Chambers

GLOBAL PRACTICE GUIDE

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

TMT

Chile
Macarena López M
Ecija Otero

chambers.com

2020

CHILE

Law and Practice

Contributed by:
Macarena López M
Ecija Otero see p.14

Contents

1. Cloud Computing

Laws and Regulations

In Chile, there is a lack of regulations concerning cloud computing. Law No 19.628 (Data Protection Act, DPA) does not include a specific provision regarding cloud providers; however, the activity of cloud computing may be considered as data processing.

According to the DPA, data processing is defined broadly as: any action or set of technical operations or procedures, automated or not, that make it possible to collect, store, record, organise, prepare, select, extract, match, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use it in any form. Consequently, the current DPA makes no distinction between those who control or own personal data and those who provide personal data processing services to owners.

The DPA only mentions the person responsible for a data registry or a bank register, which means any private legal entity or individual, or government agency, that has the authority to implement the decisions related to the processing of personal data. Therefore, there are no different duties for owners, controllers or processors. Nevertheless, government agencies can only process data regarding matters within their respective legal authority and subject to the rules set out in the Data Privacy Act.

Furthermore, the DPA states that any individual can process personal data and it is necessary to comply with the provisions contained in the DPA. The following requirements shall be met – the processing of personal data shall be authorised by one of the three following: the DPA; another legal provision; or the subject or holder of the personal data specifically consenting thereto. In addition, personal data shall be used only for the purposes for which they have been collected (the so-called "finality principle"), and those purposes should be permitted by the Chilean law.

Specific Industries Regulations

In banking

The Financial Market Commission (CMF) is the regulator and supervisor of the Chilean financial market. The CMF supervises entities in securities, insurance markets, banks and financial institutions.

In 2017, an amendment was introduced to Chapter 20-7 of the Updated Compilation of Rules for Banks (RAN) of the Superintendence of Banks and Financial Institutions. Chapter 20-7 regulates the outsourcing of services in the banking industry, specifically cloud computing.

Chapter 20-7 defines the term "cloud services" as an adjustable, on-demand model of services provision associated with technology information through networking, based on technical mechanisms – such as virtualisation – under different approaches or supply strategies; it also provides definitions of "private cloud" and "public cloud".

Furthermore, the regulation establishes special conditions for the outsourcing of cloud services, in order to ensure that the service provider has the appropriate expertise and certifications and fulfils the applicable regulations of the jurisdictions where the services are being carried out, as well as meeting the appropriate safety and encryption standards.

The Financial Market Commission (CMF) issued, on 26 December 2019, a new amendment to Chapter 20-7 of the Updated Compilation of Rules for Banks (RAN) and to Circular No 2, providing the conditions that shall be fulfilled in the externalisation of services by banks, their subsidiaries, which decide to outsource some activity.

By complying with some specific requirements, those modifications will exempt regulated entities from the current obligation to have a data processing site in Chile for services that are outsourced outside the country and that involve activities considered to be critical or strategic. In addition, the CMF determine that the board of directors of each regulated entity (banks, financial institutions, etc) shall be responsible for evaluating and weighing the benefits and difficulties involved in the outsourcing of services, including so-called "contingency sites", being able to hire the providers that best meet their needs. This authorisation is subject to the compliance with operational requirements and to the issuance of a report by a company of recognised prestige and experience in the evaluation of this type of service.

The new regulation also allows for the banks or the financial institutions to outsource cloud computing and other services to be provided from jurisdictions that do not have a country risk rating in terms of investment grade, provided that there are suitable personal data protection and security laws in place. In this case, banks or the financial companies shall be responsible for recording the analysis performed in this regard.

Processing of personal data by public entities

There is a special guidelines regulation applicable to public procurement processes in relation to cloud computing services. The Digital Government Division of the Office of the Presidency (SEGPRES) issued a resolution, *Directiva* No 32, on 26 November 2018, which contains comprehensive guidelines for state administrative bodies to contract cloud services. Although the resolution states that it only contains general, non-binding rec-

ommendations for state administrative bodies and providers, it explicitly recognises that its compliance would constitute good practice in the context of acquisition processes.

The ChileCompra Division is the institution that manages the country's public procurement system. It is a decentralised public service, under the Ministry of Finance. The procedures for purchases could be either: (i) a Marco Agreement (when the virtual store and the electronic catalogue contains the products and services) – this is the result of a public tender of the so-called ChileCompra Division by itself; or (ii) a public tender opened through www.mercadopublico.cl in case the product or service in the Marco Convention store is not found. ChileCompra Division has issued public tender documents regarding cloud computing to help public bodies to contract this type of service.

At the end of 2019, ChileCompra issued a public tender regarding cloud computing, specifying what clauses must have the contracts, requirements, SLA, definitions, etc, in order to help public services to hire cloud computing through the ChileCompra and public market platform. This process is the one that public entities must use when they do not find what they are looking for within the general catalogue of products and services – mentioned in (i) – and, therefore, must go to this second form of contracting (ii) through public tender to hire cloud computing.

Processing of personal data in the context of cloud

There are no specific rules regarding the use of cloud computing. Currently, the DPA does not contain a specific provision regarding cloud providers, but it could be understood that the activity of cloud providers might be considered as data processing. Thus, according to the DPA, data processing is defined as any operation or set of technical operations or procedures, automated or not, that make it possible to collect, store, record, organise, prepare, select, extract, match, interconnect, dissociate, communicate, assign, transfer, transmit or cancel personal data, or use it in any form.

