

Many technologies are currently deemed to fall within the scope of local telecommunications rules, for example: voice-over IP is, according to the enforcement authority (National Authority for Communications or ENACOM), a "value-added service"; and RFID tags – it is required that a band or channel of frequency be assigned by ENACOM, as a radio frequency system requires prior authorisation. Other technologies do not fall within the scope of telecommunications, such as instant messaging or online video channels, because the providers do not operate a network nor lease network space, which are necessary for its proper working; instead, they use the internet service offered to the user by another supplier.

The government has defined a programme for the telecom sector with certain priorities:

- to build a modern high-speed broadband infrastructure;
- to develop 5G mobile network quality;
- to develop a modern framework for the digital era;
- to stimulate demand for advanced services; and
- to eliminate Argentina's digital gap.

According to Act 27.078, a unique licence is required to provide a telecommunication service, either fixed or mobile, wired or wireless, national or international, with or without its own infrastructure. Telecommunication services may only be provided after a licence has been granted, in respect of the specific services covered by that licence.

The unique licence has a nationwide scope and there are no mandatory investment obligations; providers are free to choose the technology and network architecture that they consider the most appropriate for the efficient provision of services. The licence does not include the award of a spectrum, which is subject to a separate procedure.

The procedure to obtain the unique licence is established by the Licensing Regulation for Information and Communication Technology Services issued by the Ministry of Modernisation (Resolution No 697/2017). There are no restrictions for the granting of the unique licence to natural persons or juridical entities. Applications must include personal and corporate documentation, information on the services to be provided, and financial statements. The main aspects of the procedure are as follows.

Resolution No 697/2017, rules for the payment of ARS20,000 as tariff; online registration forms including address, legal capacity and other information about the company; the submission of a sworn statement regarding the compliance of regulations and technical specifications related to the information and communications technologies services to be rendered; the unique licence has no expiry date; there are no restrictions on foreign investments in the telecommunications market, other than those established by Act No 25,750 (Media Ownership Act) for providers of internet access services.

Also, all telecommunications service providers are required to grant interconnection to other telecommunications service providers on a non-discriminatory, transparent and proportional basis, based on objective criteria. The parties may agree on the specific interconnection terms and conditions.

Furthermore, the transfer of licences and the controlling stock of operators are subject to regulatory approval.

The ENACOM approval may be granted explicit or deemed approval if ENACOM does not make any official observation within the 60 days after the filing of the petition. Once the licence is granted, the solicitor must register the services to provide. Also, the provider must pay:

- as monitoring and controlling charge, a fee of 0.50% of the total revenues earned from the provision of the services, net of taxes, interconnection costs and duties (except for this control fee);
- the contribution for the Fiduciary Fund of Universal Service, equivalent to 1% of the total income from the services;
- if it applies, the radio electrical duties and fees for each radio electrical station, system and service which operates throughout Argentina;
- the administrative fees that the enforcement authority is allowed to establish;
- the charges according to Act 26.522, considering the amount of gross invoicing.

The Quality Regulation of Information Technology and Communications Services (Resolution No 580/2018) establishes the standard of quality and procedure to apply sanctions.

9. Audio-Visual Services and Video Channels

According to Act 26.522 (Audiovisual Communication Services Act), Act 27.078 (Argentina Digital Act), Decree 267/2015 and Decree 1340/2016, all services of information and communication technology, and audiovisual services, must be treated in the same way, regardless of the kind of technology used. Audiovisual communications services are an activity of public interest

and regulations include those for advertising agencies, content producers and channels (tv, radio).

To provide audiovisual services, a formal licence granted by ENACOM with annual updates is required. The procedure is established by the Licensing Regulation for information and Communication Technology Services issued by the Ministry of Modernisation (Resolution No 697/2017), as stated in **8. Scope of Telecommunications Regime**.

Once the licence is granted, the provider must register the services with the Public Register of Licences and Authorisations for Audiovisual Communication Services (Resolution No 1502-AFSCA/14). Also, the provider must be registered with the Public Information System of Audiovisual Communication Services Suppliers.

In relation to online video channels or any other OTT services, they are not specifically regulated and there is no licence requisite, except tax obligations (according to Decree 354/2018, OTT services are subject to Value Added Tax). OTT services are not expressly included in the concept of telecommunications because the OTT services provider does not operate by itself a network nor leases network space, and the regulator has not expressly established any requirement.

10. Encryption Requirements

Currently there is no legislation establishing a generic obligation to use encryption technology. However, there are specific cases – particular industries, sectors and/or circumstances – in which the use of encrypted or encrypted is mandatory or recommended (eg, the public sector, financial sector, health sector, etc).

Regulation AAPI 47/2018, which sets forth recommended (non-binding) security measures for all kind of personal data processing, recommends the use of encryption technology for the process and/or hosting of "sensitive" data (data revealing religious, sexual, political, racial, ethnic, moral or philosophical preferences, as well as health data and criminal records).

