Privacy International's submission Argentina's draft law on the protection of personal data, 2022

September 2022

ABOUT US

Privacy International (PI) welcomes the opportunity to respond to this consultation on the proposed data protection bill to reform the current law 25.326.

PI is a registered charity based in London that works at the intersection of modern technologies and rights. We regularly examine how company practices impact individual privacy and autonomy, especially where the use of data and technology is concerned. We campaign for strong regulations and better protections for the public.

We are frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and have advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

CONTACTS

Alexandrine Pirlot de Corbion
Director of Strategy
alex@privacyinternational.org

Lucie Audibert
Lawyer and Legal Officer
luciea@privacyinternational.org

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

INTRODUCTION

Privacy is a fundamental human right. Protecting privacy in the modern era is essential to effective and good democratic governance. This is why data protection laws exist in over 145 countries worldwide including various countries in Latin America,[1] and instruments have been introduced by international and regional institutions such as the the OECD,[2] Council of Europe,[3] and the Red Iberoamericana de protección de datos.[4]

Privacy International welcomes the continued efforts by Argentina to provide protections for the right to privacy, already enshrined in the Constitution of Argentina. PI welcomes the main aim of the draft law for protection of personal data ("the Bill"), namely to regulate the processing of personal data in order to guarantee fully the exercise of data subjects' rights in accordance with Article 43 of the Constitution (Article1 of the Bill).

Privacy International notes the advances made in the Bill to include protections for personal data to reflect the new challenges and opportunities that result from the data-driven ecosystem we live in, with the inclusion of provisions on cloud computing, automated decision-making including profiling, credit ratings and services and innovative marketing.

Based on our experience of working on privacy for over 25 years, our expertise on international principles and standards applicable to the protection of personal data, our leadership and research on modern technologies and data processing, Privacy International wishes to make a number of observations and recommendations on the draft law (these are non-exhaustive and are intended to highlight our main concerns).

CAPÍTULO I DISPOSICIONES GENERALES

ARTÍCULO 1 - Objeto

Privacy International welcomes the direct reference to the Constitutional protection of the rights of individuals under Article 43(3) of the Constitution and the reference to Argentina's international human rights treaties to which it is a signatory.

[1] See Graham Greenleaf, Now 157 Countries: Twelve Data Privacy Laws in 2021/22 (2022) 176 Privacy Laws & Business International Report 1, 3-8, UNSW Law Research. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4137418
[2] See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013, available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonald ata.htm
[3] See the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 1981, available at http://conventions.coe.int/Treaty/en/Treaties/html/108.htm
[4] See the non-binding Iberoamericana Network 'Estandares de Proteccion de Datos Personales Para Los Estados Iberoamericanos' available at: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

ARTÍCULO 2 - Definiciones

Clear definitions are essential to a strong and accessible law, and Privacy International welcomes the inclusion of new and/or updated definitions in this Bill. However, Privacy International has the following observations as to how these definitions could be strengthened:

Anonymisation – 'Anonimización'

This definition does not make clear that pseudonymised data does not constitute anonymised data. While pseudonymisation is defined later in Article 2, the concept is not used anywhere else in the legislation, and nowhere is made clear that pseudonymised data constitutes personal data. The definition of Anonymisation should therefore specify that pseudonymised data does not constitute anonymised data. In addition, Article 3 ('Ambito de aplicación material de la Ley') should specify that the law applies to pseudonymised data.

Data protection authority - 'Autoridad de aplicación"

In light of Article 50 which provides for and upholds the autonomous or independent quality of the competent supervisory authority, Privacy International recommends revising the wording of this definition to reflect this, to read as follows: "Autoridad de aplicación autónomo".

Personal data - 'Datos personales'

This definition does not address the question of identifiability sufficiently, specifically indirect identifiability. It is essential that the definition recognise that personal data should include data that combined with other data relates to an identifiable individual. It should also give explicit recognition to online identifiers (this could be IP addresses, cookie IDs, advertising IDs) as well as location data, amongst other types of data commonly known as metadata.

