PRIVACY INTERNATIONAL

Submission on Argentina's Draft Law on the Protection of Personal Data, 2018

December 2018

About us

Privacy International was founded in 1990. It is the leading charity promoting the right to privacy across the world. Working internationally through an International Network of partners, Privacy International works, within its range of programmes, investigates how our personal data is generated and exploited and advocates for legal, policy and technological safeguards.

We are frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has 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.

To find out more about privacy and data protection in Argentina, please refer to 'The State of Privacy in Argentina'[1] (last updated in January 2018).

Contacts

Ailidh Callander
Legal Officer, Privacy International
ailidh@privacyinternational.org

Alexandrine Pirlot de Corbion
Programme Lead, Privacy International
alex@privacyinternational.org

[1] Accessible here: https://privacyinternational.org/state-privacy/57/state-privacy-argentina

Overview

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 120 countries worldwide including various countries in Latin America,[2] and instruments have been introduced by international and regional institutions such as the the OECD,[3] Council of Europe,[4] and the Red Iberoamericana de protección de datos.[5]

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")[6], namely to regulate the processing of personal data in order to guarantee fully the exercise of data subjects in accordance with Articles 18, 19 and 43 of the Constitution. (Clause 1 of the Bill.)

In September 2018, the National Executive sent the proposed Bill to the National Congress.[7] The proposed law was directed to the Senate and it will be considered by two commissions: the Commission of Constitutional Affairs (Comision de Asuntos Constitucionales) and the Commission of Rights and Guarantees (Comision de Derechos y Garantías). As the legislative process continues, Privacy International is calling for an open, constructive and consultative process. Privacy International hopes to contribute constructively to the next steps of this process along with the national civil society organisations in Argentina.

Furthermore, Privacy International notes the advances made in the draft law for protection of personal data to include protections for personal data to reflect the new challenges and opportunities that result from the data-driven ecosystem we are seeing emerge, with the inclusion of provisions on cloud computing, automated decision-making including profiling, credit application and services and innovative marketing.

Based on our experiences 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.

While these efforts have positive intentions, a number of concerns ought to be addressed with the aim of strengthening the data protection framework, in particular:

[2] See Graham Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (2017) 145 Privacy Laws & Business International Report, 10-13, UNSW Law Research Paper No. 45available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

[3] 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

[4] 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

[5] 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

[6] The Bill is available at: https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf

[7] You can access the proposed bill here: https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147- 2018_datos_personales.pdf

Further clarity on definitions and concepts

Throughout the Bill there are defined and undefined concepts that require further clarity to ensure the law is implemented in such a way as to protect individuals' data. These are flagged throughout this submission.

Restriction of legal basis for processing (clause 11)

Of particular concern are the broad basis for processing individuals' data, including from public sources ("fuentes de access public irrestricto") and on the basis of legitimate interests ("interés legítimo"). These conditions are open to abuse and require further restriction.

Removal of implied consent ("tácita") (clause 12)

The law distinguishes between explicit and implied consent. Implied consent should be removed, for the reasons set out in this submission.

Strengthening of individuals rights (Chapter 3)

Whilst the Bill provides for a range of data rights for individuals, there are a number of steps that should be taken to strengthen these rights, in particular in relation to automated decision-making and profiling.

Restriction of exemptions (clause 36)

The exemptions provided for in clause 36 of the Bill are too vague and broad and require further clarity, restriction and oversight to ensure people's rights over their data are respected.

More effective sanctions and redress (Chapter 9)

Further consideration should be given to the sufficiency of the sanctions included within the Bill, including the amount of the monetary penalties and also the ability of individuals to seek compensation and of civil society to seek collective redress.

Capítulo I Disposiciones generals

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.

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:

Data protection authority - 'Autoridad de control'

In light of clause 61(2) which provides for and upholds the autonomous or independent quality of the competent supervisory authority (Órgano de control), Privacy International recommends revising the wording of this definition to reflect this, to read as follows: "*Autoridad de control 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.

Whilst Privacy International welcomes the explicit inclusion of biometric and genetic data within the definition of personal data, the data protection authority should provide guidance on what is meant by 'la aplicacion de medidas o plazos deproporcionados o inviables' to identity individuals, and keep this under review. Otherwise there is a risk that this part of the definition can open to abuse, thus weakening the protection of individual's data and their ability to exercise their rights over it.

