Bruchou & Funes de Rioja

PRIVACY LAW: ARGENTINA

GALA
GLOBAL ADVERTISING LAWYERS ALLIANCE

GALA
GLOBAL ADVERTISING LAWYERS ALLIANCE

"A Global Legal Perspective on Data Protection Relating to Advertising and Marketing."

DÁMASO PARDO CORREA

FRANCO RAFFINETTI

1 PRIVACY LAW

1.1 How is privacy regulated in Argentina?

Privacy rights were incorporated into the Argentine legal system with the 1994 constitutional reform, as the result of the incorporation of the habeas data procedure. Since then, privacy rights have acquired constitutional protection, being considered as fundamental rights that cannot be suppressed or restricted without sufficient cause. In addition, the National Civil and Commercial Code (Section 1770) and several international treaties executed by Argentina have recognized privacy rights as fundamental rights.

In general terms, the Argentine data protection system follows the European legal regime. Moreover, in 2003, the European Union issued a resolution establishing that Argentina had a level of protection consistent with the protection granted by the Data Protection Directive 95/46/EC with respect to personal data, and Argentina continues to hold this status.

1.2 What are the key laws regulating privacy? Please point out national laws, local or state-specific laws, sector-specific laws, and self-regulatory frameworks, with special focus on adverting aspects.

The current legal framework regulating privacy is vast and complex, the main regulations—including those focusing on advertising aspects—are as follows:

(a) Data Protection Law No 25,326 ("DPL");

(b) DPL Regulatory Decree 1558/2001 ("Regulatory Decree");

(c) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108");

(d) Provisions issued by the Access to Public Information Agency ("APIA") (and its predecessor, the National Directorate for Personal Data Protection ("NDPDP"));

(e) Disposition 4/2004, approving the Ethics Code of the Association of Direct and Interactive Marketing ("AMDIA");

(f) Law No 26,951 (the "Do-Not-Call Law"), creating the "Do-Not-Call Registry" and expanding the protection of data owners' rights. This regulation allows a data owner to block contact from companies advertising, selling or giving away products and services. Companies offering products and services by telephonic means must register with the Agency and consult the list of blocked numbers on a monthly basis before engaging in marketing calls. Furthermore, Law No 2,014 of the City of Buenos Aires and Law No 14,326 of the Province of Buenos Aires have created their own do-not-call registries within their jurisdiction;

(g) Resolution 132/2018, providing the current procedure to register databases;

(h) Disposition 18/2015, approving the "Privacy Good Practice Guide for the Development of Apps and Software" which establishes that a privacy policy should be clear and easily accessible for users. In addition, the privacy policy for apps designed for use on phones or tablets must be shown in a useful way for users, bearing in mind the size restrictions that apply to these devices;

(i) Disposition 20/2015, regulating the collection of photos, films, sounds or any other data in digital format through unmanned aerial vehicles or drones;

(j) Disposition 60/2016, concerning aspects of the international transfer of personal data. The transfer of personal data to countries that have not enacted adequate legislation on personal data protection is forbidden. Additionally, this Disposition approves two sets of standard model clauses for data controller to data controller transfers as well as data controller to data processor transfers;

(k) Resolution 159/2018, approving a set of guidelines for binding corporate rules as a self-regulating mechanism available for multinational companies to legitimate international data transfer within their group;

(l) Law No 27,275, creating the APIA as its controlling authority. The APIA—which is autarchic and independent—is currently responsible for the application of the DPL and the Do-Not-Call Law; and

(m) Resolution 14/2018, setting out the information which owners and users of public and private databases have to include on their websites, as well as in any other communication or advertising, that guarantees the data subjects' knowledge of their rights and how to exercise them.

1.3 How is privacy law enforced? Please address both regulators and self-regulatory bodies.

The NDPDP, part of the National Department of Justice and Human Rights, was the data protection authority since it was formed in 2001. However, Emergency Decree 746/2017 replaced it with the APIA.