Sensitive data – 'Datos sensibles'

Privacy International welcomes the inclusion of the categories of sensitive data already identified in the Bill. We would suggest adding reference to data pertaining to the commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Lending institutions – 'Entidades crediticias'

We find the definition of 'entidades crediticias' very limiting given that there is a whole new industry of lending companies which are not part of the formal financial/banking system. Our research has raised concern that this emerging industry is left unregulated.[5] These companies should be subject to the same data protection and security obligations as traditional financial institutions to ensure that the international nature of their operations is not being used as a loophole to evade regulation. We would also request that this definition clarify its application to all credit referencing agencies.

ARTÍCULO 3 - Ambito de aplicación material de la Ley

Privacy International welcomes the explicit recognition of the protection of journalistic sources and the right to freedom of expression. It is important that the law is used to strengthen as opposed to undermine all fundamental rights. Data protection and freedom of expression should not be seen as incompatible, as this is often the contrary. Data protection and privacy are essential enabling rights for freedom of expression - for example, journalistic sources will be better protected if strong data security measures are implemented, and individuals will be freer to speak if their personal data is not collected and analysed every time they do so. Given that this article would mean that the law does not apply at all (as opposed to an exemption to certain provisions) further details or at the very least guidance should be provided as to how this applies in practice to ensure that rights are truly upheld.

We welcome the amendment made to the scope of application of the law to include the Army, security and intelligence agencies and forces.

In addition, this article should specify that the law applies to pseudonymised data.

CAPÍTULO II TRATAMIENTO DE DATOS PERSONALES

We welcome the inclusion of the key data protection principles as follows:

- Principle of Fairness, Lawfulness, and Transparency
- Principle of Purpose Limitation
- Principle of Minimisation
- Principle of Accuracy
- Storage Limitation
- Principle of Accountability

[5] See Privacy International's research on Financial Privacy, including our report 'Fintech: Privacy and Identity In the New Data-Intensive Financial Sector", available at: https://privacyinternational.org/topics/financial-privacy

We also welcome the list of lawful bases for processing as follows:

- Consent
- Performance of a public function
- Compliance with a legal obligation
- Performance of a contract
- Vital interests of the data subject
- Legitimate interests of the controller

Below we set out some outstanding concerns in relation to these principles and lawful bases for processing.

ARTÍCULO 7 - Principio de finalidad

The inclusion of the principle of purpose limitation is important. However, the current text of the Bill allows for the further processing of personal data "for archiving purposes in the public interest or scientific, statistical or historical purposes." It is unclear what those statistical and scientific purposes are and there is no condition that such purposes be in the public interest. This provision should at least be subject to a number of safeguards such as requiring compliance with the principle of data minimisation, mandating anonymisation where the purposes described in this article can be fulfilled in that manner, and mandating pseudonymisation where they cannot.

ARTÍCULO 10 – Plazo de conservación

As with Article 7, further limitations and safeguards should be added for the situations where personal data is to be kept indefinitely for archiving purposes.

ARTÍCULO 12 - Bases legales para el tratamiento de datos

With regards to Article 12 (f), the definition of legitimate interests may be too vague and open to abuse by controllers who are unable to rely on other lawful bases. Indeed, since the coming into force of the General Data Protection Regulation (GDPR) in the EU, controllers have liberally relied on this lawful basis to perform personal data processing when it enabled them to market their products or services or to make profit out of the processing, with minimal or no consideration for individuals' fundamental rights and freedoms. We would recommend that this article include a provision requiring controllers who rely on this lawful basis to publish and/or to provide, upon request by a data subject (i.e. not only upon request by the data protection authority), a copy of the legitimate interests assessment they performed.

ARTÍCULO 16 - Tratamiento de datos sensibles

The definitions of the following terms "el interés vital" in subsection (b), |finalidad histórica, de archivo de interés público, estadística o científica" in subsection (f) and "asistencia humanitarian" in subsection (i) need to be further qualified to prevent abuse.

In relation to subsection (a), the consent condition for processing of sensitive data does not establish a sufficiently high threshold for consent. Given the heightened risks to data subjects when their sensitive data is processed, this condition should require explicit consent – which requires that consent is affirmed in a clear statement (as opposed to just a clear affirmative action). Explicit consent cannot be inferred from someone's actions.

In relation to subsection (g), processing of sensitive personal data in the application of labour or social security law can have significant consequences for data subjects, in particular where such processing can lead to the denial of certain social benefits. This condition should therefore require authorities to demonstrate they have applied appropriate safeguards for preserving the fundamental rights and the interests of the data subject in such processing.

