Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

TMT

Peru
PAYET REY CAUVI PÉREZ ABOGADOS

chambers.com

2019

Law and Practice

Contributed by PAYET REY CAUVI PÉREZ ABOGADOS

Contents

PAYET REY CAUVI PÉREZ ABOGADOS has a TMT practice group that includes partners and associates from the firm's competition and regulatory practice groups. Members of the dispute resolution practice group are also involved in several judicial and arbitration cases regarding the TMT sector, while members of the corporate practice group have been involved in various transactions directly related to TMT-sector companies. With extensive experience in the TMT market, Payet, Rey, Cauvi, Pérez Abogados specialises in designing strategies for administrative procedures before the Ministry of Transport and Communications and the telecoms regulatory agency OSIPTEL regarding sanction procedures, price adjustment procedures, mandates, interconnection and network access, consumer regulations, antitrust, data protection law and zero-rating services. The practice advises media and technology companies concerning compliance with various laws and regulations, and the design of commercial agreements and policies. The firm's integrated full-service team has dealt with some of the most important transactions involving major corporations' acquisition of telecommunications infrastructure.

Authors

Gerardo Soto is a partner of the firm who specialises in regulatory law and administrative law. He has extensive experience of advising clients in the telecoms, energy, transportation and mining sectors, dealing with regulatory agencies including the Ministry of Energy and Mines, OSINERGMIN (mining supervision) and OEFA (environmental supervision) and defending administrative proceedings initiated by the above-mentioned and other regulatory agencies. Prior to joining the firm, he headed the law department of OSIPTEL. Gerardo has written various articles on regulatory law in specialised journals.

Sebastian Gamarra is an associate of the firm who is experienced in administrative law, the regulation of public services, concessions and infrastructure projects and competition law. He has written articles on telecommunications law and regulation for specialised legal web publications.

1. Cloud Computing

1.1 Laws and Regulations

The main statute regulating cloud processes is Law 29733, Law for Personal Data Protection ('Law 29733') and its Regulation, approved by Supreme Decree 003-2013-JUS (the 'Regulation').

This regulatory regime imposes various obligations to individuals and companies who, in the development of their activities, access and administer personal data of current or potential customers, employees or other individuals by using (or not) cloud computing systems.

Specifically, Article 33 of the Regulation refers to data processing via cloud computing systems (' *medios tecnológicos tercerizados* '), by pointing out that these processes ought to be conducted in strict compliance with Personal Data Protection obligations.

Such obligations require, in some cases, adapting the terms and conditions of contracts pursuant to which personal data is accessed, adopting internal security measures to ensure the confidentiality and safety of personal information, implementing channels for access to the personal information by owners, as well as registering before the competent national authorities the personal data databases they may be managing, among other subjects (for further information of these regulations see **7 Monitoring & Limiting of Employee Use of Computer Resources**, below).

Moreover, by virtue of Resolution No 001-2018-PCM/SEGDI, the Secretary of the Digital Government of the Prime Ministry Office approved the 'Guidelines for the use of cloud services by entities of the Public Administration of the Peruvian State'. These guidelines are only applicable for public sector and establish several requirements to contract with cloud services providers and manage personal and public data.

1.2 Regulations in Specific Industries

See **1.1 Laws and Regulations**.

1.3 Processing of Personal Data

See **1.1 Laws and Regulations**.

2. Blockchain

2.1 Risk and Liability

Peru does not have a specific law or regulation for blockchain matters. Thus, besides the data protection regime and gen-

eral laws related to intellectual property and civil contracts (which are applicable for any kind of economic activity or technology in the country) there are no legal conditions at present to develop and use blockchain technology.

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

3.1 Big Data

The Peruvian legal framework does not include regulations related to the development of big data, machine learning and artificial intelligence projects. In this sense, Peru has an open environment in terms of legislation despite the lack of public investment in this field across the country.

Conditions regarding insurance and liability matters are regulated through private contracts. However, the civil code admits certain rules for compensation for non-contractual liability, in the event of any damages and negligence caused by the responsible party.