For data processing, it is required to fulfil the provisions contained in the DPA, especially those regarding the authorisation or consent of the data subject, the finality principle (ie, personal data shall be used only for the purposes for which they have been collected, and those purposes should be allowed by the Chilean law) and notifying about the potential public communication of the data.

A failure to comply with those provisions – eg, lack of consent of the data subject – may result in exposure to risks such as fines between approximately USD75 and USD760. In addition, because fines are determined in a summary procedure before the court, the risks of legal disputes and lawsuits are high. Furthermore, the DPA states both non-monetary and monetary damages that result from improper processing of personal data shall be compensated.

2. Blockchain

Risk and Liability

As yet, there is no specific legal regulation in Chile, although the presentation of a bill on the subject has been announced. However, various public entities have incorporated this technology. During the last year, the General Treasury of Chile announced a platform dedicated to processing citizens' taxes, so that this obligation becomes faster and more transparent. In addition, the National Electric Coordinator stated that blockchain would be used to certify fuel cost and stock declarations in the country's electrical system.

Furthermore, two financial entities announced the incorporation of blockchain technology: the Central Bank of Chile is experimenting with this technology and the Santiago Stock Exchange has partnered with two other companies to work on technology-based solutions.

Risks and liabilities are either connected to operational environments and/or to the type of transaction or activity supported by a blockchain solution; thus, the main example of blockchain difficulties in the Chilean legal framework is represented by crypto-assets and, most particularly, bitcoin. According to the Central Bank of Chile, crypto-assets are neither legal tender money nor foreign currency.

Notwithstanding the above, the use of crypto-assets has increased significantly in recent years, but there are unanswered questions regarding the liability of operators of crypto-assets in relation to end-user payers and payees, especially in circumstances related to fraud.

Additionally, since exchange platform operators are not subject to anti-money laundering requirements, conflicts between cryptocurrency operators and a number of banks have been going on for several months. A group of operators brought legal actions against certain commercial banks before the Chilean Competition Court (TDLC) regarding the closing of bank accounts used by operators to settle crypto-assets exchanges in money, alleging an alleged infringement to antitrust law.

The TDLC decided in favour of this group of operators of crypto-assets, indicating that they were paid compensation for the closure of the accounts.

Notwithstanding the aforementioned, to the contrary, there is a latter ruling of the Supreme Court which established that a group of operators that executes the purchase activity and sale of Ethereum and bitcoin that are algorithms – computer programs – lack physical display and do not have intrinsic value by themselves. As there is no legal framework to regulate this financial activity, the court decided against the operators and in favour of the commercial banks that had closed the bank accounts used by those operators of crypto-assets. The court stated that there is not a single person or entity, but a group of operators which use a decentralised set of bitcoin protocol on the internet.

It is necessary to regulate this market because its anonymity can protect illegal operations (eg, tax evasion, money laundering) and because such instruments are neither legal tender money nor equivalent to currencies – therefore, the powers that the Central Bank has for the regulation of currencies do not apply to this case.

Intellectual Property

Blockchain offers rights management from creation to commercialisation.

Essentially, blockchain is a technology that is used to transmit value through a network of contributors/participants. Accordingly, there are several ways in which IP title-holders can use blockchain platforms to enhance control and exploit their IP works, improve collaboration and achieve fair and proficient IP rights management in the digital environment by making the process more transparent and efficient, also cutting out financial intermediaries.

The IP life cycle of the future will ensure that the intangible assets are attributable at the time they are created and that they are protected against fraud and operate in an efficient and innovative network.

Blockchain as a software or database can be protected under the Chilean Copyright Act (Law No 17,336).

At the present time, there still many issues that remain unresolved, such as the required processing control of blockchains, the compatibility and interoperability of different blockchain platforms, and legal issues such as data ownership, privacy, liability, jurisdiction, etc.

Data Privacy

Regulators are still reflecting on how blockchain implementations can comply with data privacy laws. The first issue is determining who is the controller and who is the processor in the case of blockchain and distributed ledgers; due to the lack of a single person or entity that fits the definition.

The DPA requires a lawful basis for processing personal data. In the case of private or permission-based networks, the creators and operators of such networks can prescribe rules for participation, including the types of data to be collected and the purpose for collecting the data. This will ensure notice and transparency at the outset. In addition, if participants are required to agree to terms and conditions, then the contract could serve as a basis for processing personal data.

Conflicts with data subject's rights of the DPA

Blockchains are generally designed so that data, once entered, cannot be changed. This immutability directly conflicts with DPA and GDPR provisions allowing data subjects to request that their data be corrected or deleted. According to the Chilean DPA, one of the data subject's rights is to request to the controller the cancellation of personal data when there is no lawful basis for processing it, or when the existing basis is no longer valid. Additionally, the data subject is entitled to request a modification of stored personal data in the controller's databases when they are erroneous, outdated or incomplete.

However, those rights cannot be readily invoked unless there is a clearly identified controller, such as in a private or permission-based network that has access to all the data on the network. If a network has multiple nodes, with each node having access to only a subset of personal data, it may be necessary to set up a mechanism where requests can be circulated to all required nodes for response.

Blockchain solutions are cross-border by default, there are no territorial restrictions associated to the membership of the blockchain and international transfers of personal data are invariably involved. At present, the DPA does not include a specific provision in this respect. However, considering that transfer of data is deemed as data processing according to the DPA, it follows that it will require authorisation from the individual (ie, the data subject), unless there are exceptions contemplated by the DPA Law and the authorisation is not subject to these exceptions.

