Security Incidents and Cookies in Latin America Countries

INTA Data Protection Committee, Education & Awareness Subcommittee

Chair: Philip V. Marano (Greenberg Traurig LLP)

Vice Chair: Nicola Benz (MLL Legal)

Subcommittee Chair: Stephanie O. Sparks (Hoge Fenton Jones & Appel)

Project Leader: Filipe Fonteles Cabral (Dannemann Siemsen)

Authors: Filipe Fonteles Cabral (Dannemann Siemsen), Sandra Iriarte Maria (Palomo Abogados), Rosa Fabara Vera (Bustamante Fabara)

INTA Liaisons, Lori Schulman, Erica Vaccarello

ACKNOWLEDGEMENTS TO:

Diego Fernández (Marval, O'Farrell & Mairal)
Alberto Rivera (Ferrere)
Macarena Gatica (Alessandri Abogados)
Laura Valverde (Facio & Cañas)
Carimer Gúzman (Castillo & Castillo)
Nadya Susana Leon Retana (Romero Pineda & Asociados)
Nicole Foga (Foga Daley)
Carlos Díaz Sobrino (Bello, Gallardo, Bonequi y Garcia, S.C.)
Marta Almanza Glyva (Guinard & Noriega)
Cristobal Gonzalez R. (Berkemeyer Attorneys)
Catherine Escobedo Paredes (Barlaw – Barrera & Asociados)
Gustavo Fischer (Fischer Abogados)
Luis Henriquez (Bolet y Terrero)

December 2023

Security Incidents and Cookies in Latin America Countries

We live in a global digital economy where the use (and abuse) of personal data has increased dramatically. For this reason, many jurisdictions have enacted consumer privacy and data protection laws worldwide, requiring companies to handle personal data with care, limit use of such data for legitimate business purposes, and provide consumers rights to consent to use, access, etc. to their own personal data – all in a transparent manner and under potential liability for violating these principles. Companies that process personal data with care and respect individual privacy rights may also benefit from increased levels of consumer trust.

The objective of this report is to map the legislative and regulatory standards regarding security incidents and the use of cookies among Latin American countries. It will be noted that six countries lack specific regulation of security incidents (Paraguay, Venezuela, Bolivia, Chile, El Salvador and Guatemala), and nine lack regulation of cookies (Paraguay, Venezuela, Bolivia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala and Jamaica), but in some cases civil laws may serve as a guide.

The term “security incident” may have different meanings depending on the jurisdiction. This report refers to "security incidents" as meaning any confirmed or suspected adverse event involving a data breach such as unauthorized, accidental, or unlawful access that results in destruction, loss, alteration, leakage of data, as well as any form of inappropriate or unlawful data processing that could put the rights and freedoms of data subjects at risk, and, as such, requires notification. This language and meaning will be used throughout the report no matter the country it refers to.

Personal data security incidents and their regulation

- Question 1.1. *Are personal data security incidents regulated by local law and/or acts issued by the local Data Protection Authority?*

Ten (10) Respondents from the following jurisdictions indicated “yes”, personal data security incidents are regulated by local law and/or acts issued by the local Data Protection Authority: Panama; Peru; Uruguay; Brazil, Mexico, Argentina, Costa Rica, Dominican Republic, Ecuador, and Jamaica.

Six (6) Respondents from the following jurisdictions indicated “no”, personal data security incidents are not regulated by local law and/or acts issued by the local Data Protection Authority: Paraguay, Venezuela, Bolivia, Chile, El Salvador, and Guatemala.

Most of the respondents of the survey reported that personal data security incidents are regulated in their countries, either by a specific body of regulation that treats them as a data breach, by acts issued by the local Data Protection Authority, or by some kind of law that regulates the matter for specific cases, like in Peru (specific regulation applied to Government entities). Argentina is a party to the Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data, also known as Convention No. 108, and the Protocol that modifies Convention No. 108, commonly

known as Convention No. 108+. In the case of Uruguay, the Data Protection Authority ("URCDP") has prepared a Guide with recommendations for the Management, Documentation and Communication of Security Breaches in Personal Data. Still in Uruguay, when there is a security incident, the National Computer Security Incident Response Center of Uruguay - CERTuy - may intervene. It should be noted that the laws and regulations on security incidents are relatively new in said countries (2018-2022), so interpretation and implementation are still under constant development. Brazil, Uruguay, Argentina, and Mexico have specific regulations issued by an authority and apparently more mature understandings.