In addition, the Peruvian Constitutional Tribunal has not issued any sentence regarding the fundamental rights involved in the process or creation of machine learning or artificial intelligence. Nevertheless, the Tribunal has established in several sentences the importance of privacy and the appropriate use of personal data (both recognised as fundamental rights by the Peruvian Constitution). Thus, it is imperative that big data project leaders are fully compliant with all protection of privacy and security requirements contained in Law No 29733.

3.2 Machine Learning

See **3.1 Big data**.

3.3 Artificial Intelligence

See **3.1 Big data**.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions Affecting a Projects' Scope

In the absence of a public policy or specific law for Internet of things (IoT) projects, one of the most important restrictions for these projects (in addition to Law No 29733 requirements) is the observance of the right to secrecy and the inviolability of communications. This right guarantees that communications will not be intercepted or known by third parties unless prior consent of those involved in communication has been granted or with a due motivated authorisation by a judge.

Law No 27697 points out that communication should be understood as "any form of transmission of the content of thought, or an objectified form of it by material or energetic means". Thus, the right protects information contained in letters, telegrams, e-mails, text messages, telephone conversations, computer systems etc (in accordance with Article 13.4 of Law 29733).

Protection guarantees that third parties unrelated to those involved in the communication may not perform (with respect to the information contained in the communication) the following activities: theft, interception, interference, change or alteration of the text, deviation of communication, outreach, dissemination, publication, use and even the facilitation of means to carry out such activities.

It should be noted that protection reaches the integrity of the content of the communication, regardless of the topics that are addressed in the communication. In this sense it will protect both the content of any personal information and public information. The reason for this is that the secrecy of communications is not only oriented to protect the right to privacy, but the integrity of conversations (this because their primary objective is to avoid interception or interference by a third party).

This right is recognised by the Peruvian Constitution as a law of fundamental nature, which enjoys a higher level of protection. Therefore, a standard has been developed aimed to delimit the scope of this right and ensure appropriate protection by a public entity (including criminal and telecom laws).

Any type of violation of communications without the prior consent of the parties or the motivated authorisation made by a judge is considered a crime under the provisions of the Criminal Code (Article 161).

Also, according to the General Law of Telecommunications (Article 87) and its Regulation (Article 13), the violation of the right to private communications is classified as an infraction (in the case of telecommunications operators). Moreover, due to the evolution of telecommunications and mass media, various regulations that specifically refer to the obligations of the telecommunications operators have also been developed (ie, Ministerial Resolution No 111-2009-MTC-03 and Resolution No 015-2016-CD-OSIPTEL). Therefore, operators are obligated to implement mechanisms to ensure that the users' communications remain private, and any unveiling of their content must be proportionate only in accordance with those regulations.

5. Challenges with IT Service Agreements

5.1 Specific Features

IT service providers that store personal data which has been transferred outside Peru must comply with the rules of Law No 29733 (Article 11), which establish an obligation to guarantee the same levels of security and privacy for personal data as required in Peru.

These set levels involve technical measures to avoid alteration, loss, processing or any unauthorised access to personal data. The security measures should be appropriate and consistent with the level of processing to be carried out.

IT service providers are not required to establish a local presence in the country (except for an address for notification purposes in matters regarding personal data). Also, Peru does not have price revision restrictions or any special prohibitions related to IT services.

6. Key Data Protection Principles

6.1 Core Rules Regarding Data Protection

The provisions of Law No 29733 and its Regulation only protect the personal data of individuals, although the obligations and requirements apply to both individuals and companies. This regime creates several categories in order to systematise the levels and conditions of data protection, as follows.

Personal data comprises numerical, alphabetic, graphic, photographic, acoustic or any other type of information pertaining to natural persons that identifies them or makes them identifiable. For example, the name of a person, their e-mail address, their telephone number, their national identity document number, their fingerprint, among others, are considered to be personal data.

One special category of personal data is so-called sensitive data, which pertains to information on the racial or ethnical origin of a person, economical income, political opinions or convictions, among other types of information.

Processing personal data consists of any operation or technical procedure (automated or not) that allows for the collection, registration, organisation, storage, conservation, preparation, modification, extraction, consultation, use, blockage, suppression, communication by transfer or dissemination or any other form of processing that facilitates the access, correlation or interconnection of personal data.