Although it is not expressly regulated in the DPA, the transfer of personal data is part of a specific section in the bill aimed at restructuring the Chilean DPA which is currently being discussed in the National Congress.

Service Levels

Blockchain-enabled contracts or smart contracts should play a significant role in automating parts of service level agreements (SLAs) in the coming years. Service level agreement management is one of the most promising areas for blockchain use – for example, aiming to create software products that enable SLA

management among telecom operators utilising blockchain in specific, smart contracts.

It will be necessary include a regulation that considers all of the issues raised above so that, within a legal framework, the rights and guarantees of people are respected and, at the same time, the development of technology and innovation is not prevented. The laws and regulations will need to be updated to adapt to these new technologies because safeguards need to be taken and businesses and consumers should be protected from misuse.

Jurisdictional Issues
These technologies do not have natural frontiers or jurisdictions as limitations because are designed to operate over the internet.

The Chilean DPA does not contain an explicit provision on the scope of the law limited to personal data owners and processors established or operating in the Chilean jurisdiction.

It will be necessary to provide a global regulatory framework in order to ensure the rights of the people. Local complementary laws and regulations should also be implemented in order to achieve the same goal. In addition, antitrust and net neutrality regulations should be reviewed and strengthened in order to guarantee free competition and technological innovation.

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

Big Data
Automation in decision-making through the algorithmic analysis of large databases (big data), without the appropriate checks and balances, can lead to discriminatory, arbitrary results, and/or violate people's fundamental rights. It is necessary to set limits and controls to combat information asymmetries and their consequences.

The collection of large databases can violate people's privacy and makes the protection of privacy becomes more difficult because the information is multiplied and exchanged between different entities around the world without borders.

Since most of the projects imply the collection and processing of large amount of personal data of individuals, Law No 19,628 (DPA) is applicable. The processing of personal data can only be carried out if authorised by the DPA, by other laws or with the express consent of the data subject. If the DPA authorises, there is no need for the express consent of the data subject.

The DPA authorises the processing of personal data:

- when data come from or is collected from publicly accessible sources;
- for the exclusive use of private legal entities, their associates and the entities to which they are affiliated, for statistical, pricing or other purposes of general benefit to the former;
- by public entities, within their competence and subject to the provisions of the DPA; and
- in case of sensitive data, when the treatment is necessary for the determination or granting of health benefits to their owners.

Consequently, pursuant to the DPA, unless otherwise expressly permitted by law, the collection of data must comply with both consent and the notice rule and the purpose limitation requirement, among other requirements set forth in the DPA. However, an exception to both the data subject's consent being the general lawful basis of data processing (including data collection) and the purpose limitation requirement is the processing of certain personal data retrieved from publicly available sources. Nevertheless, all other DPA requirements for processing personal data remain applicable and in force.

Notwithstanding the aforementioned, a bill aimed at replacing the DPA is currently being discussed in the National Congress, establishing GDPR standard rights for data subjects to object decisions based solely on the automated processing of their personal data, including the elaboration of profiles. The bill includes this phenomenon and requires that this secondary use of personal data be based on a compatible purpose – ie, that there is a contractual relationship with the holder that justifies this differentiated use or that there is a new consent by the holder. This contrasts with the European experience, in which the consent criterion co-exists with enablers to exploit the data, which is complemented by demands of responsibility and control mechanisms endorsed by companies that process this data.

Machine Learning (ML)
There is a lack of regulation in the Chilean legal framework regarding the use of predictive tools based on machine-learning algorithms.

The DPA only refers to the prohibition of the execution of any type of prediction or commercial risk assessment not based exclusively on objective information related to delays or defaults in payment from the individuals or legal persons in question. Moreover, even if there is no guideline regarding how to handle biases in algorithms or other automated decisional techniques, then Law No 20,609 (Anti-Discrimination Act, ADA) shall be applicable. The ADA establishes a legal action that may be filed by persons who are victims of arbitrary discrimination.

Finally, similarly to the GDPR, the Data Protection Bill includes a data subject's right to request human intervention when is not legally feasible to exercise the right to request, not being subject to a decision with legal effects based solely on automated data processing.

Artificial Intelligence (AI)
Despite the government's concern about the increase of AI, there is currently no regulation on the matter. However, the local securities and insurance supervision agency, the Chilean Financial Market Commission (CMF), is conducting research about possible future changes to securities trading and financial advice regulation in order to face the rise of robot-adviser technologies. In such regard, the CMF is aware that the current tools that are in place to ensure the quality of financial advice are useless when an AI is deployed for recommending investment opportunities.

Intellectual Property Issues Related to Big Data, ML and Cloud Computing Storage Solutions
Regarding the intellectual protection of databases, Article 3 of Law No 17,336 (Copyright Act) establishes a non-exhaustive catalogue of "works" that can be protected by copyright.

The Copyright Act protects the rights that the authors of intellectual works in the literary, artistic and scientific domains acquire through the sole fact of their creation, whatsoever their form of expression, and the neighbouring rights it establishes.

The following, among others, are especially protected: (i) computer programs, whatsoever their mode or form of expression, and source programs or object programs, including their preparatory documents, technical descriptions and user manuals; (ii) data collection or collection of other materials, in typewritten form or any other form, which, due to the selection or disposition of their contents, constitute creations of an intellectual nature. According to the Copyright Act, this protection does not embrace the data or materials themselves and any subsisting copyright in connection with the data or material included in the referred collection.