In the public sector, Regulation 1/2015 of the National Office of Information Technologies (ONTI) establishes the cases in which cryptographic controls should be used for governmental entities – ie, for the protection of access codes to systems, data and services, for the transmission of classified information outside the scope of the organisation, for the protection of information when this arises from the risk assessment carried out by the IT manager, etc.

In the financial industry, several regulations issued by the Argentine Central Bank (applicable only to financial entities) set certain encryption requirements and minimum-security standards (including detailed technical measures) for management, implementation and risk control regarding the provision of IT services to financial entities. In particular, Communication A 6354, as amended by Communication 6375 (allowing banks to hire cloud services and data outsourcing abroad, as long as the many requirements therein established are complied with by both the Argentine financial institution and the foreign data processor/cloud provider) requires "mechanisms for encryption of data and communication channels". Furthermore, among the Technical Operating Requirements for Integrity and Logging, such regulation mandates that IT providers "shall formulate an encryption policy for data at rest, in transit or in both statuses including an allocation of responsibility for all controls defined in each data status".

Among the public offering regime, Regulation 704-E/2017 of the National Securities Commission, applicable only to listed companies and capital market agencies, stipulates that the storage and transmission of authentication data shall be protected through internationally recognised cryptographic algorithms. In addition, it establishes encryption requirements for other situations (ie, when the information goes beyond the limits of local networks and cross-public networks).

With respect to health data, Act 26,529 (Argentine Medical Records and Patients' Right Act) states that for such data "the use of restricted access shall be adopted with identification keys, non-rewritable storage means, control of modification of fields or any other suitable technique to ensure their integrity".

Finally, the implementation of "digital signature", pursuant to Act 25,506, Regulation 399-E/2016 of the Ministry of Modernisation – further regulated by Decree 182/2019 – establishes cryptographic requirements among the Single Certification Policy such that all digital signature certifiers shall apply for the issuance of the digital signature certificate.

In relation to telecoms operators, there are no specific regulations or restrictions on encryption of communications.

Richards, Cardinal, Tützer, Zabala & Zaefferer has a TMT team comprising three partners, four senior lawyers, four junior lawyers and three paralegals. The team works with lawyers from other areas within the firm, mainly in the following TMT-related matters: outsourcing agreements, international data transfers, cloud computing services agreements, data protection regulation in the provision of telecommunications, over-the-top and IT services, telecommunication regulatory framework, TMT governmental licences and permits for the provision of telecommunication services, telecommunications infrastructure projects, advertising through different media, IT regulation and analysis for industries such as financial, health and agribusiness, legal review of software and applications development, mandatory security and technical requirements for data hosting and processing, data security incidents management, IT law assessment in public sector contracts, and antitrust law matters in the provision of telecommunication services. The firm has 17 years' experience of TMT practice and its clients include Microsoft, Accenture, Mercedes-Benz and Fox. Located in Buenos Aires, it has a wide network of correspondents throughout Argentina and Latin America.

Authors

Lisandro Frene is a partner at the firm and is head of the IT and data protection department as well as co-head of the TMT department. He has a wealth of experience in TMT, data protection, IP, IT and fair trade. A member of the International Association of Privacy Professionals and the International Bar Association's Technology Committee, where he is the vice-chair of the Artificial Intelligence & Robotics Subcommittee, Lisandro is a professor on the Master's degree course in business law at the Austral University in Buenos Aires (covering technology, privacy and internet-related issues) and a lecturer on technology and data privacy matters at several institutions. He is the author of various articles in domestic and international reviews about TMT, IT, IP and data privacy, and has an LLM degree from the Benjamin Cardozo School of Law at Yeshiva University in New York.

Juan Pablo M Cardinal is head of the TMT practice, and co-heads the IT and data protection department. A partner at the firm, he is highly experienced in TMT, IP, IT, data protection and cloud services. Juan Pablo is a regular assistant to the International Bar Association's Technology Committee and is a member of the Colegio Público de Abogados de la Capital Federal. He has served as a professor of privacy and TMT-related matters since 2000 on a Master's degree course at the Austral University in Buenos Aires and has an LLM degree from the New York University School of Law.

Damián Navarro is a partner at the firm and head of the public law department. He has considerable expertise in public law and TMT. Damián, who is a member of the Asociación Argentina de Derecho Administrativo and the Colegio Público de Abogados de la Capital Federal, has a Master's degree in administrative law and public administration from the University of Buenos Aires.

Richards, Cardinal, Tützer, Zabala & Zaefferer

Av. Leandro N. Alem 1050
Piso 13
Buenos Aires (C1001AAS)
Argentina

Tel: +54 11 5031-1500
Fax: +54 11 5031-2700
Email: frene@rctzz.com.ar
Web: www.rctzz.com.ar