Among other responsibilities, the APIA is responsible for:

(a) operating a registry of databases (keeping records of the registration and renewal of databases);

(b) enforcing the DPL and the Do-Not-Call Law, carrying out inspections and imposing sanctions; and

(c) creating new dispositions and regulations related to data protection matters.

The APIA is also responsible for ensuring the effective exercise of the right of access to public information and the enforcement of transparency within the public sector.

The APIA's inspections/audit proceedings can be ex officio or initiated upon a complaint. The administrative process that the APIA must follow to investigate and impose penalties is set out in the DPL, the Regulatory Decree and in Decree 1160/2010. Administrative decisions can be appealed before the judicial courts.

In addition to the APIA, there are specific regulators for certain industry sectors, such as the Argentine Central Bank ("BCRA") which regulates data handled by financial institutions. There are also many non-governmental organizations ("NGO"s) exclusively dedicated to data protection matters, but with no enforcement authority, such as: Argentina Cyber Secure (www.argentinacibersegura.org/); Association for the Civil Rights (adc.org.ar/) and Argentina Internet Chamber (www.cabase.org.ar/), among others.

2 SCOPE

2.1 Which companies are subject to privacy law in Argentina?

The DPL applies to individuals or legal entities carrying out the processing of personal data of Argentinean residents, regardless of where such processing is performed.

Pursuant to the DPL, the registration of databases is a legal duty which is mandatory for all local data controllers and data processors.

2.2 Does privacy law in Argentina apply to companies outside the country? If yes, are there specific obligations for companies outside the country (eg, requiring a company representative in the country)?

Yes, companies outside the country that process data of Argentinean residents must comply with local law and regulations.

3 PERSONAL INFORMATION

3.1 How is personal information/personal data defined in Argentina?

"Personal data" is defined by the DPL as any type of information that relates to identified or identifiable individuals or legal entities.

3.2 What categories of personal information/personal data are considered sensitive (eg, children, biometric, health, video, geo-location, financial)? Are there specific obligations around sensitive information?

"Sensitive data" is defined in Section 2 of the DPL as any personal information revealing racial or ethnic origin, political views, religious beliefs, philosophical or moral stands, union affiliations or any information referring to the health or sexual life of an individual. As a general principle, sensitive data collection, processing and/or treatment is forbidden unless expressly authorized by law.

Section 7 of the DPL states that individuals cannot be compelled to provide sensitive data. Moreover, sensitive data can only be collected and/or treated in cases where there are circumstances of general interest authorized by law, or for statistical or scientific purposes, provided that data owners cannot be identified. Section 7 also provides that it is prohibited to create files, banks or registers storing information that directly or indirectly reveals sensitive data. Notwithstanding, the Catholic Church, religious associations, and political and labor organizations are entitled to keep a register of their members.

Data referring to criminal records can be treated only by the competent public authorities, within the framework established by the corresponding laws and regulations.

Furthermore, Section 8 of the DPL provides that public or private health institutions, as well as medical science professionals, are entitled to collect and treat such personal data as relate to the physical or mental condition of patients who make use of their services, or who are or have been in their care, in pursuance of the principles of professional confidentiality.

3.3 What are the key privacy principles that companies need to follow regarding their processing of personal information/personal data (eg, transparency, choice, purpose limitation)?

By Sections 4 and 10 of the DPL, the following fundamental principles apply to data processing, namely:

(a) Personal data collected must be true, adequate, relevant, and not excessive in relation to the scope and purpose for which the data has been obtained.

(b) The collection of personal data cannot be done by unfair or fraudulent means.

(c) Personal data subject to treatment cannot be used for purposes different from or incompatible with those purposes for which it was collected.

(d) Personal data must be stored in such a way as enables data owners to exercise their right of access.

(e) The data must be destroyed once it has ceased to be necessary or relevant to the purposes for which it has been collected.

(f) Those responsible or involved in any part of data processing are bound by the duty of confidentiality.

4 ROLES

4.1 Does privacy law assign different roles to companies based on how they process personal information/personal data (eg, controller versus processor)? If so, how do these roles affect obligations and contractual requirements?

No.