A personal data database is any organised set of personal data, automated or not, regardless of the means employed (physical, magnetic, digital, optic or others to be created), whatever the form or modality of their creation, formation, storage, organisation and access.

The owner of a personal data database will be the individual, the company, the private legal entity or public entity that determines the purpose and contents of the personal data database, the processing thereof and its security measures.

Usually, a company, regardless of its economic activities, will be the owner of the personal data database that contains information about its employees and clients that are individuals. For example, a financial institution will be the owner of the personal data database that contains information about its clients.

The personal data database processor is any individual, company, private legal entity or public entity that individually or jointly with another entity processes the information at the request of the owner of the personal data database.

Examples of personal data database processors would include IT service providers that perform software or hardware maintenance, a company that provides postal mailing services, a call centre that promotes or sells products of another organisation, among others.

The main obligations under the Persona Data Protection regime are the following:

Obtain Consent

Owners of a personal data database must obtain the consent of the owner of the personal data intended to be processed, subject to the exceptions provided for in Article 14 of Law 29733. The most important exceptions referred to under current legislation are the following:

- when personal data is collected or transferred in response to the exercise of functions of public entities acting within the scope of their powers (eg, when the consumer protection agency requests a business' client list);
- in the case of personal data contained or intended to be contained in sources accessible to the public (eg, information contained in the telephone directory, newspapers, magazines, etc);
- when the personal data is necessary for the execution of a contractual relationship to which the personal data owner is a party (eg, when the e-mail address, mailing address or phone number of a customer is used to comply with certain purposes of the contract or send monthly billing statements);
- when an anonymisation or dissociation procedure has been applied. An anonymisation procedure is an irreversible processing of personal data which prevents identification or does not make the identity of the data subject identifiable. A dissociation process involves a reversible

processing of personal data which prevents identification of the data subject.

Adopting Safety Measures
With the purpose to ensure the security of personal data, owners of personal data must embrace technical measures to prevent unauthorised access, alteration, loss, processing or unauthorised access. The levels of safety measures in place ought to be in accordance with the prescriptions of the Regulation.

Allow the Exercise of the Personal Data Owner's Rights
The personal data database owner must allow the exercise of the following rights granted to owners of the personal data:

- right to information (regarding the purposes of the processing) and right of access to the provided data;
- right to update, include, rectify, revoke and delete data; and
- right to prevent the supply of data to third parties when it affects their fundamental rights and right of opposition to the processing with objective justifications.

Duties of the personal data database processor before the personal data owner
The processors of personal data databases are forbidden to process information compiled for purposes that have not been authorised by the owner of the personal data.

Likewise, the processors employed must comply with the obligations to adopt the necessary measures to ensure safety in the processing of information, maintain the confidentiality of the personal information being processed and enable the exercise of the personal rights of the owners of the information.

Transfers of Personal Data
The transfer of personal data implies the transmission or supply of personal data to third parties (eg, a private legal person, a public entity or an individual other than the personal data owner), inside or outside the country.

Thus, for example, the exchange of databases of customers between related companies for commercial purposes constitutes an act of transfer. Similarly, the acquisition of a database of potential customers from a third party for purposes of marketing activities constitutes an act of transfer.

The transfer of personal data is deemed a modality of processing and, as such, any transfer of personal data requires the free, prior, express and unequivocal, and informed consent of the personal data owner, except those performed under the exceptions to which we have referred.

The transferee of the personal data has the burden of demonstrating that the transfer was performed in accordance with regulatory requirements. The recipient of personal data assumes the condition of personal data database owner and must process the personal data in accordance to the information provided by the issuer to the data subject.

The trans-border flow of personal data is only possible when the recipient assumes the same obligations that correspond to the owner of the personal data database. To ensure this, the issuer may execute contracts or other instruments permitted by law.

Transfers of personal data between companies that are under common control (ie, business groups, subsidiaries and related companies) guarantee the proper processing of personal data if such companies have adopted a code of conduct laying down internal rules for the protection of personal data.

National Register of Personal Data Protection
The Law imposes the obligation to register personal data databases to ensure their publicity and facilitate the exercise of the rights that the law recognises to data subjects that have been alluded to previously.

