Session Leaders

Aline Fachinetti
DPO and Manager for Americas Region
Edenred

Arturo J. Carrillo
Professor, GW Law School & co-Director, Global Internet Freedom Project

Guillermo Larrea
Jones Day Mexico
Of Counsel
Data Privacy & Cybersecurity
• SESSION GOAL - Explore the complexity of the latest regulatory developments and data privacy trends in Latin America, a region experiencing rapid digital transformation.

• AGENDA
  • Welcome/Introductions
  • Context & Overview
  • Specific Laws/Details
  • Break
  • Issues, Hot Topics & Discussion

• METHODOLOGY:
  • Interactive presentations & dialogue/Q&A
United States
- Market driven
- Sectorial approach
- Consumer protection

Europe (EU)
- Privacy as a fundamental right
- Omnibus laws
- Centralized enforcement

Latin America
- A "Third Way"
- Merging of legal traditions
- Panorama...

Context
Context

- Constitutional Law
- Habeas Data
- Public Actors
- Private Actors
Overview
Evolution of LatAm Data Privacy Law

**First Wave**

**Second Wave**

**THIRD WAVE**
- Mexico (2017), Brazil (2018), Ecuador (2021)
- Panama (2019)
Panorama of LatAm Data Privacy Law

Countries with Data Privacy Laws (5/21)
- Argentina, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, Uruguay
- Costa Rica, Mexico, Panama

Countries Reforming or Debating Data Privacy Laws
- Argentina, Bolivia, Chile, Colombia, Guyana, Paraguay, Suriname
- El Salvador, Guatemala, Honduras

Countries Without Data Privacy Law and Related Legislative Activity
- Venezuela
- Belize
All jurisdictions in the region recognize some kind of concept of privacy.

Right of access to personal data of public sphere and Habeas Data, are almost always recognized.

Most of Latin American countries have data protection agencies.
New regulation

Panamanian Data Protection Law Enters in Force

Ecuadorian Plenary Session Approves Data Protection Law

Brazil’s Data Protection Law Enters in Force and Becomes Retroactively Effective
MEXICO´S REGULATION

DATA PROCESSING PRINCIPLES
Legitimacy, Consent, Information, Quality, Purpose, Loyalty, Proportionality, Accountability.

PRIVATE PARTIES
- Federal Law on Protection of Personal Data Held by Private Parties
- Regulations to the Federal Law on Protection of Personal Data Held by Private Parties

PUBLIC PARTIES
- General Law on Protection of Personal Data Held by Public Parties

INDIVIDUAL RIGHTS
Right to Access, right to rectify, right of cancellation and right of opposition.

ENFORCEMENT
National Institute of Transparency, Access to Information, and Personal Data Protection ("INAI")
Cybersecurity in Latin America

Nicaragua's Special Cybercrime Law

Mexico's Cybersecurity Law Initiative

Panama's Cybercrime Law

Brazil's General Data Protection Law
Specific Laws/Details
A Mexican senator presented a bill to amend the Data Law

Proposes obligation of providing data breach notifications to the data owners and to the INAI (max. 72 hours)

Currently, the LFPDPPP only imposes the obligation to notify when economic or moral rights are significantly affected
Obligation of the controllers to appoint a representative or implement a mechanism to comply with their obligations within Mexican territory

What constitutes the data subjects' economic rights for purposes of a breach
Mexican Senate approved the bill to reform the Federal Law of Telecommunications and Broadcasting, providing for a national register of cellphone users. This register will be mandatory and will contain the following data:

- Cellphone number and time of the SIM card’s activation
- Full name of the line holder
- Nationality
- Official identification number with photograph and unique population number
- Biometric data of line holder

The INAI filed an unconstitutionality action before the Supreme Court of National Justice against the reforming and adding of the Law, specially due to the creation of the National Registry of Cellphone Users.
The Deputies Chamber budget does not contemplate resources to implement such registry.

Conflicts articles 6 and 7 of the Constitution and access to telecommunications services, which are fundamental rights.
It also grants undue power to the Federal Telecommunications Institute.

The SCJN has yet to determine whether the unconstitutionality action proceeds or not.
### Main characteristics

- It does not maintain a specific model.
- It is more specific than the TPP / CPTPP.
- Encourages OECD principles and APEC principles.
- Encourages compatibility and interoperability.
- Recognizes the CBPR system as a valid mechanism for international transfers.
- Establishes the application of legal frameworks that must be necessary and proportionate.
- Encourages cooperation and compatibility among the three countries.
- Adds a clear definition of personal data.
- Provides a legal framework that provides for the protection of personal information.
- Encourages cooperation between government agencies in personal information protection investigations.