Among the six respondents that answered "no" to the question, many stated that their jurisdictions have no local law governing security incidents. However, countries such as Bolivia, Chile, El Salvador, and Guatemala refer to a Constitutional general regulatory framework that serves as basis for limitations to the government authorities to access personal data. They also refer to "scattered" regulations regarding the processing of data in specific institutions, such as bank information or public record and files, insurance companies and other sectors of the market that could commercialize the data.

- Question 1.2. *Is it necessary to report personal data security incidents to local Authorities? If so, under what circumstances?*

The answer to this question varies. Four of the respondents, Dominican Republic, Ecuador, El Salvador, and Guatemala, stated that, depending on the facts and circumstances of each case, there may be such an obligation to report security incidents to local authorities. In Panama if there is a security incident that results in any unlawful or unauthorized use of the individual subject's data that could lead to a risk of the protection of that personal information, then there will be an obligation on the Data Controller (that is, the natural or legal person which determines the purposes and means of the processing of personal data) to report the incident to the Authority. For the Dominican Republic, the processing and transfer of personal data is unlawful when the owner of the data has not given her or his free, express, and informed consent, which must be in writing or by another means that allows it to be matched to the particular processing and/or transfer, according to the circumstances. Personal data security incidents related to sector-specific bank secrecy need to be reported to the corresponding authority, which is the bank superintendent. For Ecuador, the only time that it is necessary to report an incident to the Authority is when the security incident constitutes a risk to the rights and freedom of the personal data holder. In the case of Guatemala, the obligation to report such incidents might only be applicable for when it also constitutes a breach of a provision of the Law against organized Crime, in the case of tax evasion or if the breach may affect the rights of the parties of a specific agreement regarding trade secrets that could constitute a crime per se.

In the case of Panama, Peru, Uruguay, Brazil, Costa Rica and Jamaica, such obligation to report to Authorities does exist in their respective laws. For example, the respondents from Panama commented that under Act No.81 of 2019 and an Executive Decree No.285 of 2021, which regulates the Act No.81 law, if there is a case of a breach of security understood as any unlawful or unauthorized use of the subject's data that could lead to a risk of the personal information protection, then there will be an obligation on the Data Controller to report the incident to the Authority. On the other hand, Peru's respondents affirm that the theory might be different than the practice. Public administration entities,

providers of digital services in the financial sector, of basic services (electricity, water, and gas), of health and of transportation of people, internet service providers, providers of critical activities and educational services have the obligation to notify the National Center for Digital Security. However, the regulations have not been published yet and therefore, there is not really a timeframe to report them or a sense of it being mandatory yet.

For Uruguay, the law determines that the data controller has 24 hours to take the necessary measures to minimize the impact of the security incident and must communicate the incident to the data protection authority within 72 hours of awareness. The law provides for the action of the National Computer Security Incident Response Center of Uruguay ("CERTuy"), with whom the URCDP will evaluate the content of the communication and the measures adopted, and will agree on the procedure to be followed, which will be communicated to the data controller or the data processor where applicable.

In Brazil, the supervisory authority (ANPD) shall be notified of the occurrence of any security incident that may result in any relevant risk or damage to the data subjects. For Costa Rica, the law grants a five working days period to report to the Agency and take corrective actions; and in Jamaica, the obligation to report exists once the breach in respect to the data controller's operations affects or may affect personal data.
The respondents of Mexico and Argentina that answered that there is regulation on the personal data security incidents by local law clarified, however, in this second question that there is no obligation under the law to report any incidents to local authorities.

- Question 1.3. *Is it necessary to report personal data security incidents to data subjects? If so, under what circumstances?*

In the jurisdictions of Paraguay, Venezuela, Argentina, Bolivia, Chile, Dominican Republic and Guatemala, there is no obligation to report any personal data security incident to data subjects.

The respondents from Brazil, Ecuador, Jamaica, Panama, and Uruguay replied that if there is a case of a breach of security that could lead to a significant risk of damage or harm to the data subjects, then the data controller has the burden to report the incident to them. In Mexico data subjects shall be notified about the breach only if their moral and economic rights have been damaged (breach of financial data, for example, falls into that category). Same as in Costa Rica, where there is a 5-day term to report the breach or irregularity to the data subject and the corrective measures taken. In the case of El Salvador, the owner of the data will only be informed if there is a breach regarding financial institutions for the certification services providers (electronic signature).