The National Register for the Protection of Personal Data, in charge of the National Authority for the Protection of Personal Data (the 'Personal Data Authority') of the Ministry of Justice and Human Rights, has been created for these purposes.

Sanctions
The Personal Data Authority may impose fines (up to approximately USD125,000) on those who fail to comply with the provisions set forth in Peruvian data protection legislation.

The procedures to sanction breaches of the Law and the Regulation are initiated ex officio, at the request of the Directorate of Supervision and Control of the National Authority of Personal Data or by complaint of an affected party.

Fining procedures will have two instances. In the first instance the competent authority will be the Direction of Sanctions, which will be responsible for instructing the procedure and issuing the initial fining decision. These decisions are subject to review on appeal by the General Directorate.

7. Monitoring & Limiting of Employee Use of Computer Resources

7.1 Employees' Restrictions on Computer Use
There is no specific regulation regarding monitoring and limiting the employee's use of the company's computer resources.

Thus, companies usually implement internal policies to regulate the use of their computer resources (eg, corporate e-mail). However, certain decisions of the Constitutional Tribunal and Supreme Court have established that those regulations and any other action of the employee that aims to supervise or monitor such resources are legal and valid as long that they don't infringe the right to privacy of the employee.

8. Scope of Telecommunications Regime

8.1 Technologies within Local Telecommunications Rules

According to the Peruvian telecommunications framework (General Law of Telecommunications and its Regulation, approved by Supreme Decree 13-93-TCC and Supreme Decree 20-2007-MTC respectively), telecommunication services are classified as public utility services, private services and private services of public interest:

- public utility services are rendered to any kind of third parties in exchange of a consideration;
- private services are rendered to satisfy own needs (ie, they are not rendered in favour of third parties); and
- private services of public interest are basically television and radio broadcasting.

Likewise, telecommunication services are classified – from a technical perspective – as follows:

- *carrier service* – provides with capacity for transmission of signals allowing the rendering of final services, broadcasting services and value-added services. These services are necessarily deemed as public utility services. For purposes of rendering carrier services, a single concession of telecommunications is required;
- *final service* – provides with complete capacity for the communication between users. Examples of final services are fixed telephony services, mobile services, radio trunking, mobile satellite services etc. These services could be private or public utility services. For purposes of rendering final services, the following is required:
  (a) a single concession in the case of public final services; or
  (b) an authorisation, permit or licence in the case of private final services, as the case may be.
- *Broadcasting service* – provides for one-way point-multipoint communications. These services could be public utilities or private services. For purposes of rendering broadcasting services, the following is required:
  (a) a concession in the case of public broadcasting services (eg, cable TV); and
  (b) an authorisation, permit or licence in the case of broadcasting services which are not considered public utility services, as the case may be.
- *value-added service* – is supported on carrier services, final services and/or broadcasting services and adds a specific characteristic on such telecom services. Examples of value-added services are fax and Internet access, among others. For purposes of rendering value-added services, a registration before the Ministry of Transportation and Communication (MTC) is required.

Most types of technologies which are used by mobile or Internet services (as voice-over-IP and instant messaging) are not under the scope of telecommunications regulation. This applies to RFID tags (in this case only the equipment which support these technologies are subject to approval by the MTC).

Finally, concessions, authorisations, permits and licences for rendering telecommunication services in Peru are granted by the MTC. Peruvian telecommunication regulation provides for scenarios where such concessions, authorisations, permits and licences are granted:

- *single concession* – entitles entities to render public utility services. In the case of rendering public value-added services, no concession would be needed except for prior registration with the MTC.
- *authorisation* – entitles entities to render telecommunication services for the operation of radio-communication equipment without a concession.
- *permit* – entitles entities to install telecommunication equipment in a specific area.
- *licence* – entitles entities to operate a broadcasting service which is not a public utility service.

9. Audiovisual Services and Video channels

9.1 Main Requirements

Television or Radio Services

To provide television or radio broadcasting services of an educational, commercial or community type it is necessary to obtain an authorisation granted through a resolution of the Vice Ministry of Communications at the request of a party or via public tender. It should be noted that only companies constituted or domiciled in Peru are permitted to be holders of such authorisations (Article 24 of the Radio and Television Law, Law 28278).