### Prohibitions

- Prohibition of restrictions on cross-border data transfer flow, except:
  - Legitimate public policy objective, + (i) non-arbitrary measure (ii) non-discriminatory measure (iii) non-excessive measure.
Recognizing cybersecurity threats to digital businesses

- Malicious intrusions or dissemination of malicious codes that affect electronic networks.

Promotes national incident response mechanisms

- Proposes identification and mitigation mechanisms

Proposes collaboration between countries to share knowledge and best practices

- Proposes that companies apply the standards and best practices according to their jurisdiction

Acknowledges the need for risk-based mechanisms and international standards for hazards

- Recommends risk-based approaches as more effective than prescriptive regulation
Recommends risk-based approaches as more effective than prescriptive regulation

• Elaboration of impact analysis, for example:
  • Data transfers made by the company
  • Security in digital platforms

• Recognition of data protection principles

• Reinforcement of compliance programs

• Implementation of mechanisms to identify and mitigate malicious intrusions

• Adoption of digital security measures and preparation for cybersecurity incidents
Brazil’s LGPD
Brazil’s Data Protection Law approved on August 2018

On September 18, Brazil’s data protection law (LGPD) became effective (most parts of the law)

The LGPD addresses:
- Extraterritorial jurisdiction
- Specific provisions for sensitive personal data
- Enumerates data subjects’ rights and requires to provide data subjects’ access
  - Lays out 10 principles, which should be considered when processing personal data

- Lawful basis
  - Requires incident breach notices with specific information.
  - States the mandatory need of a data protection officer.

- Creates a National Data Protection Authority, which will be responsible for overseeing compliance, penalties, etc.
  
  Operational since a few months ago

Administrative Penalties will not be enforceable until August 1, 2021

Will reach up to 2% of income, up to the limit of BRL 50 Million
# ANPD – Brazil’s Authority

<table>
<thead>
<tr>
<th>Topic</th>
<th>Start of regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1º/2021</td>
</tr>
<tr>
<td>ANPD's Internal Rules</td>
<td>●</td>
</tr>
<tr>
<td>ANPD's Strategic Planning</td>
<td>●</td>
</tr>
<tr>
<td>SME simplified rules</td>
<td>●</td>
</tr>
<tr>
<td>Sanctions</td>
<td>●</td>
</tr>
<tr>
<td>Incidents notification</td>
<td>●</td>
</tr>
<tr>
<td>DPIA</td>
<td>●</td>
</tr>
<tr>
<td>DSRs</td>
<td></td>
</tr>
<tr>
<td>DPO</td>
<td>●</td>
</tr>
<tr>
<td>International Transfer</td>
<td>●</td>
</tr>
<tr>
<td>Lawful basis</td>
<td></td>
</tr>
</tbody>
</table>
COLOMBIA'S REGULATION

PRINCIPLES OF DATA PROCESSING
Legality, Purpose, Liberty, Accuracy or Quality, Transparency, Access, Limited Circulation, Security and Confidentiality.

INDIVIDUAL RIGHTS
Right to know, update, and rectify and right to request proof of consent, right to know the use of the data, right to complain, right to revoke consent and to request deletion and right to access.

REGULATION
Statutory Law 1581

ENFORCEMENT
Colombian Superintendence of Industry and Commerce (SIC)
COLOMBIA

SIC Requests Google to Comply with the National Data Protection Standard.

- Their Information Processing Policy did not comply with the Colombian regulations.

SIC Fines Movistar for Consulting User’s Credit History for Marketing Purposes

- A fine of US$69,209.80 for consulting a user’s credit history for commercial and sales purposes, without user’s consent.

SIC Orders TikTok Application to Comply with Colombian Standards of Data Protection.

- Ordered TikTok to implement additional data protection measures, since they failed with 47.37% of the Colombian standards.
ARGENTINA
- Body temperature data must be relevant, in accordance to its purpose and must be erased when it is no longer necessary.
- All terms in which the temperature data processing will take place must be available.
- Inaccurate or incomplete data must be deleted and replaced.
- Body temperature data cannot be used for different or incompatible processing purposes.