In relations to subsection (h), this condition for processing is not sufficiently bounded. Processing of sensitive data by authorities of the State can profoundly threaten the rights and freedoms of data subjects if sufficient safeguards are not established.

ARTÍCULO 17 - Tratamiento de antecedentes penales y contravencionales.

We are concerned by the lack of safeguards this provision provides in particular given that this sort of data has not been included in the definition of 'sensitive personal' data as we noted above. Even where such data is processed by or under the supervision of public authorities, protections must be in place. This is extremely important given the sensitive nature of this data.

ARTÍCULO 20 - Notificación de incidentes de seguridad

Privacy International welcomes the inclusion of Article 20 which provides an obligation on the data controller to inform the data subject of a security incidents as it relates to their personal data.

The current provisions limit this obligation to cases whereby the security breach implies high risks ("altos riesgos") for the rights of the data subject. The Bill does not provide sufficient detail as to what would constitute high risks. Privacy International suggests that further detail be provided in the Bill itself to enable the assessment of what constitutes high risks

for the rights of the data subject and/or requires the independent data protection authority to develop key guidance to support this impact assessment of a breach.

CAPÍTULO 3 TRANSFERENCIAS INTERNACIONALES

ARTÍCULO 23 - Transferencias internacionales basadas en una decisión de adecuación

This list is a good starting point. However we would recommend that the Bill requires an adequacy decision to reflect on the international commitments of the receiving entity, their other obligations under legally binding conventions or instruments, or their participation in multilateral and regional systems.

This provision also needs to include a monitoring process to identify any developments that would affect the adequacy decisions, and if the level of adequacy is no longer guaranteed, take steps where necessary to revoke, amend or suspend the decision until the situation is rectified.

ARTÍCULO 25 - Excepciones

We are concerned by the following provisions:

- paragraph (a): the threshold for relying on consent for international transfers is too low. This condition should require explicit consent, and require that the data subject has been informed of the possible risks of such transfer due to the absence of an adequacy decision and appropriate safeguards;
- paragraph (b): even where the data subject enters into a contract which requires international transfers, there must be safeguards in place;
- paragraph (c): interpretation as to what public interest is left open.

CAPÍTULO 4 DERECHOS DE LOS TITULARES DE LOS DATOS

Privacy International welcomes the inclusion of articles 26-33 which provide for the rights of data subjects. We stress however that the burden should be on the data controller to facilitate the exercise of these rights and the authority should provide relevant guidance.

ARTÍCULO 26 – Derecho de acceso

Further guidance should be provided as to what is meant by asking the data subject to provide 'previa acreditación de su identidad'. Whilst it is important that people's personal data is not disclosed to others in error, this requirement should not be used to undermine individual's ability to exercise their rights.

ARTÍCULO 28 - Derecho de oposición

This article enables a data controller to refuse to comply with a data subject's right to object should there be "legitimate grounds". However, we would like to stress once again that the onus must be on the data controller to provide evidence for the need to continue processing the data of that individual, with reasons which override the interests, rights, and freedoms of that individual. Clarity must be provided on what constitutes "legitimate grounds", and on balance and if in doubt the interests and rights of the individual should prevail. Should the data controller not comply with this request, the individual should be provided with an explanation and have the right to further challenge such a decision.

ARTÍCULO 29 - Derecho de supresión

Some of the exceptions included in this provision are very broad and need to be defined further such as for "public interest" or "legitimate interest" of third parties, as well as wider historical and archiving purposes, and for the process of "memory, truth and justice". Further guidance on what this constitutes would help ensure interpretation of these vague terms does not curtail data subjects' rights in arbitrary and discriminatory ways.

ARTÍCULO 31 - Derecho a la portabilidad de datos personales

Further guidance is needed on this right so that the exemptions in paragraphs a) to d) are not abused.

There is an exemption that this right to does not apply to data "*inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento*" which may open a loophole to distinguish between data provided by the data subject compared to data inferred, derived, created, generated, or obtained through analysis.

ARTÍCULO 32 - Ejercicio de los derechos

We are pleased that the exercise of data subjects' rights is free and welcome the 10-day period in which the requests to exercise rights must be responded to and fulfilled.

We note the provision regarding the rights of individuals who have passed away, if the law is intended to apply to the deceased then this requires consideration and clarity.