When applying for an authorisation, pursuant to Article 29 of the Regulation of Radio and Television Law, legal entities must submit the following information: the identity document number of the legal representative and certificate of their status as shareholder, partner or associate; information in relation to the corporate or shareholder composition of the company indicating its participants and their data that must be delivered by themselves or by the legal representa-

tive for reasons of force majeure; technical and financial documents as well as the communication project indicating, in a generic way, the type and characteristics of the television programming.

Investment of foreigners in companies holding licences to provide radio and television services in Peru is subject to the Principle of Reciprocity. This implies that the participation of a foreign investor in such activities will be admissible, under the same conditions in which the investment of Peruvian capital in the same activity in the investor's country of origin would be admissible.

Authorisations are obtained by location and have a maximum validity period of ten years beginning with a period of twelve months for installation and testing. Also, operation of the radio or television service requires a payment for processing rights to obtain the authorisation and, once obtained, a payment of the annual fee for use of the spectrum.

Cable TV

To provide a public telecommunication service as a cable TV channel operator, pursuant to the General Law of Telecommunications and its Regulation (Article 144), an investor is required to obtain a single concession, which involves the submission of the following supporting information:

- personal data of legal representatives and shareholders of the company;
- not be impeded by sanction to contract with the State;
- have a share capital of more than USD12,000;
- a technical profile of the service which will be provided;
- projected investment for the first five years; and
- a letter of guarantee to ensure the investment in case the service includes Lima or Callao.

It should be noted that in the case where an investor owns a television channel and intends to transmit it via a paid service operator (cable TV), any authorisation or permit will not be necessary.

Video Channels and OTT Content

As stated by the regulatory agency of telecommunications OSIPTEL, in Resolution No 063-2017-CD/OSIPTEL, under the Peruvian legal framework OTT services and any video channel services or platforms broadcast via the Internet are not regulated.

However, since the General Law of Telecommunications establishes a broad definition of telecommunication services, the possibility that the agency may extend its regulations to OTT services in future cannot be ruled out.

Moreover, companies must comply with the provisions of the applicable Copyright Law (Legislative Decree 822), which indicate the parameters that must be respected in the development of any company that is dedicated to transmitting audiovisual content that is protected by copyright. In this way, the transmission of audiovisual works in analogue or digital form is considered an act of public communication, and therefore it is necessary to have the author's authorisation to do so.

10. Encryption Requirements

10.1 Legal Requirements Governing the Use of Encryption

Encryption matters are regulated only in relation to the use of digital signatures, while other uses are not under specific regulation. Use of electronic and digital signatures is regulated by Law 27269.

Article 3 of Law 27269 defines a digital signature as "that electronic signature that uses an asymmetric cryptography technique based on the use of a single key pair; associated with a private key and a public key mathematically related to each other, in such a way that people who know the public key cannot derive the private key from it". It should be noted that although the digital signature is a type of electronic signature, due to its technical characteristics it is endowed with greater security and privacy (unlike other types of electronic signatures, such as digital key systems or intranet). That is why Article 3 of the Regulation of the Law 27269 (Supreme Decree No 052-2008-PCM) gives it the same validity and legal effectiveness as the handwritten signature.

In this sense, only a digital signature can be used validly as a handwritten signature. Other types of electronic signatures are excluded from this feature, so they cannot be used as handwritten signature supplements in legal proceedings.

However, for digital signatures to be admitted validly in procedures and/or legal processes, the Regulation of the Law 27269 has provided that these are issued necessarily within the framework of the Official Electronic Signature Infrastructure. This means that digital signatures must have been granted using a certificate issued by an accredited certification or registration entity, in addition to being used by means of digital signature software accredited before the competent administrative authority (in this case, the agency INDECOPI).

PAYET REY CAUVI PÉREZ ABOGADOS
Av. Víctor Andrés Belaúnde 147
Edificio Real 3,
Piso 12 San Isidro
L 27, Lima - Perú

Tel: +511 612 3202
Email: lexmail@prcp.com.pe
Web: prcp.com.pe