5 OBLIGATIONS

5.1 Please summarize the key obligations required by privacy law, with special focus on advertising (eg, posting a privacy policy, keeping records of processing operations, appointing a privacy officer, registering with a privacy authority, conducting risk impact assessments).

All marketing communications in Argentina must include:

(a) information to recipients on their right to request their exclusion from the relevant database;

(b) an opt-out mechanism; and

(c) two legal transcriptions (in Spanish).

Unsolicited communications or those sent without consent must evidence their marketing nature in a noticeable manner. For emails, their subject field must read “Advertisement” and cannot include anything else.

6 DATA SECURITY AND BREACH

6.1 How is data security regulated in Argentina? Is there a minimum standard for securing data? If so, are there any resources to help companies address this standard?

Resolution 47/2018 of the APIA establishes a set of recommended security measures for the processing and conservation of personal data, which include different recommendations in connection with personal data, depending on whether or not the data is stored by electronic means. These aim at ensuring the continuous improvement of the administration, planning and control of information security.

It is important to point out that, whilst previous regulations provided for mandatory security measures, Resolution 47/2018 establishes a set of "recommendations" that can be adopted or not, or even replaced by other more effective measures based on the practices and circumstances of the processing of personal data. Moreover, the Resolution does not impose any particular data storage technological method or solution, allowing database controllers to make their own IT solution decisions.

6.2 How are data breaches regulated in Argentina? What are the requirements for responding to data breaches?

In Argentina, the obligation to report data security incidents is not legally established. Under the DPL, there is no specific legal obligation to report data breaches to authorities. Such an obligation has not been regulated and has not been established by any particular reports to the authorities or the affected individuals.

It is worth mentioning that there is a bill, submitted to Congress by the Argentine Executive Power in November 2020, which is intended to amend and replace the DPL, which addresses, in detail, data breach incidents and the proceedings to be followed if they occur, following the EU General Data Protection Regulation ("GDPR").

7 INDIVIDUAL RIGHTS

7.1 What privacy rights do individuals have with respect to their personal information/personal data?

The main rights for data owners contained in the DPL are the right of information, access and erasure. According to Section 14 of the DPL, data owners have the right to request and obtain information on any personal data included in a database. Moreover, the data controller must provide this information within ten calendar days of notification, free of charge. Data subjects can exercise these rights every six months or more, unless a legitimate interest is proven.

Additionally, data owners have the right to request that the rectification, updating or the erasure of their data from databases. The data controller must comply with the request within five days.

8 MARKETING AND ONLINE ADVERTISING

8.1 How are marketing communications (eg, emails, texts, push notifications) regulated from a privacy perspective?

(a) By Disposition 4/2009, all marketing communications in the country must include a notification to recipients of their right to request their exclusion from the relevant database, the way to exercise such right and the transcription of certain legal provisions (in Spanish). In addition, unsolicited communications, or those sent without consent, must evidence their marketing nature in a noticeable manner; when sent through email, their subject must include the term "Publicidad" ("Advertisement"). Companies carrying out direct marketing campaigns must ensure that they implement effective mechanisms to fulfil all potential opt-out requests.

(b) In 2014, the Do-Not-Call Law created the Do-Not-Call Registry, expanding the protection of data owner's rights. This regulation allows the data owner to block contact from companies advertising, selling or giving away products and services. Companies offering products and services by telephone must register with the Agency and check on a monthly basis the list of blocked numbers before engaging in marketing calls.

(c) Resolution 14/2018 establishes that the owners and users of public and private databases must, prior to the collection of the data, clearly and expressly exhibit, in a visible place, the following information, making particular reference to the way in which data subjects may exercise their rights:

(i) the purpose of the data processing,

(ii) any possible recipients of data,

(iii) the existence of the database and the identity of the data controller,

(iv) whether providing the data is mandatory or not, and

(v) rights data owners have.

Likewise, the following wording must be included: "LA AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, en su carácter de Órgano de Control de la Ley No 25.326, tiene la atribución de atender las denuncias y reclamos que interpongan quienes resulten afectados en sus derechos por incumplimiento de las normas vigentes en materia de protección de datos personales" ("THE AGENCY OF ACCESS TO PUBLIC INFORMATION, as the Controlling Authority of Law No 25,326, has the attribution of attending to any claims and allegations filed by those affected in their rights for non-compliance with the current data protection regulation").