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.

Biometric data and *genetic data* are included in the definition of 'datos personales' and not listed within the definition of sensitive *personal data.* Privacy International suggests that biometric and genetic data should always be regarded as sensitive personal data, and included within the definition of the term. Consideration should be given to whether any other categories of personal data should be included.

Disociacion de datos

The Bill must be clear on the difference between pseudonymised data (whereby an individual can be re-identified and thus is still personal data) and anonymous data from which an individual cannot be identified. In doing this, consideration must be given that due to advances in technologies, truly anonymising personal data is becoming increasingly difficult.

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.[8] 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.

Source of unrestricted public-access and source of public access – Fuente de acceso publico irrestricto y Fuente de acceso publio restricto

Privacy International is concerned that these two definitions remain quite vague and do not provide necessary detail to identify whether the data being processed is intended to be publicly available, and that the data subject is aware of that categorisation and its implications as it relates to clause 58 in relation to lending information. Privacy International recommends these definitions be further refined to prevent unambiguity and risk of broad or erroneous interpretation of what constitutes publicly accessible data.

[8] 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

This is particularly relevant in light of the increased reliance by law enforcement agencies and companies to social media intelligence. Privacy International has ongoing concerns, for example, at the SOCMINT is a technique law enforcement and other security agencies are increasingly relying upon across the world. To them, it is an inexpensive strategy that they argue has little impact on people's privacy as it relies only on so-called "publicly available" information. This inaccurate representation of SOCMINT fails to account for the intrusive nature of collection, retention, and use of the data. This selective representation has a clear purpose too: it has resulted in this form of surveillance being mostly unregulated or subject to unpublished regulations.

Further, the privacy's implications of monitoring 'publicly available' information on social networking sites should be addressed. The fact that data is publicly available does not suffice for unregulated and un-checked collection, retention, analysis and other processing.

In particular, the collection and use of publicly available social media data without informed public awareness and debate, a clear and precise statutory framework and robust safeguards fall short of standards of protection of the right to privacy and of personal data protection. This is becoming increasingly concerning in light of the development of technologies that can process and aggregate a vast range of data, including personal data, creating profiles of individuals.

ARTÍCULO 3 - Excepciones a la aplicacion 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 countering each other, for example, sources will be better protected if strong data security measures are implemented. Given that this clause means 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.

ARTÍCULO 4 - Ámbito de aplicación

The scope of the Bill acknowledges that personal data travels across borders. The personal data of the individual must be protected, irrespective of whether their data is processed within or outside the territory where they are based. Further clarity on the application of extra-territorial jurisdiction in practice may help avoid any conflict of laws.

Capítulo II Principios relativos al tratamiento de datos

We welcome the inclusion of the key data protection principles which include:

- Fair, Lawful, and Transparent
- Purpose Limitation
- Minimisation
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

ARTÍCULO 5 - Principio de lealtad y transparencia

Privacy International welcomes the inclusion of the two essential principles of Fairness and Transparency. It would be helpful to specify explicitly in this principle that the processing also be "Lawful", this is also covered in clause 11 (Licitud). However, the inclusion should further emphasise that the processing but be complaint with all laws for example, if the processing is discriminatory or interferes with the protection of other human rights it would not be permitted. Together the implementation of these principles should prevent people's data being used in ways they would not expect.

ARTÍCULO 6 - 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."* or where the processing, according to the context, could be reasonably expected by the data subject . It is unclear what those statistical and scientific purposes are and there is no limitation that such purposes be in the public interest. Further consideration should also be given to what could be considered reasonably assumed by the data subject, in terms of further processing and whether this could be open to abuse. At the very least, there should be safeguards such as notification.

ARTÍCULO 9 - Plazo de conservación

As with clause 6, further limitations and safeguards should be added for the situations where personal data is to be kept indefinitely.

ARTÍCULO 11 - Licitud del tratamiento de datos.

This clause covers the situations in which the processing of the data will be lawful.

In relation to clause 11(b) which reads: "*El tratamiento de datos se realice sobre datos que figuren en fuentes de acceso público irrestricto",* for reasons outlined above under definitions, we are concerned that one of the legal grounds for processing personal data be that the data already be public accessible. Just because personal data is publicly available does not mean that the data they hold should be permitted to be used for other purposes than those defined at the point of collection.