ML algorithms can be subject to a twofold protection as copyrighted work: (i) as part of a computer program, in respect to its computer code implementation; and (ii) as a database, in case such algorithm ends up being a core component of an original compilation by virtue of its features as a data arrangement and processing tool (eg, a "random forest algorithm" fitted to classify customers in a particular matrix of features).

Insurance Policies Available to Data Assets
Regarding insurance of data and other informational assets, there is no special regulation that differs from the general rules applicable to casualty and property insurances. According to the CMF's website, there are several policies concerning civil liability arising from data protection regulations and losses caused by data breaches.

4. Legal Considerations for Internet of Things Projects

Fifth-generation mobile telephony (5G) has been presented as the promise of future telecommunications development, its faster speed meaning an ability to move more data, to connect more devices at the same time, and to aid the development of artificial intelligence (AI) and the Internet of Things (IoT).

The National Cybersecurity Policy (NCSP) establishes that it is necessary to promote the protection of public and private-sector networks and computer systems, especially those that are essential for the proper functioning of the country, ensuring the operational continuity of basic services. In addition, it seeks to establish common standards and protocols on how telecommunications will operate, prevent negative effects on the rights of citizens, including constitutional guarantees related to privacy, the protection of their personal data, the inviolability of communications, freedom of expression and access to information.

Currently, IoT services do not require a special authorisation, nor are they subject to specific requirements. Nonetheless, some general telecommunications standards do contemplate certain restrictions relating to the frequency bands and equipment being used to provide IoT services, as well as considering rules concerning the protection of personal data and the inviolability of communications that should be considered in the deployment of IoT services.

General Telecommunications Regulation
An IoT service that uses the radioelectric spectrum to transmit information from one point to another should comply with the requirements of the General Plan for the Use of Radioelectric Spectrum, Decree No 127-2006 of SUBTEL, which states the use that can be assigned to a specific frequency band.

As SUBTEL has not allocated a frequency band for IoT services, the use of a frequency band must be officially applied for; SUBTEL grants experimental licences which have a duration of five years, renewable for another such period at the request of the interested party (Law No 19,168 Telecommunications Act, LGT). To obtain such a licence, or to renew an existing licence, the payment of a single spectrum right is required. According to the LGT, experimental permits – also granted by SUBTEL – are of a temporary nature (their duration is two months) and may

not be used to provide commercial services. Spectrum usage rights do not need to be paid.

Regarding the equipment used for IoT, the project developer should consider obtaining a certification or an authorisation by SUBTEL, according to the Technical Standard for Reduced Scope Equipment (Decree No 1985-2017), depending on the equipment's specific technical characteristics.

Decree No 1463 of 2016 of SUBTEL regulates the minimum technical specifications that need to be fulfilled by equipment used in mobile networks; thus, IoT devices must be registered in a database with respect to which SUBTEL has real-time access.

Regulation of IoT Regarding Data Protection and Inviolability of Communications

IoT with domestic objectives must meet not only general telecommunications standards, but also abide by restrictions based on the regulation of privacy. The guarantees of Article 19 No 4 and No 5 of the Constitution respect and protect the privacy and honour of the person and their family, and protect their personal data, establishing the inviolability of the home and all forms of private communication. The specific regulation on privacy is contained in Law No 19.628 (DPA), detailed in **6. Key Data Protection Principles**.

The criminal code establishes the illegality of the capture, interception, recording or reproduction of private communications and private events, in private premises or places that are not freely accessible to the public, without the authorisation of the party affected (Article 161 A). In this regard, malicious wiretapping through IoT devices, such as the leak of private communications recorded by smart devices, should not be treated differently than traditional illegal communications interceptions (ie, machine-to-machine).

5. Challenges with IT Service Agreements

Specific Features

The Chilean legal framework is appropriate for executing IT agreements, ranging from simple ones to extremely complex contract agreements.

The most frequently used clauses in the IT industry within IT agreements are limited liability, "as is" disclaimers, service level agreements (SLAs), audit rights, no-assignment rules and non-disclosure agreements.

Nevertheless, the following are some aspects of Chilean law that any service provider, software developer and/or IT contractor should consider in order to reach the most favourable agreements with Chilean-based customers.

Limitation of liability clauses – both limitation on recovery for certain damages and liability caps – are generally accepted and enforced by courts when professional parties execute a contract but there is gross negligence and wilful misconduct, among other similar circumstances. In case of public entities those type of clauses are not allowed.

Law No 19,628 (DPA) does not currently include a specific provision regarding restrictions on international data transfers of personal information. Nevertheless, the transfer of personal data outside the jurisdiction of Chile may be considered as a use of data and will require authorisation and other restrictions established by the Law.

The Financial Market Commission (CMF) is the regulator and supervisor of the Chilean financial market. The CMF supervises entities in securities, insurance markets, banks and financial institutions. In 2017, an amendment was introduced to Chapter 20-7 of the Updated Compilation of Rules for Banks (RAN) of the Superintendence of Banks and Financial Institutions. Chapter 20-7 regulates the outsourcing of services in the banking industry, specifically cloud computing.

Chapter 20-7 defines the term "cloud services" as an adjustable, on-demand model of services provision associated with technology information through networking, based on technical mechanisms – such as virtualisation – under different approaches or supply strategies; it also provides definitions of "private cloud" and "public cloud". Furthermore, the regulation establishes special conditions for the outsourcing of cloud services, in order to ensure that the service provider has the appropriate expertise and certifications and fulfils the applicable regulations of the jurisdictions where the services are being carried out, as well as meeting the appropriate safety and encryption standards.