These regulations are applicable in all cases of marketing addressed to Argentine residents, irrespective of the country or jurisdiction from which the marketing communications are delivered.

8.2 How is the use of tracking technologies (eg, cookies, pixels, SDKs) regulated from a privacy perspective?

The use of cookies, pixels or other tracking technologies has not been regulated yet, nor particularly addressed in any APIA recommendation. However, applying the DPL's principles, companies trying to obtain information through tracking technologies must obtain the user's consent to collect information.

8.3 How is targeted advertising and behavioral advertising regulated from a privacy perspective?

Targeted advertising and behavioral advertising are not specifically regulated by local law. The regulations described in question 8.1 also apply to these type of advertising activities.

8.4 What type of notice and consent do advertisers need to share data with third parties for customer matching (eg, Facebook Custom Audiences or via LiveRamp)?

The processing of personal data for advertising or marketing purposes, including data sharing, is permitted without prior consent when the data is limited to the creation of consumer profiles that categorize personal preferences and similar types of behavior, and/or when the data owners are solely identified by their belonging to generic groups and the individual data is strictly necessary to market or advertise to the individual (Section 27 of the Regulatory Decree).

8.5 Are there specific privacy rules governing data brokers?

No.

8.6 How is social media regulated from a privacy perspective?

Social media is not specifically regulated. However, general principles arising from the DPL and its regulations and dispositions apply also to social media.

8.7 How are loyalty programs and promotions regulated from a privacy perspective?

Loyalty programs and promotions are subject to the rights and obligations arising from the data protection legal framework.

9 DATA TRANSFER

9.1 Are there any requirements or restrictions concerning data transfer (eg, restrictions on transferring data outside the country or between group companies)?

(a) Section 12 of the DPL forbids any transfer of personal data of any kind to countries or international or 'supranational' organizations that do not grant an adequate level of protection pursuant to the APIA's standards. The list of countries considered as having 'adequate' level protection includes: the member states of the EU and the European Economic Area, Switzerland, Guernsey and Jersey, the Isle of Man, the Faroe Islands, Canada (only private sector), New Zealand, Andorra, Uruguay, Israel (automated data treatment only) and the UK.

Such prohibition does not apply where:

(i) the data subject has given express consent, by authorizing the international transfer of their personal data (including to countries not granting "adequate levels of protection"), or

(ii) an adequate level of protection arises from contractual clauses or self-regulation systems of the data assignor and data assignee (such as binding corporate rules, global policies or codes of conduct).

(b) Disposition 60/2016 has also approved two sets of standard model clauses for data controller to data controller transfers as well as data controller to data processor transfers. These models are based on the EU Model Contracts for the transfer of personal data to third countries.

(c) Furthermore, Resolution 159/2018 issued by the APIA sets out 'Guidelines and Basic Contents of Binding Corporate Rules' for the international free flow of personal data among companies of the same economic group. The guidelines are aligned with Section 47 of the GDPR, addressing issues such as basic conditions for the legality of the transfer, procedures to ensure data subjects' rights, joint liability of parties, applicable jurisdiction in case of controversies and APIA auditing rights.

Argentine companies transferring personal data to affiliates in countries without 'adequate' personal data legislation, based on corporate rules other than those established by Resolution 159/2018, must submit them to the APIA for its approval.

9.2 Are there any other issues companies need to consider when transferring data (eg, privilege issues when transferring data between group companies)?

As mentioned in question 9.1, Disposition 159/18 sets out guidelines for companies to draft and implement binding corporate rules or 'BCRs', which regulate intra-group international transfers of personal data.

Local law and regulations encourage companies to implement a privacy policy which regulates their personal data collection, treatment and processing and security mechanisms. The APIA can request company's privacy policy and BCRs upon inspections.