We are concerned that paragraph (c) of clause 11 which reads that: "*El tratamiento de datos se realice en ejercicio de funciones propias de los poderes del Estado y sean necesarios para el cumplimiento estricto de sus competencias",* provides a too broad discretion to public authorities to process personal data.

Clause 11(g) provides that a legal ground for processing personal data is legitmate interest of the data controller or a third pary, and reads: "*El tratamiento de datos sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente."* This clause is problematic as it refers to the "legitimate interest"

of the *el responsable del tratamiento", (*data controller) or a third party. Firstly, the proposed Bill does not define what "legitimate interest" means. Given the wide scope of the term legitimate interest it is essential that this condition is qualified. For example, the data controller must also demonstrate that the processing is necessary and proportionate to the legitimate interest pursued and the interests and rights of the data subject must take precedence. In the case of private entities it is important to take into account that they could claim that 'their legitimate interest' is to make profit, and this should not be a legal ground for processing of personal data. Privacy International has raised this issue during the passage of other data protection laws, such as GPDR and highlighted abuse of this basis by industry, for example in data brokers and AdTech companies.[9]

Furthermore, this legal ground should not be accessible to public authorities. Public authorities should not be able to rely on this justification when processing is carried out in the course of the performance of their duties, as a public authority they must identify the public interest and the relevant public task/statutory function.

Finally, we note that processing necessary for the performance of a contract with a data subject is not included this may require further clarification.

ARTÍCULO 12 - Consentimiento

Privacy International remains concerned by the amendment to Section 5 of the current Personal Data Protection Act 25.326 by clause 12 of the Bill. Our concern is based on the following reasons.

We are concerned that this provision provides that the form of consent will depend on the circumstances (*las circunstancias)*, the type of data (*el tipo de dato personal)* and the reasonable expectation of the data subject (*las expectativas razonables del titular de los datos).* This leaves room for various standards of consent, which can lead to confusion and abuse and thus undermine meaningful consent by individuals. This concern is heightened with the introduction of *implied* consent (*consentimiento tácita)* without clear guidance and conditions as to contexts in which implied consent would be sufficient. Consent is a core principle of data protection which allows the data subject to be in control of when their data is processed, and it relates to the exercise of fundamental rights of autonomy and self-determination.

Acknowledging that new environments are emerging with the way data is processed, and some may argue that it is not also practically desirable and/or feasible to obtain consent. However, in this environment, characterised by the continued lack of transparency and accessibility of data protection and privacy frameworks of data controllers, it is increasingly challenging for data subjects to be aware of the data being processed, and whether they have given consent. This reform process provides an opportunity to re-conceptualise and strengthen the concept of consent in the current ecosystem, but this should not result in lowering the level of protection of data subjects, and undermining consent, a core tenant of data protection as recognised by various legal frameworks including the Article 8 of the EU Charter of Fundamental Rights. Article 5 of the Council of Europe Convention 108+ and the standards for personal data protection by the Red Iberoamericana de Proteccion de Datos.

Consent must be freely given, specific, informed and unambiguous or as put in the Ibero-American States standards 'indubitable' and 'inequívoca'. Implied consent, is by its very nature ambiguous and it is unclear

[9] For example, see "Why we've filed complaints against companies that most people have never herad of – and what needs to happen next" https://privacyinternational.org/advocacy-briefing/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and

how these elements will be implemented in practice, and furthermore there is a question as to what other control mechanisms given to the data subject can be enforced such as to revoke consent, as well as right to rectify, delete, etc. The failings of implied consent were recognised during the data protection reform process in the EU, and the text of the GDPR together with guidance adopted by the European Data Protection Board is clear that implied consent does not meet the necessary conditions of consent.

Privacy International recommends that the Bill remove the option for implied consent and include the requirement that the consent be unambiguous, i.e. an "*unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

At the very least, Privacy International suggest that the Bill provides further clarity on what constitutes "suficiente" when assessing the behaviour of the data subject to ensure that a thorough assessment mechanisms are in place to ensure consent is freely given, specific and informed, and there are measures in place to prevent broad interpretation of this provisions allowing implied consent by default rather than expressed consent. The onus is on the data controller to ensure it can provide evidence that the data subject has provided free, specific and informed consent for every single use of their personal data.