It includes mandatory clauses that refer to business continuity, subcontracting, data-deleting procedures, and supervising rigorous supplier/provider selection processes, according to their internal risk assessment procedures. In addition, the regulation establishes special conditions for the outsourcing of cloud services in order to ensure that the service provider has the appropriate expertise and certifications and fulfils the applicable regulations of the jurisdictions where the services are being carried out, as well as abiding by the appropriate safety and encryption standards.

On 26 December 2019, The Financial Market Commission (CMF) issued a new amendment to Chapter 20-7 of the Updated Compilation of Rules for Banks (RAN) and to Circular No

2, providing the conditions that shall be fulfilled in the externalisation of services by banks, their subsidiaries, which decide to outsource some activity.

By complying with some specific requirements, those modifications will exempt regulated entities from the current obligation to have a data processing site in Chile for services that are outsourced outside the country and that involve activities considered to be critical or strategic. In addition, the CMF determine that the board of directors of each regulated entity (banks, financial institutions, etc) shall be responsible for evaluating and weighing the benefits and difficulties involved in the outsourcing of services, including so-called "contingency sites", being able to hire the providers that best meet their needs. This authorisation is subject to compliance with operational requirements and to the issuance of a report by a company of recognised prestige and experience in the evaluation of this type of service.

Chapter No 20-7 of the Updated Compilation of Rules for Banks (RAN) of the Superintendence of Banks and Financial Institutions from the Financial Market Commission regulates the outsourcing of services in the banking industry, specifically to cloud computing, after an amendment introduced in 2017. It included mandatory clauses that refer to business continuity, subcontracting, data-deleting procedures, and supervising rigorous supplier/provider selection processes, according to their internal risk assessment procedures. In addition, the regulation establishes special conditions for the outsourcing of cloud services, in order to ensure that the service provider has the appropriate expertise and certifications and fulfils the applicable regulations of the jurisdictions where the services are being carried out, as well as abiding by the appropriate safety and encryption standards. On 26 December 2019, the Financial Market Commission (CMF) issued an amendment to the regulation to Chapter 20-7, providing for the conditions that shall be complied with by banks, their subsidiaries, the companies which provide them support and the issuers and operators of payment cards, regarding "the outsourcing of services".

It is important to bear in mind the bill on computer crimes, which establishes that computer crimes be added to Law No 20,393 regarding criminal liability of legal persons/entities, this in terms of the crimes of money laundering, terrorist financing and bribery offences. The issues of compliance in data governance and cybersecurity are precisely related to this type of IT services agreement. The bill is expected to be enacted in 2020.

6. Key Data Protection Principles

Core Rules Regarding Data Protection
The legal framework governing privacy can be found in Article 19 No 4 of the Political Constitution of the Republic of Chile, which guarantees the respect and protection of privacy and honour of the person and his or her family. Article 19 No 4 of the Chilean Constitution was amended by Law No 21,096, establishing the Right to Protection of Personal Data; it precisely recognises the protection of personal data within the scope of the constitutional guarantee of the protection of private life and honour, stating that the treatment and protection of this data will be subject to the forms and conditions established by law.

Furthermore, Chile has a data protection law, Law No 19,628 on Privacy Protection (Data Privacy Act, DPA); this regulates the treatment of personal information in public and private databases or bank register. Further, regarding the public sector, there are some special rules concerning use of the public database or bank register by public agencies, and restricted rights for holders of personal data stored or processed by public entities.

Law No 19,496, which provides provisions regarding credit information, operates along with the DPA (Article 9, amended by Law No 20,521) which contains provisions about personal data related to obligations of an economic, financial, banking or commercial character to ensure that the information delivered through risk predictors is accurate, updated and truthful.

Law No 20,584, which regulates privacy on healthcare, encompasses provisions concerning the privacy of medical records and operates together with the DPA, which details the confidentiality of doctors' prescriptions and laboratory analyses, together with examinations, etc, related to health services.

Distinction Between Companies/Individuals
Only individuals are under the protection of the DPA.

General Processing of Data
Currently, the DPA has no requirements for the appointment of privacy or data protection officers (DPOs).

The processing of personal data could only be carried out if authorised by the DPA, by other laws or with the express consent of the data subject. If the DPA authorises, there is no need for the express consent of the data subject. The DPA authorises the processing of personal data:

- when data come from or are collected from publicly accessible sources;

- for the exclusive use of private legal entities, their associates and the entities to which they are affiliated, for statistical, pricing or other purposes of general benefit to the former;
- by public entities, within their competence and subject to the provisions of the DPA; and
- in case of sensitive data, when the treatment is necessary for the determination or granting of health benefits to their owners.

Currently, there is no exception regarding fulfilment of contract and the DPA does not include the need to adopt internal or external privacy policies.

The law contains a definition of the dissociation process, which means all personal data processing by which the information obtained cannot be related to an identified or identifiable individual (ie, anonymisation, pseudonymisation).