For Peru, the respondents see it as unclear. Even though the law establishes that the National Center for Digital Security is responsible for identifying, protecting, detecting, responding, recovering, and collecting information on digital security incidents at the national level to manage them, the Center has only published a daily alert of security incidents through a website, but not directly to the owner of the data.

- Question 1.4. *Who should be responsible for reporting security incidents (controller or processor)?*

Respondents from the following jurisdictions indicated that the data controller is responsible for reporting security incidents: Panama; Peru; Uruguay; Brazil, Mexico, Argentina, Costa Rica, Chile, Dominican Republic, Ecuador, and Jamaica.

Respondents from the following jurisdictions indicated that the processor or other persons may be responsible for reporting security incidents: Peru (respondents say it is unclear because even though there is an obligation by the data controller, also citizens, civil organizations or the academia may report security incidents). In the case of Venezuela, either the controller or the processor may agree to be responsible for reporting incidents.

The following jurisdictions marked this question as non-applicable: Paraguay, Bolivia, El Salvador, and Guatemala.

- Question 1.5. *What information should be reported to the local Data Protection Authority?*

Argentina: the nature of the breach; category of personal data affected; identification of affected users; measures taken by the person responsible to mitigate the incident; measures taken to avoid future data breaches.

Brazil: a description of the nature of the affected personal data; information on the data subjects involved; indication of the technical and security measures taken for data protection; the risks related to the incident; the reasons for the delay, in case the communication is not immediate; the measures that were or shall be adopted to reverse or mitigate the damages; and the measures taken to avoid future similar incidents.

Chile: description of the incident; incident date and time; possible or identified causes; products or services affected; type and name of supplier or third party involved (if applicable); type and estimated number of customers affected; units and/or assets affected (if applicable); actions taken and in progress.

Costa Rica: all relevant information about the data breach.

Jamaica: The facts surrounding the security breach; a description of the nature of the contravention or security breach, including the categories, number of data subjects concerned, and the type and number of personal data concerned; the measures taken or proposed to be taken to mitigate or address the possible adverse effects of the breach; the consequences of the breach; and the name, address and other relevant contact information of its data protection officer.

Panama: the nature of the incident; which personal data was compromised; corrective actions that were immediately taken; recommendations to the data subject to protect his/her interests; and available means to the data subject to obtain more information.

Peru: all available details must be mentioned, including but not limited to name and surname of the person responsible for the report, name of the controller, information about the incident (entity affected by the incident, description of the incident, screenshots if any, etc.).

Uruguay: all relevant information, such as the certain or estimated date of the occurrence of the violation, its nature, the personal data affected, and the possible impacts generated.
The following jurisdictions marked this question as non-applicable: Paraguay, Venezuela, Mexico, Bolivia, Dominican Republic, El Salvador, and Guatemala.

- Question 1.6. *What is the deadline to report a security incident to the local Data Protection Authority?*

The following jurisdictions marked this question as non-applicable: Paraguay, Panama, Venezuela, Mexico, Bolivia, Dominican Republic, El Salvador, and Guatemala.

The jurisdictions that do have specific legislations noted a quick guide to the information that should be reported:

Argentina: 48 hours;
Brazil: 2 working days;
Chile: it depends on the regulation but generally within 30 minutes of becoming aware of the incident;
Costa Rica: 5 working days;
Dominican Republic 10 working days;
Jamaica: 72 hours;
Peru: 48 hours;
Uruguay: 72 hours.

- Question 1.7. *What are the consequences for not reporting a security incident?*

The following jurisdictions marked this question as non-applicable: Paraguay, Venezuela, Mexico, Bolivia, and Guatemala.

Panama, El Salvador, Peru, and Argentina reported that there is no specific penalty, but it should be considered a serious infringement to data protection regulations.

Uruguay, Brazil, Mexico, Chile, Ecuador, Dominican Republic, and Jamaica consider this an offence to their legislation on Data Protection. The consequences would depend on administrative procedures and may result in fines, suspension of operation, administrative sanctions, written warnings, and, in the case of Uruguay, even the revocation of the license to operate.