In addition, Privacy International also recommends the independent supervisory authority to develop relevant guidelines for developing guidance, procedures and mechanisms to determine whether valid consent has been obtained.

ARTÍCULO 13 - Revocación del consentimiento

Whilst Privacy International welcomes the right of the data subject to withdraw their consent at any time, Privacy International suggests that the data controller should be obliged to inform the data subject of their *right* to withdraw consent and the implications of this, prior to obtaining consent, and so prior to data collection. Consent should be as easy to withdraw as it was to give.

ARTÍCULO 14 - Excepciones al consentimiento previo

Privacy International is concerned by the potentially broad exceptions of clause 14. The list of exceptions listed in this clause refer to data which is defined as personal data, and therefore should fall within the scope of protection of this law.

We are particular concerned by the exemption of lending information (*la información crediticia)* especially given the narrow definition of this data in this Bill.

ARTÍCULO 15 - Información al titular de los datos.

The right of individuals to know what personal data that controllers hold on them is a fundamental component to data protection law.

The UN Human Rights Committee, in interpreting the scope of obligations of states parties to the International Covenant on Civil and Political Rights, noted, back in 1989 in General Comment No 16 that:

> *"In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."*

More recently in its 2018 annual report on "The right to privacy in the digital age", the Office High Commissioner for Human Rights noted that "The individuals whose personal data are being processed should be informed about the data processing, its circumstances, character and scope, including through transparent data privacy policies." (A/HRC/39/29, para 29)

Therefore, in addition to what is currently required under this clause Privacy International recommends that the following also be required to be given to the data subject at the time of collection of their personal data:

- the period for which the personal data will be stored;
- the source of the personal data;
- the recipients that the personal data may be shared with;
- the existence of profiling, including the legal basis, the significance and the envisaged consequence of such processing for the data subject;
- the existence of automated decision-making and at the very least meaningful information about the logic involved, the significance and; the envisaged consequence of such processing for the data subject.

Furthermore, this duty should be strengthened by specifying the means/form in which this right should be implemented. Consideration should be given to including requirements as to the form in which this information/ notice is provided i.e. it should be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

ARTÍCULO 16 - Tratamiento de datos sensibles

As noted above in the section of 'definitions', Privacy International suggests that biometric personal data and genetic data should always be regarded as sensitive personal data. Leaving it to the discretion of unspecified competent body risks lowering the applicable standards and level of protection afforded to such data in the draft law.

In an era where data generated and processed is then aggregated, analysed, and compared with other sets of data sets, we are greatly concerned that even information that is not initially sensitive could quickly become sensitive. Biometrics certainly require additional protections because of their unique ability to track individuals across systems, their inability to revoke, and the often sensitivity of the information held within and derived from biometrics. We are also concerned that other forms of data can be uniquely identifiable, such as the signature of our movements, our device identifiers, and these can be linkable between non- sensitive and sensitive data. This signature then becomes a unique identifier, just as a

biometric, for example linking a device to an individual to a health record. We recommend further guidance and thought in this domain and suggest that the Bill requires the independent competent authority to develop guidance and keep this issue under review.

Furthermore, paragraph (g) which permits the processing of personal data if that data has been made manifestly public. This condition gives cause for concern, in particular due to the lack of clarity as to what is made meant by "el interesado" and "manifestamente públicos". This provision is very problematic as it could be that the data was made public unlawfully. Also given the current data ecosystem which is characterised by the continued lack of transparency and poor implementation of data protection and privacy frameworks, it is increasingly challenging for data subjects to be aware of the data being processed about them, the data subject may not be aware that their sensitive personal data has been made by public by themselves or a third party or the consequences of this.

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 18 - Tratamiento de datos de niñas, niños y adolescentes

Privacy International suggests that this provision is strengthened by requiring the data controller to obtain verifiable forms of consent as outlined above in our comments on clause 12.

The Bill should require that the independent supervisory authority develop standards and guidelines on this and the reasonable efforts to verify consent.

ARTÍCULO 19 - Principio de seguridad de los datos personales

Privacy International welcomes the important consideration given to taking sufficient measures to protect the personal data of data subjects. However, Privacy International suggests expanding the obligation to protect the personal data beyond the data itself to include the devices and the infrastructure itself used at every stage of processing including generation, collection, retention and sharing.