Processing of Personal Data

The Data Privacy Act states any individual can process personal data, if the following requirements are met:

- The processing of personal data shall be authorised by either: (i) the DPA, (ii) another legal provision, or (iii) if the subject/holder of the personal data specifically consents thereto. In addition, the authorisation granted by the holder/subject of the personal data regarding to the processing of his or her data shall comply with the following requirements in order to be effective:
  - (a) it shall be accurately informed about the purpose of the storage of the personal data and if this data will be communicated to the public;
  - (b) the consent shall be specified; in writing; and
  - (c) the personal data must be used only for the purposes for which it has been collected, unless it comes from or has been collected from public sources – further, the data shall be accurate and up to date.
- the rights granted by the Data Privacy Act shall be respected and fulfilled;
- the purposes of the collecting and processing shall be allowed by the Chilean law.

To exercise the right to access, the data subject must address the person responsible for the data registry or bank claiming his or her right to access his or her data. This right to access may refer to:

- the origins of the data (ie, how this data was collected);
- the addressee of the data;
- the purpose of the storage of the data; and
- the identification of the persons or agencies to whom his or her data is regularly transmitted.

Access to information on personal data shall be free of charge. This right to access cannot be limited by means of any act or agreement, except in case of government agency, the security of the nation or national interest. Data subjects also have the right of rectification if the personal data is erroneous, inexact, equivocal or incomplete, and such a situation has been evidenced.

Data subjects also have the right of deletion of personal data if its storage lacks legal grounds or if it has expired, when the subject has voluntarily provided his or her personal data, it is used for commercial communications or he or she does not want it to continue appearing in the respective registry, either definitively or temporarily.

Data subjects may oppose or object to the use of personal data for purposes of advertising, market research or opinion polls. If the person responsible for the personal data registry or bank register fails to respond to a request within two business days, or refuses a request on grounds other than the security of the nation or national interest, the subject of the personal data shall have the right to attend before the civil court requesting protection to his or her right of access or the other rights granted by the DPA.

7. Monitoring and Limiting of Employee Use of Computer Resources

Article 5 of the Labour Code expressly states that employers can exercise their rights within the limits imposed by the Constitution, especially regarding respect of privacy. Employers must abide by and comply with the privacy statements. Article 154bis of the Chilean Labour Code states that the employer shall maintain a reserve of all private information and data of the employee to which it has access due to the labour relationship.

In this matter, the issue raises the existence of a possible conflict between, one the one hand, the constitutional guarantee of the inviolability of all forms of private communication and, on the other hand, the employer's power to organise, direct and manage his or her company, which comes from the constitutional guarantee of the right of property (articles 19 No 5 and No 24 of the Constitution).

The Labour Authority (LA) has ruled that the employer has the right to regulate the conditions, frequency and timing of use of their property, provided they do not infringe the constitutional guarantee of the inviolability of all forms of private communication. In this regard, the LA sees no objection in the regulation of corporate emails, provided this does not affect the abovementioned constitutional guarantee.

According to Ruling No 260/0019-2002 of the LA, the employer can regulate the conditions, frequency, and timing of the use of corporate email and, where necessary, can ensure that all emails sent from the company server are copied to management. Although the employer cannot access personal emails in any respect, it is possible to limit their access.

Regarding employee monitoring in general, the LA states that a determination as to whether or not certain forms of business control are appropriate must be carried out considering the employer's objectives for its implementation, which will ultimately establish whether the form of control at issue affects the employees' dignity and free exercise of fundamental rights (Ruling No 3125-2018).

The LA has ruled that it can review or audit corporate emails to an extent that meets certain requirements or conditions since corporate email and computer resources are tools that the employer makes available to employees for the faithful performance of its orders. The control measures of the employer regarding the use of corporate email cannot involve excessive control that infringes the rights of privacy and dignity of the employee. The review or audit must be incorporated in the internal rules so that employees are aware that it can be monitored and audited. In addition, it should include an internal procedure for reviewing such as mailings, computer use, etc, which must protect and not infringe the privacy rights, dignity, and honour of the employees. The review should be random (all employees of the company, or an area or a section of the company) or be the result of a specific complaint about misuse of the computer resources of the company, which should be evident in the rules of procedure. The review, in this case, should be limited to verifying the existence of the alleged infringement.

Through Ruling No 260/19 of 15 November 2019, LA expressly stated that any email sent by the employee from the email account provided by the company will be automatically copied and deposited in an employer's folder; thereby, such emails do not have the character of private communication but are rather the property of the company, which is fully empowered to monitor and keep these emails, even after the end of the employment relationship. However, this criterion applies only in the case of emails sent by the worker, in which the employer has a copy sent from his or her electronic mailbox – it does not apply to any emails received, for which the worker can legitimately have higher expectations of privacy, since it is correspondence in respect of which the worker-user of the corporate email lacks full control.

Furthermore, any control measure – that is, not only those that find their foundation in the law, but in other normative sources – can only be carried out by suitable means and be consistent with the nature of the employment relationship and, in any case, its application must be general, guaranteeing the impersonality of the measure in order to respect the dignity of the worker.

8. Scope of Telecommunications Regime

Technologies within Local Telecommunications Rules

Currently, there is not a specific technology deemed to fall within the scope of local telecommunications rules. Thus, the Telecommunications Act (the LGT), defines "telecommunications", classifying the different "telecommunications services" in its Article 3, based on their purposes and not on the technology with which they are or should be provided.

Notwithstanding, there is special sectorial regulation in telecoms when defining some services, citing the technology which is to be used; moreover, there is regulation about the conditions that certain equipment must meet when using a specific technology. Decree No 484-2008 on public VoIP services states this service is a public telecommunications service as long as it is likely to establish voice communications intended for the community in general, and interconnect with other public telecommunications services (eg, calls from an IP voice network to a public telephone network).