We are concerned by the provision that there must be 6 months intervals in between each free access request of a data subject unless new reasons are provided by the data subject for their additional requests, and that the Data Controller will be able to charge data subjects for the processing of their requests. The exercise of these rights should not come at a cost to the data subject. This financial burden may deter data subjects from exercising their rights, and this would likely further impact those already in a marginalised position that may be disproportionally affected by invasive data processing practices.

ARTÍCULO 33 - Excepciones

Privacy International is concerned by the possible broad interpretation of exceptions in Article 33 in particular given the lack of definition and scope of what constitutes the following terms: "*la seguridad pública, la defensa de la Nación, la protección de la salud pública, de los derechos y las libertades de terceros y en resguardo del interés público.*"

In addition to the listed requirements to justify the curtailment of data subjects' rights provided for in this article, Privacy International would also recommend the independent competent supervisory authority to develop relevant guidelines for each of those exceptions.

CAPÍTULO 5 OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

ARTÍCULO 39 - Evaluación de impacto relativa a la protección de datos personales

Privacy International welcomes the introduction of the requirement of an impact assessment when a type of processing is likely to result in a high risk of harm to the rights of data subjects. We note that this article contemplates the authority establishing other cases where impact assessments will be mandatory. This would be a positive development and the authority should also promote impact assessments as best practice across the board, regardless of the level of risk identified prior to processing. Further consideration should be given to making impact assessments available to individuals who are subject to the processing.

One concern remains as the requirement only applies where a high risk to the rights of data subjects is identified, rather than to the rights of any natural persons. Indeed, any large-scale processing operation may have consequences for individuals beyond the data subjects whose data is concerned by the processing. Hence we would recommend that this Article be amended to require an impact assessment where a type of processing is likely to result in a high risk of harm to the right of natural persons.

There are many risks associated with storing the very information that an individual's identity is in part composed of. The misappropriation of this information can deny individuals their identity and lead to limits on personal freedom. Furthermore, the processing of such data raises concerns about discrimination, particularly in environments prone to social sorting. It is thus imperative that the processing of such personal data be robustly overseen and managed by this Bill.

ARTÍCULO 43 - Delegado de Protección de Datos

Privacy International welcomes the inclusion of this provision, but would nevertheless request adding a requirement that the name and contact details of the data protection officer be publicly available and submitted to the independent supervisory authority. It is also important that independence of Data Protection Officers is protected.

CAPÍTULO 7 AUTORIDAD DE CONTROL

ARTÍCULO 43 - Delegado de Protección de Datos

An initial version of the proposed law provided for the establishment of an independent data protection authority, the Agencia Nacional de Protección de Datos Personales (ANPDP).

However, the Argentinian Data Protection Authority has since been brought into the structure of the Access to Information Agency following the passing of a Presidential Decree of Need and Urgency, (which this situation was not), on 26 September 2018 which modified the newly adopted Access to Information Law.

We are concerned that this change will impact the data protection regime in Argentina.

In addition to the powers and functions of the authority provided for within the Bill, should be the ability to issue not just guidance but binding Codes of Conduct.

CAPÍTULO 8 PROCEDIMIENTOS Y SANCIONES

ARTÍCULO 53 - Trámite de protección de los datos personales

This provision should explicitly include provisions for collective redress. The information and power imbalance between individuals and those controlling their personal data is growing and collective complaints would ensure corrective action by organisations processing personal information, which would benefit all those affected.

Provision should therefore be made in the process to allow individuals to be represented by qualified representatives and for certain qualified bodies, such as non-profit groups working in the field of data protection, to make complaints and seek remedies. Such bodies should also be able to bring complaints before the authority, without the mandate of an individual, for example, where they have identified systematic contraventions of the law. This can be particularly important where for example the contravention is complex to identify but affects many individuals, such as with a connected toy or in cases of online tracking.

ARTÍCULO 54 - Resolución

This article fails to include that one outcome could be that a person whose rights are found to have been violated should have a right to compensation for the damage suffered – material or non-material (e.g. distress).

This underlines the need for robust enforcement models to be in place to ensure that any violation can be investigated and acted upon by a relevant authority.

ARTÍCULO 58 - Sanciones

Further consideration should be given to whether the maximum amount of the fine is sufficient to be seen as a threat and thus encourage implementation of the law.