URUGUAY
Uruguayan Data Protection Agency Issues Recommendations on the Use of Vaccination Center Images.
- An image is classified as personal data.
- An individual's vaccination information is sensitive data.
- Prior to an individuals’ photo collection and processing, consent is required.
- Prior to the images dissemination, a balancing exercise between right to data protection and freedom of the press must be carried out.
Verify that the electronic site enabled for registration is the official site, void providing unnecessary personal, financial, or health information to strangers or through social strangers or through social networks or phone calls. Request the privacy notice. Public officers do not have the authorization to take any pictures.

INAI Issued Statement About Protecting the Privacy of Vulnerable Individuals during the COVID-19 Pandemic Period.
The INAI stated there will be challenges in terms of personal data protection, as ensuring the privacy of individuals whose conditions may be associated with complications in the event of contracting COVID-19 such as persons with HIV, diabetes, hypertension or cancer.
Issues, Hot Topics and Discussions
Preliminary issues list:

- Civil actions
- Right to be forgotten
- Reas. security
- Convention 108
Civil actions
This as a result of the lack of action of Google against the unlawful use of their Blogger platform, in which a user disseminated content that damaged the economic rights of U. Richter. Attorney U. Richter obtained a final judgment in his favor and against Google Inc. Google must compensate him for moral damages and punitive damages. The judgment may set a precedent on:
- the exercise of freedom of expression
- the responsibility of the platforms on the content generated by third parties
Right to be forgotten
Unpacking the Right to Be Forgotten

The RTBF in Europe

Derecho a la cancelación in Latin America

“Oil & Water”

Google v Spain
GDPR (Art.17)
Habeas data
ARCO Rights
Mexico, Argentina, Colombia, Peru
<table>
<thead>
<tr>
<th>INAI ordered Google Mexico to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- De-index certain URLs from the Google Mexico search engine</td>
</tr>
<tr>
<td>- Delete personal data relating to an individual from its databases</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>An individual claimed that his name on a Google Mexico search engine disclosed:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- his name,</td>
</tr>
<tr>
<td>- the name of his (deceased) father,</td>
</tr>
<tr>
<td>- the names of his brothers,</td>
</tr>
<tr>
<td>- and information pertaining to his business activities.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INAI decided Google Mexico was responsible for the processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Though, Google stated that they were legal entity distinct from Google Inc., which was the data controller.</td>
</tr>
</tbody>
</table>
Google México was sanctioned for:
- not replying the individuals request
- they must de-index the listed URLs so that they could no longer be found through a search

INAІ also ordered the company to respect:
- the user’s right to be “forgotten”
- and right of deletion

Mexico recognizes the personal data protection and privacy is a fundamental right - ARCO rights.

Although it is not directly recognized, as in some parts of Europe, the right to be forgotten can be broken down from:
- guidelines on privacy and data protection,
- and it has been confirmed through judgments that it is respected.
Reasonable security
Reasonable security

Confirmation of the legal framework for the personal data processing

Informing data subjects of any extraordinary data processing

Protection of the identity of data subjects

Creation of policies applicable to day to day situation

Monitoring of teleworking

Minimum data collection and retention periods
Reasonable security

- Incident response plan
- Control of communications and messages
- Use of security measures
- Updates and trainings
Convention 108
<table>
<thead>
<tr>
<th>CoE Convention 108 &amp; 2018 Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981)</strong></td>
</tr>
</tbody>
</table>
| • Argentina  
• Mexico  
• Uruguay |
| **2018 Protocol Amending Convention 108** |
| • Uruguay (signature)  
• Argentina (signature) |
| **Convention 108(+)’s Relationship to the GDPR** |
| • Technical considerations  
• Connection to “Adequacy” determinations  
• Is “Adequacy” overrated? |
| **The Future of Data Privacy in Latin America** |
| • Convention 108(+)  
• Data privacy laws  
• The Role of the GDPR & other models (e.g., CCPA) |
CONVENTION NO. 108
MÉXICO

ENTRY INTO FORCE
01/10/2018

HAS NOT BEEN SIGNED
PENDING

RATIFIED
28/06/2018

MEXICO
Questions + Contact

Aline Fachinetti
DPO and Manager for Americas Region
Edenred

Arturo J. Carrillo
Professor, GW Law School & co-Director, Global Internet Freedom Project

Guillermo Larrea
Jones Day Mexico
Of Counsel
Data Privacy & Cybersecurity