10 VIOLATIONS

10.1 What are the potential penalties or sanctions for violations of privacy or data security law?

Penalties are established in Sections 31 and 32 of the DPL and in the Regulatory Decree. The APIA may apply sanctions for any violations of the Argentine data protection legal framework. The sanctions can include warnings, suspensions, fines and closure or erasure of the database, without prejudice to any applicable civil or criminal liabilities. There are precedents for the authority fining companies which fail to comply with the data protection legislation, although such fines are usually low.

In addition, Section 157 of the Criminal Code provides that imprisonment of between one month and two years may be imposed on any person who:

(a) knowingly and unlawfully, or by violating data confidentiality and security systems, accesses a personal database;

(b) unlawfully provides or discloses to third parties information registered in a personal database that should be kept confidential by provision of law; or

(c) unlawfully inserts data in a database.

Penalties imposed by Sections 117 and 157 of the Criminal Code will be increased if the perpetrator is a public officer.

10.2 Do individuals have a private right of action? What are the potential remedies?

Anyone with a legitimate interest—individual or company—may file an administrative claim before the APIA. The APIA may also start a preliminary investigation *ex parte*. Pursuant to the regular process set out in the Administrative Proceedings Regulation, administrative decisions can be appealed before the judicial courts.

11 MISCELLANEOUS

11.1 Are there any rules that are particular to the culture of Argentina which affect privacy?

No.

11.2 Are there any hot topics or laws on the horizon that companies need to know?

(a) In 2020, lawmakers of the main opposition party introduced a new bill ("Bill") in the Lower Chamber, intended to replace the DPL which was enacted in 2000, and has become outdated in relation to technological and legal developments, especially following the passing of the GDPR.

The Bill introduces new definitions aligned with the EU regulation, and that of Brazil, such as the concept of database, personal data and sensitive data. At the same time, the Bill introduces new concepts regarding genetic data, biometric data, economic groups, security incidents and international transfer. Also, it limits the scope of the concept of data subjects to human persons.

Among other changes, the Bill introduces new grounds for the collection and processing of personal data other than consent, such as legitimate interests; the obligation to report any security incident to the controlling authority and to data subjects; and increases exponentially the penalties for infringements.

(b) In March 2022, Argentina's president confirmed the appointment of a new Director of the APIA, a post which had been vacant since January 2021.

The new Director has stated that the 4 central axes of her work plan for the APIA are:

(i) Institutional strengthening of the APIA;

(ii) Quality improvement in active transparency and open data;

(iii) Updating regulations and reinforcing the management of personal data protection; and

(iv) Consolidation of the Federal Council for Transparency.

Regarding the updating of regulations, the Director highlighted that there is a broad understanding of the need to update the DPL. In this sense, she proposed analyzing the EU GDPR and regional best practices, such as the Brazilian law. In any case, she affirmed that, in parallel to the promotion of a draft law, concrete and incremental decisions and resolutions will be taken to address the broad range of personal data protection challenges.

11.3 Is there any other information not covered in this chapter that companies need to know, including general advice or cautions around processing personal information/personal data in Argentina?

No.

12 OPINION QUESTIONS

12.1 What changes in the privacy landscape have you observed over the past few years? In your opinion, what propelled/triggered these changes?

The global privacy landscape is constantly changing. Data is regarded as power and even considered as the new commodity; at the same time, data subjects and regulators are increasing demanding data privacy to avoid personal data violation. The global scenery drives Argentina to the imminent enactment of a new law, in line with the GDPR.

12.2 What do you envision the privacy landscape will look like in 5 years?

Recent administrative changes in the APIA, together with expected legislative changes, along with the Bill, which is aligned with GDPR, may lead to a different scenario in the upcoming years.

It is expected that local law and regulations will be aligned with international standards and the principles established by the GDPR.

12.3 What are some of the challenges companies face due to the changing privacy landscape?

In the current changing privacy landscape, companies' challenges will be aligned with the ones they are now facing in the EU.

GALA

GLOBAL ADVERTISING LAWYERS ALLIANCE

28 Liberty Street, 35th Floor, New York, NY 10005

Tel: 212.705.4895 | Fax: 347.438.2185 | Email: sbess@galalaw.com

www.galalaw.com