There is no reciprocal connection between the VoIP service and the public telephone network, such as calls are made through the internet or without a dial-in number; therefore the service would not be defined as a public telecommunications service and, subsequently, such services would not fall under the scope of the aforementioned Decree.

VoIP

The installation, operation and exploitation of public VoIP services, require a concession of public telecommunications services, granted by the Ministry of Transport and Telecommunications (MTT). Furthermore, as a public telecommunications service, it must comply with all the obligations that this qualification entails (the LGT). Concessions are granted without the need for a public contest, because they do not use the scant resources of the radioelectric spectrum.

RFID

Equipment for radiofrequency identification (RFID) must comply with the provisions of Decree No 1985-2017, which establishes the respective technical standard. These standards require that equipment emitting radio waves in certain frequency bands with a certain electric field strength must undergo a certification process in advance.

Instant messaging
In broadcasting, an OTT (over-the-top, free streaming) service consists of the transmission of audio, video and other content over the internet without the involvement of traditional operators in the control or distribution of content. OTT services such as instant messaging services are not regulated by telecommunications regulations – no authorisation is required, and there are no standards of service quality, interconnection obligation or other specific rules to be complied with. Nevertheless, the Consumer Protection Act and the DPA are applicable.

9. Audio-Visual Services and Video Channels

Main Requirements
The requirements for providing any telecommunications service, including audio-visual services, are regulated for the use of the radio spectrum and according to if the service is limited or freely available.

Radio services
According to the Telecommunications Act (Law No 18,168, the LGT), radio services require a licence granted by the Ministry of Transport and Telecommunications (MTT), which has a duration of 25 years; a licence for community radio services has a duration of ten years, being regulated by the Citizen Community Broadcasting Services Act (Law No 20,433).

Radio services are granted through a public bid to the applicant offering the best technical condition. The applicant must be a legal entity incorporated in Chile, and have a legal address in the country. The entity's presidents, directors, managers, administrators and legal representatives must be Chilean and not have a major criminal conviction. In the case of a board of directors, foreigners may be nominated as directors but they may not constitute the majority. Once the licence is granted, the applicant must publish an extract of it in the *Official Gazette* (Decree No 126-1997). Before starting transmissions, SUBTEL shall inspect and authorise the company's facilities (the LGT).

TV and radio content regulation
Regarding content regulation, free-to-air broadcasters and permit holders of pay-TV services must comply with several rules for the proper functioning of television services.

These include the obligation of broadcasting a certain amount of cultural content per week, restrictions on content deemed violent, pornographic or immoral, time restrictions on certain movies rated by the cinematographic rating board and limitations on advertising of some products, such as alcohol.

In the case of radio broadcasting licensees, according to the Promotion of Chilean Music Act (Law No 19,928), there is an obligation of broadcasting a minimum daily quota of Chilean music, including emerging and local artists.

None of these regulations apply to online video channels.

Free-to-air broadcasting
According to the National Television Council Act (Law No 18,838), free-to-air broadcasting services require a licence granted by the National Television Council – the licence has a duration of 20 years (in the case of licences with their own necessary technical means), and of five years (in the case of licences with technical means provided by third parties).

The Digital Terrestrial Television Introduction Act of 2014 (Law No 20,750), encouraged the transition from analogue to digital broadcasting. It also established the obligation to achieve total digital coverage by the 2020, the date of the so-called "analogue blackout". However, the MTT has the facility to extend the original term by means of a Supreme Decree.

Limited telecommunications services, such as pay-TV, require a permit granted by SUBTEL to a legal entity (the LGT). Satellite television permits have a duration of ten years; in the case of cable TV there is no expiry date if the radio spectrum is not used.

10. Encryption Requirements

Legal Requirements
There is no general legal requirement for the use of encryption techniques on electronic communications and documents. However, encryption as a cryptographic process of encoding information for confidentiality, integrity and authenticity purposes is subject to certain regulations, depending on the characteristics of each framework of use of this technology.

Encryption Exemption
According to the DPA, those responsible for or in control of the database are required to ensure that those involved in personal data processing comply with confidentiality obligations because of the security liability of the personal data storage in the database and that the rights of the data subjects are safeguarded.

In case of a request for personal data through an electronic network, the following information must be recorded: (i) the inquirer's identity, (ii) the requested purpose, and (iii) the specific data being transferred.

Regarding security requirements, the DPA does not impose any type of security measures of the data subjects in relation to processing of personal data. However, responsibility for the database in which personal data is stored (after its collection) should be managed with due diligence, confidentiality and assuming responsibility for damages.

Furthermore, there are specific rules regarding banks and financial institutions in which the data of their clients and their wire transfers, encryption and notice of security breach is mandatory. This regulation is transitory and was dictated by the entity that supervises the banks (the CMF). Currently, the bill that includes regulation in these matters is pending in Congress.

Furthermore, there are specific rules regarding banks and financial institutions that are mandatory and that must complied with: for example, customer data and electronic transfers must be encrypted, and it is mandatory for banks and financial institutions to notify any security breach to the CMF within 30 minutes. Notwithstanding the foregoing, this regulation is transitory and was issued by the CMF. A bill that includes the regulation of all these matters is currently pending in Congress.

Other Regulations

Additionally, there are some other regulations that contain cybersecurity provisions applicable only for certain areas, such as those listed below.