- Question 1.8. *What are the consequences for a late report of a security incident?*

The following jurisdictions marked this question as non-applicable: Paraguay, Venezuela, Bolivia, and Guatemala.

The jurisdictions that don't have specific legislations on this particular matter are Panama, Argentina, Costa Rica, El Salvador.

For Peru, Brazil, Uruguay, Mexico, Chile Ecuador and Jamaica, failure to report on time would be considered an offense and may result in the application or aggravation of administrative sanctions.

- Question 1.9. *Is there any particularity regarding personal data security incidents in your country that foreign controllers should be aware of?*

Respondents from the following jurisdictions indicated no: Paraguay, Brazil, Argentina, Bolivia, Ecuador, El Salvador, Guatemala, and Jamaica.

Respondents from the following jurisdictions indicated some peculiarities under their jurisdiction:

Panama: the data controller is accountable for reporting security incidents to the Authority and has the responsibility to have all incidents documented and available for the Authority.

Peru: The Secretary of Digital Government reported that they are working on the guidelines that will govern the national registry of cyberattacks and the regulations of the Urgent Decree No. 007-2020.

Venezuela: digital banking services must inform their clients about the management and privacy of their personal data, as well as security incidents that may occur with their personal accounts, as provided by the "Regulations on Information Technology, Dematerialized Financial Services, Electronic, Virtual and Online Banking for Entities Subject to the Control, Regulation and Supervision of the Superintendency of Banks and Other Financial Institutions". Also, they must generate audit reports on attempts to violate networks or equipments and detect possible computer crimes that may violate client´s confidentiality. These reports must be stored for at least one year and must be delivered to the Superintendency of the Banking Sector Institutions when required.

Mexico: the communication of a data breach to the Data Protection Authority is voluntary (non-mandatory).

Bolivia: Decision 897 of the Andean Community Commission established a two-year period for its members to adopt data protection guidelines provided therein. These guidelines include data security incidents regulation and the obligation to report them. The deadline to implement these guidelines ends on July 14th, 2024.
Chile: the bill that modifies the current data protection law, still pending in congress, establishes the need to appoint a representative in Chile and fines have been increased to 4% of the previous year's global income. It should be noted that these provisions could be modified during legislative discussion.

Dominican Republic: all matters related to the protection of natural persons, with respect to the processing of personal data, in relation to any international convention or treaty to which the Dominican Republic is a signatory, shall be governed in accordance with its provisions.

Cookies and their regulation

- Question 2.1. *Are cookies regulated by local law and/or acts issued by the local Data Protection Authority?*

Respondents from the following jurisdictions indicated yes, cookies are regulated by local law and/or acts issued by the local Data Protection Authority: Panama, Peru, Uruguay, Brazil, Mexico, Argentina, and Chile.

Respondents from the following jurisdictions indicated no, cookies are not regulated by local law and/or acts issued by the local Data Protection Authority: Paraguay, Venezuela, Bolivia, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, and Jamaica.

Among the respondents that answered affirmatively to the question, many informed that their jurisdictions have no local law governing the issue, only guidelines or opinions issued by the local data protection authority or other official government body (as the consumer authority in Chile). Some respondents also referred to best practices adopted in their country.

Cookies are not specifically regulated in Panama. Considering that it is a form to track down browsing history, the storage of cookies should be informed in the privacy policies of the website. However, there is no consensus on the subject.

In Peru there are no specific regulations or guidelines on the use of cookies, however, the National Data Protection Authority issued an Advisory Opinion on the subject in 2022 - "Advisory Opinion No. 02-2022-JUS/DGTAIPD - Opinion on the provisions of Law No. 29733, Personal Data Protection Law, and its regulations: right to information, data transfer and data processing through cookies". The Peruvian authority states that the collection of data through cookies, which would allow identifying a person, is an act of personal data processing, and, therefore, it is subject to the general regulations of the Peruvian Data Protection Law and its regulations.

The respondents from Uruguay observed that, although cookies are not expressly referred to or regulated by the Data Protection Law in that country, it does not mean that whoever wishes to use cookies should not comply with the legal and regulatory requirements. Hence, the prior consent of the data subject should be obtained before the installation of a cookie. The data that will be subject to processing may not be used for purposes other than, or incompatible with, those that motivated its collection, and must be deleted when it is no longer needed or pertinent to the purposes for which it was collected.