Furthermore, Privacy International would like to suggest that the draft Bill as well as the independent supervisory authority provide further guidance on the type of appropriate technical and organisational measures that the data controller should consider to ensure a level of security appropriate to the risk, this may include but not be limited to:

- the pseudonymisation and encryption of personal data;
- guarantee of ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

- a process for regularly monitoring and evaluation as well as audit of the effectiveness of technical and organisational measures for ensuring the security of the processing.

ARTÍCULO 20 - Notificación de incidentes de seguridad

Privacy International welcomes the inclusion of clause 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.

However, Privacy International is calling for this provision to be revised to include the timeframe in which the data subject must be notified.

The current provisions seems to 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 the independent data protection authority to develop key guidance to support this impact assessment of the breach.

ARTÍCULO 23 - Transferencia internacional

Clause 23 fails to provide the necessary safeguards to ensure the protection of personal data when transferred internationally. Privacy International recommends that the provisions in this clause be strengthened to ensure effective protection against the transfer of personal data to countries where such data may be used, processed or otherwise transferred in ways that infringe on the rights of the data subject.

We are in particular concerned by the phrasing of clause 23 which requires only one of the provisions (a) to (n) as a legal ground for international data transfers as a number of these grounds fail to provide any safeguards at all.

Furthermore, we are concerned that:

- paragraph 2(e) will permit the sharing of personal data within group companies with little or no safeguards to the rights of data subjects;
- paragraph 2(f) even where the data subject enters into a contract which requires international transfers, there must be safeguards in place;
- paragraph 2(g) is left open for interpretation as to what public interest is;
- paragraph 2(l) will be construed as providing a broad exception to any forms of intelligence sharing.
- Paragraph 2(m) permits self-regulation for transfers, without clear safeguards and oversight.

Paragraph (b) relating to adequacy of other countries frameworks should be strengthened as noted below.

ARTÍCULO 24 - Carácter adecuado del país u organismo receptor

Clause 24 (together with clause 25) fails to provide the necessary level detail on the mechanism for international data transfers.

Further, the assessment of the level of protection of personal data afforded in the third country should include explicitly:

- rule of law, human rights, including national legislation in force and regulatory/professional rules;
- existence and effective functioning of independent supervisory authorities to ensure compliance with the law.

Insufficient clarity is provided in the current provisions on the process for making such decisions, the factors that are be taken into account as well as implementation, oversight and enforcement of such decisions.

ARTÍCULO 26 - Servicio de tratamiento de datos personales por medios tecnológicos tercerizados

It is important that data processors, as well as controllers have direct responsibility for protecting people's data. Further safeguards should be considered, including for example a requirement to notify controllers of any data breach. For reference see Article 28 of GDPR.

Capítulo 3 Derechos de los titulares de los datos

Privacy International welcomes the inclusion of Clauses 27-36 which provide for the rights of data subjects. The burden should be on the data controller to facilitate the exercise of these rights and the authority should provide relevant guidance.

ARTÍCULO 27 – Derecho de acceso

Further guidance should be provided as to what is meant by asking the data subject to provided '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 exercisee their rights.

ARTÍCULO 28 - Contenido de la información

In addition to the information provided in paragraphs a to h, the data subject should be provided with at least the following information:

- the recipients (destinartaros) of the personal data, the option of only providing 'categories' should be removed;
- the legal basis for processing; and
- the existence of profiling and the consequences.

Paragraph h should not be limited by the intellectual property rights, and provisions must be in place to prevent this being used to circumvent the rights of individuals to receive information and understand automated decisions made about them.

Clauses 27 and 28 the individual should ensure that as well as having access to their data and being provided with information about the processing, an individual should be provided with a copy of it. Furthermore, particular measures must be taken when the data subject faces challenges in understanding the information they are provided with, it must be provided in an accessible and intelligible form.

The authority should produce clear guidance on how to deal with personal data of third parties, in some instances, personal data may be conjoined e.g. the personal data of both the data subject and a third party.

ARTÍCULO 30 - Derecho de oposición

This clause must be reviewed as it seems to imply that the right to object is only possible in cases where the data subject has not consented to their personal data being processed. However, this is limiting as there could be other legitimate reasons behind a data subject's request that a data processor or controller stop processing their personal data.