Law No 19,223 on cybercrimes regulates (i) unauthorised access to databases or information, and (ii) unauthorised disclosure of such information, among other criminal actions. Currently, there is a Bill in the Congress which will amend all rulings on cybercrimes, and in which the use of encryption technologies with the wilful purpose of obstructing the course of justice shall be considered an aggravating circumstance of criminal liability when committing any of the criminal offences proposed in the draft.

The General Telecoms Law (GTL) in Article 24 H rules in relation to the obligation of seeking to safeguard network security for internet service providers (ISPs) and telecommunications concessionaires.

Decree No 83 of 2005, issued by the Ministry General Secretariat of the Presidency, deals with the Confidentiality and Security of Electronic Documents for the Public Administration.

In 2017, the government's first National Cybersecurity Policy was released. The objectives by 2022 include a risk management approach to preventing and reacting to incidents, including the protection of information/critical infrastructure and preventing and reducing cybercrime. In relation to this, the NCSP states the requirement of differentiated standards in cybersecurity, as follows.

- All information infrastructures that depend on or provide products or services to the Chilean government or citizenship services must, at a basic level, adopt cybersecurity measures in accordance to standards that duly consider confidentiality, integrity and the availability of the information and the systems that operate, according to the risks and threats that exist, in a manner consistent with its size, maturity, and the level of criticality and confidentiality of the information and/or processing they support.
- In the case of critical information infrastructures, they must assess their risks and address them according to standards that duly consider the confidentiality, integrity and availability of the critical information infrastructure (ICI), to have an effective and harmonious security system that allows prevention, management and recovery of cyber-attacks and other computer security incidents, with contingency plans to ensure the operational continuity of its services.
- The standards and best practices to be used will be compatible with international guidelines, ensuring the confidentiality, integrity and availability of information, without prescribing specific solutions, except for qualified cases.

On 11 November 2019, Law No 21,180 on the Digital Transformation of the State was published. Its purpose is to initiate the process of digitalisation and modernisation of the administrative procedures followed before the state administration bodies. Among the main innovations that will be incorporated under the State Digital Transformation Law are the following.

- It will be obligatory that any procedure carried out before an entity of the state administration must be carried out through electronic procedures maintained by each public entity in an electronic file. Only in exceptional cases, established by law, can physical procedures be carried out.
- The communications made between entities of the state administration must be made through electronic means, electronic copies of these being sent to those interested in the administrative procedure.
- Any document that accompanies an administrative procedure must be done electronically. Paper-based documents must be digitised, and their authenticity and integrity will be corroborated in the manner determined by future regulations. Electronic documents shall be governed by the provisions on electronic signature of Law No 19,799. The power to act in an administrative procedure may be recorded in a document signed by electronic signature. "Advanced electronic signature" or public deed will be required when the solemnity of the act so requires.

Ecija Otero has an expert knowledge of information technology, TMT, privacy, cyber, IP, and digital transformation, and is one of the most representative law firms in the Hispanic and Portuguese languages in this area, providing legal services to multinationals, nationals and foreign companies. In Chile, the firm is highly specialised in licensing and software development agreements, technological platforms, data protection and privacy, technology contracts, cloud services, copyright, internet computer crimes, cybersecurity and compliance. Furthermore, the firm has notable expertise in policy enforcement management on matters affecting the IT areas, IP, privacy, telecoms, cybersecurity, net neutrality, software, and copyright industries. The team has worked for the responsible regulating bodies and therefore has detailed knowledge and a constantly up-to-date expertise, meaning it is able to offer high-quality comprehensive advice in all aspects related to data protection law, privacy and cybersecurity. Ecija Otero has wide experience elaborating studies and reports about technology and creative industries from a legal perspective, as well as possessing knowledge of the legal procedure regarding digital transformation of companies of all descriptions. With over 20 years of experience, Ecija Otero has positioned itself as one of the best multidisciplinary and independent firms in the Chilean IT market, offering comprehensive legal services regarding regulatory compliance and information security.

Author

Macarena López M is director/manager of the TMT, privacy, cyber, information technology and IP area of the Ecija Otero office in Chile and has been head of the firm's information technology, TMT, data protection and cybersecurity department since 2006. Macarena has more than 25 years of extensive experience, both nationally and internationally, in matters related to new technologies, intellectual property and privacy. Her areas of practice also focus on negotiation and advice on licensing, implementation and maintenance of software, data centres, telecommunications, cybersecurity, fintech and public policies in various matters related to issues affecting the software industry, privacy, video and online games, net neutrality, and data protection. Macarena worked as a foreign attorney with Greenberg Glusker, Los Angeles; during that time, she also was legal adviser to the Latin America Committee of the Business Software Alliance (BSA), Washington, D.C. and BSA country manager in Venezuela, Costa Rica and México (2004-05). She is a visiting professor at the Faculty of Law, University of Chile and on the CEDI, in the magister programmes and in various certificated courses. She was professor of Procedural Law and of Intellectual Property and New Information Technologies at the Adolfo Ibáñez University (2006-14). Macarena studied law at Universidad de Chile Law School (JD) and graduated with the highest honours, obtaining her law degree in 1997, and has an LLM from University of California, Berkeley, 2004.

Contributed by: *Macarena López M,* ***Ecija Otero***

ECIJA OTERO

Av. Apoquindo 3669
13th Floor
Las Condes
Santiago
Chile

Tel: +56 22 361 8900
Fax: +56 22 361 8999
Web: www.ecija.com