Regarding Argentina, the respondents of the survey explained that even though the use of cookies is not regulated in that country, there is case law that understands that the processing of IP addresses that can be traced back to a particular person is considered personal data processing. Thus, the general rules of the law apply to the collection of personal data through non-essential cookies.

The consumer authority in Chile (Sernac) states that the use of cookies must be informed, and if they capture personal data, they require express consent.

- Question 2.2. *Is it necessary to show cookie banners on websites?*

Respondents from the following jurisdictions indicated yes, it is necessary to show cookie banners on websites: Uruguay, Brazil, Mexico, Argentina, and Chile.

Respondents from the following jurisdictions indicated no, it is not necessary to show cookie banners on websites: Paraguay, Panama, Peru, Venezuela, Bolivia, Costa Rica, Dominican Republic, Ecuador, EL Salvador, Guatemala, and Jamaica.

Most of the jurisdictions answered negatively to this question. However, the respondents from Peru, Bolivia, Costa Rica, and Ecuador observed that, although it is not necessary to show cookie banners on websites, such action is recommended, especially in observation of personal data protection regulations.

Of those jurisdictions that responded affirmatively, some of them offered some specific information highlighted below.

In Uruguay it is necessary to inform users of the intention to track online activities and the existence of cookies and the purpose of the use of the collected information. It is also necessary to obtain the prior consent of those who browse the website where cookies are located, and information is collected.

The respondents from Mexico informed that when the data controller uses cookies in remote or local means of electronic, optical or other technology that allow him/her to collect personal data automatically and simultaneously at the time the data subject makes contact with them, the controller shall inform the data subject, through a notice or warning placed in a visible place, about the use of such technologies and about the fact that personal data are obtained through them. It should also be informed the way in which cookies may be disabled unless such technologies are necessary for technical reasons.

In Argentina, the general principle under the law is that any processing of personal data must be specifically consented to by the data subject. Such consent must be prior, given freely, based upon the information previously provided to the data subject (informed) and express. In order for the consent to be informed, the controller should provide information to the data subject about: (i) the purpose of the processing of the personal data, (ii) who will access the personal data, (iii) the existence of a database and who is the controller (name and address), (iv) if it is mandatory or not to provide the personal data, (v) what happens if the data subject refuses to provide it (or if he/she provides false data); and, (vi) the possibility to exercise access, rectification and suppression rights. In the case of cookies, this information can be placed in a cookie banner/privacy policy, which should be written in Spanish to avoid any argument for lack of understanding based on language.

- Question 2.3. *Is it necessary to obtain explicit consent for cookies?*

Respondents from the following jurisdictions indicated yes, it is necessary to obtain explicit consent for cookies: Peru, Uruguay, Venezuela, Brazil, Argentina, Bolivia, Dominican Republic, and El Salvador.

Respondents from the following jurisdictions indicated no, it is not necessary to obtain explicit consent for cookies: Paraguay, Panama, Mexico, Chile, Costa Rica, Ecuador, Guatemala, and Jamaica.

Among the jurisdictions that answered affirmatively, Uruguay, Argentina and Bolivia reported that the requirements to obtain explicit consent for cookies come from data protection law. Venezuela, on the other hand, responded that this requirement is provided by the Constitution of Venezuela, whereby the right of people to obtain information about the use and purpose of the data is established.

The respondents from Costa Rica suggested following the GDPR standards.

- Question 2.4. *What are the consequences of using cookies without explicit consent?*

The respondents from Uruguay, Panama, Chile, Costa Rica, Ecuador, Guatemala, and Jamaica replied that there are no consequences in those jurisdictions for using cookies without explicit consent.

In Peru, the consequences for using cookies without explicit consent would be: a) the initiation of an *ex officio* sanctioning procedure that could generate a fine of up to 50 UIT (approx. USD 57 500), as this is considered as a serious infringement; and b) corrective measures, if applicable.

The use of cookies without obtaining the consent of the interested party implies an illegitimate processing of personal data in Uruguay and may be subject to sanctions by the authorities. The sanctions range from observation, warning, fines, the suspension of the respective database for a period of five days and the prohibition of use of the respective database.

Similarly, in Brazil the use of cookies without consent will be considered a violation of the law, giving rise to the application of the administrative sanctions provided in the data protection law, which range from monetary fines to the suspension of the data processing activities.