This clause alludes to the possibility for the data controller to overrule the right to object of a data subject should there be "legitimate grounds". However, we would like to stress once again that 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 take precedent. 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.

The law should recognise that there are scenarios where an individual's right to object should be absolute, this should include for marketing purposes, including profiling.

Furthermore, a similar provision should be included in clause 30 as can be found under clause 29 that during the assessment period that the processing of personal data of that data subject be suspended.

ARTÍCULO 32 - Valoraciones personales automatizadas

Clause 32 requires further development.

As it currently stands, the clause makes similar errors to the EU's GDPR, limiting this provision through limiting its application to 'solely' automated decisions and even then, only certain forms of automated decisions. The use of soley, undermines this right as it means that decisions, even where there is no meaningful human involvement risk falling outside the scope of the provision. The limitation to certain types of decisions – those that produce prejudicial legal effects and those that have a significant negative

effect – also gives cause for concern, as these undefined terms can mean the provision is poorly implemented and open to abuse. The provision should seek to cover any such decisions that make impact on an individual's rights.

Furthermore, this clause should not be framed as a right to object, rather as a prohibition on automated decisions covered by this clause. In the EU, guidance[10] has clarified that Article 22 of GDPR (to which this clause is similar) is to be interpreted as a prohibition rather than a right to be invoked as this means individuals are automatically protected from the types of effects this type of processing may have.

The clause offers no indication of what types of safeguards data controllers must implement in relation to paragraphs a to c. As a minimum safeguard should include the right to an explanation, the right to human intervention and the right to an effective remedy.
Finally, a similar but separate provision should be included to apply to profiling.

ARTÍCULO 33 - 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.

ARTÍCULO 34- Ejercicio de los derechos

We are pleased that the rights are 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.

ARTÍCULO 35 – Abuso de derecho

Clarity should be provided on what is meant by good faith and an unreasonable technical or financial burden to ensure that this provision is not used to undermine the ability of individuals to exercise their data rights.

ARTÍCULO 36 - Excepciones

Privacy International is concerned by the possible broad interpretation of exceptions in clause 36 in particular given the lack of definition and scope of what constitutes "national security" and "public security and order"as well as the protection of the rights and interests of third parties.

[10] Guidelines on Automated individual decision-making and Profiling for the purposes of the Regulation 2016/679 as adopted by the European Data Protection Board, available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Furthermore, this clause would permit any authority responsible for the processing of a public database to not have to comply with any of the rights of data subjects provided for by Chapter III and any of the safeguards provided for by Chapter II.

Privacy International recommends that the bill develops and lists the standards applicable to applications of these exceptions. Such standards should at a minimum identify the public bodies mandated to collect and process personal data, fully respect and protect the right to privacy, and comply with the principles of legality, necessity and proportionality identified by international human rights standards. Privacy International would also recommend the independent competent supervisory authority to develop relevant guidelines for each of those exceptions.

CAPÍTULO 4 OBLIGACIONES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO

ARTÍCULO 39 - Tratamiento de datos por cuenta de terceros.

We wish to express our concern with regards to the extensive retention period of 2 years given in case of possibility for further processing by the data controller/ data processor. This is significant amount of time. We would like to reiterate the principle of storage limitation provided for in this bill.

Personal data should only be retained for the period of time that the data is required for the purpose for which it was originally collected and stored. The law should clearly stipulate that data should not be kept for longer than necessary for the purpose for which it was originally obtained. Any exceptions to this must be very limited and clearly defined.

Just because the data controller might come across another use of the data does not justify extensive retention periods. How long it is necessary to store data will be context-specific, however, this should be guided by other legislative obligations and regulatory guidance. For individuals to be fairly informed about the processing of their data, they must be informed how long their data will be retained, it is therefore imperative that legislation incentivises data controllers to implement the data minimisation principle by minimising the collection of personal data, and not storing it longer than necessary.

ARTÍCULO 40 - Evaluación de impacto relativa a la protección de datos personales

Privacy International welcomes the introduction of the requirement of an impact assessment in relations to sensitive personal data as well as automated decisions that significantly affect individuals. We note that this clause 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. Further consideration should be given to making impact assessments available to individuals who are subject to the processing.

In view of clause 40 (b) establishing that an impact assessment is mandatory in the case of the procession of sensitive personal data at a large scale, we would like to reaffirm our request noted above that biometric and genetic data be categorised as sensitive personal data.

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 SUPUESTOS ESPECIALES

ARTÍCULO 67 - Tratamiento de datos por organismos de seguridad e inteligencia

Clause 58 provides that the Army, security forces, police force or intelligence agency's databases of personal data that were created for administrative purposes; and databases which provide personal records to administrative and judicial authority are regulated by the general provisions of this draft Bill. That these bodies fall within the scope of the Bill is important, however, further clarification of the application of the law and the safeguards in place is needed.

The wording of the section is too broad and allows state authorities to process personal data beyond what is strictly necessary and proportionate. For example, the Spanish law –whose legislation was used as a model to draft the Argentine law- allow the processing of the data without the consent of the data subject, but states that there must be a "real danger"[11] for public security. Argentine law does not require the existence of a "real danger".[12]

Thirdly, clause 67 refers to personal data collected for police purposes. In this case, the provision only states that the data must be deleted when it is no longer necessary for the investigations that motivated its storage. The wording of this provision raises concerns because of its imprecision and broadness. Firstly, the term "necesarios" does not enable that data subjects to know exactly when their data will be deleted. Secondly, the term "razonable" leaves the authorities a broad degree of discretion to decide when to delete or to retain the data. Finally, there is no obligation established to inform the data subject that his data has been deleted, so citizens could never know if their data were removed from the databases.

Through these broadly stated exceptions, the draft Bill allows State agencies effectively to evade the restrictions on processing or transferring data without the data subject's consent or only when strictly

[11] See Section 22.2 "Ley Orgánica de Protección de Datos de Carácter Personal" (Spain) available in http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750. The provision is similar to the former Spanish data protection law, used as a model for the Argentinian data protection law.
[12] Cfr. Didier, Federico José "Data Protection and data processing for security purposes in compared legislation" available in http://www.tecnoiuris.com.ar/publicaciones/proteccion-datos-personales1.php

necessary and proportionate to the achievement of a legitimate aim. As a consequence, citizens are deprived of the main tool to protect the privacy of their data.

ARTÍCULO 68 - Bases destinadas a la publicidad.

This clause provides that consent is not necessary when processing personal data for publicity, direct sale or other analogous activities in cases when used for profiling. We are very concerned about this provision and consider that it should be removed from the Bill.

As it stands this provision places the burden on individuals, rather than automatically having their data protected from these forms of processing. There is no legitimate reason for the inclusion of this provision. Privacy International recently filed complaints with a number of data protection authorities detailing failures of data brokers and AdTech companies to comply with data protection law.[13] Inclusion of this provision facilitates this type of behaviour and fails to contemplate the intrusive nature of this from of processing.

Furthermore, we reject the provision that health care data be used for marketing purposes. Health care data constitutes sensitive personal data and must be subject to strong safeguards.

CAPÍTULO 8 AUTORIDAD DE CONTROL

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 occurred in parallel to the reform process which had been initiated in early 2017 and this has an impact on 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.

[13] For more information see: https://privacyinternational.org/advocacy-briefing/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad

CAPÍTULO 9 PROCEDIMIENTOS Y SANCIONES

ARTÍCULO 73 - 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 75 - Resolución.

This clause 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 77 - 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. Consideration could be given to whether inclusion of percentage based fine would be appropriate.

ARTÍCULO 78 - Incumplimiento de autoridad pública.

This clause provides that if a public authority is found to have failed to comply with this law, it would not be the authority provided for in Chapter 8 which would investigate the alleged violation, but the case would be referred to a relevant authority.

It is unclear why a separate regulatory regime would be in place in case of non-compliance of a public authority if all public authorities are subject to the data protection law.

We reject this provision and recommend that any violation of the data protection law fall within the mandate of the independent authority established by this law (albeit our reservations on this as noted above).

CAPÍTULO 11 DISPOSICIONES TRANSITORIAS

ARTÍCULO 89 – Vigencia

The timeframe provided for in this clause of 2 years is too extensive. The law should come into effect much sooner.

Every day in Argentina there are new policies and practices from both public and private entities which are resulting in the processing of personal data on greater scale. In order to ensure that it protects people in Argentina the government cannot wait 2 years for the implementation and enforcement of the law.