The respondents from Mexico informed that the processing of data through cookies without consent in that country would be deemed unlawful processing.

In Argentina there is no specific cookie regulation, therefore, in the case of using cookies without the explicit consent of the data subjects, the sanctions foreseen for processing personal data without the corresponding legal basis will be applicable. In this respect, DPA's Provision No. 9/2015 categorizes infringements to the law as moderate, severe, and very severe. With these parameters, processing personal data without the corresponding legal basis is a severe infringement. The sanctions to be applied for these types of infringements shall be up to 4 warnings, suspension from 1 to 30 days and/or a fine of AR$ 25,001 to AR$ 80,000 (approx. USD 156 to USD 500). Additionally, the DPA has a public registry of those who were found as infringing the law.

In Bolivia, a fine of 0,002% of the offender’s gross income obtained through the provision of the service may be imposed for processing data without the subject's prior and explicit consent. This could also be applicable for using cookies without authorization from the data subject.

The respondents from Dominican Republic informed that the use of cookies without explicit consent can open the possibility of an interest party to exercise the rights of their personal information.

In Venezuela, as the law does not provide for a specific consequence the sanction will derive from the civil actions brought by the interested parties.

- Question 2.5. *Is there a time limit for storing cookies?*

Respondents from the following jurisdictions indicated yes, there is a time limit for storing cookies: Peru, Uruguay, Brazil, Mexico, and Argentina.

Respondents from the following jurisdictions indicated no, there is no time limit for storing cookies: Paraguay, Panama, Venezuela, Bolivia, Chile, Costa Rica, Dominican Republic, Ecuador, El Salvador, Guatemala, and Jamaica.

In the jurisdictions that answered in the affirmative way, in general, the period of storage will vary depending on the purpose of the data processing and use. If the collected data is no longer needed, it must be discarded.

The Peruvian Data Protection Law mentions, in general, that the data collected should be stored "only for the time necessary to fulfill the purpose of the treatment", therefore, the same principle should be applied to the storage of cookies.

In Brazil and Mexico, the time limit storage will depend on the purpose of the data processing.

The general principle under the Argentina data protection law is that personal data must be destroyed even without the need for the data subjects to expressly request it when they are no longer necessary or relevant for the purposes for which they were collected. In addition, the data controller may not retain the data when the data subjects request their deletion in exercise of their rights.

In similar way, the respondents from Uruguay informed that in compliance with the principle of finality, the data that is subject to processing may not be used for purposes other than, or incompatible with, those that motivated its obtention, and they must be discarded once they are no longer necessary or relevant for the purposes for which they were collected.

Question 2.6. *Is there any particularity regarding cookies in your country that foreign controllers should be aware of?*

Respondents from the following jurisdictions indicated yes, there is particularities regarding cookies in their country that foreign controllers should be aware of: Uruguay.

Respondents from the following jurisdictions indicated no, there is no particularity regarding cookies in their country that foreign controllers should be aware of: Paraguay, Panama, Brazil, Argentina, Bolivia, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, and Jamaica.

Respondents from the following jurisdictions did not indicate a yes or no answer but provided comments regarding the question: Peru, Venezuela, Mexico, and Dominican Republic.

The respondents from Peru observed that the Peruvian Data Protection Authority is constantly monitoring websites with special software that allows them to identify how many and what kind of cookies such a website collect, and whether they comply with obtaining the users consent before collecting and processing their data. If the website fails to comply, the Authority will start *ex officio* sanctioning procedures that could generate fines and corrective measures as explained above.

In Uruguay, the data controllers must comply with the provisions of the Data Protection Law and its implementing regulation, and the data owners may refuse to give consent or may have the possibility to disable cookies. The consent to cookies must be explicit and the purpose for which the information is collected must be informed. Also, personal data must be deleted once it is no longer necessary or relevant for the purpose for which it was collected.

The respondents from Venezuela clarified that, in general, in accordance with the provisions of the Constitution of Venezuela, everybody has the right to access, update, modify, rectify, anonymize, and destroy the personal data that is recorded on them in private records.

In Mexico, in addition to have the cookie banner, the processing of personal data through cookies shall also be mentioned in the Privacy Notice.

Ecuador applies the same rules valid for national controllers about cookies to international controllers.