

SESSION 3: Data Protection: Data Protection Alternatives for Latin America and the Caribbean. Use of data by the private and public sectors.

Panelists

Irvin Halman - General Administrator - National Authority for Government Innovation (Panama).

Laura Juanes - Privacy Director, Facebook

Cédric Laurant, Son tus Datos (Artículo 12, A.C.)

Carlos Affonso Pereira de Souza (ITS-Rio)

Fátima Cambroneró (ISOC MX)

Moderator:

Agustina Callegari - Youth SIG

Introduction:

1. Panel presentation.
2. Addressing the current perspective or reality regarding the protection of personal data (brief presentation by each panelist on the topic).

Carlos Affonso expresses his gratitude for the invitation to LACIGF Panama 2017. He then points out that in Brazil there is a different situation regarding data protection compared to the region, because although there is no general law on personal data protection, privacy and data protection are protected under the Brazilian Political Constitution, as well as under the Civil Code and the Consumer Protection Act, which involves personal data and privacy, but there is no general law on personal data protection. This delay creates a connection with other countries in the region to observe personal data protection in other countries and learn from international experiences, their successes and failures, in order to – finally – improve Brazilian legislation.

Cedric Laurant explains that he will speak about personal data protection issues in Mexico. These issues include supervision by authorities, lack of budget, lack of independence, lack of job security due to political reasons and lack of knowledge. There are also many problems with companies conducting business in Mexico and trying to evade their personal data responsibilities. He points out that there is a lack of incentives for personal data holders and for the defense of personal data rights. Finally, he mentions the poor level of digital technology skills and tools as an issue in Mexico.

Fatima Cambronero opens by saying she is grateful for the invitation and that, to avoid repeating what has been pointed out about Mexico, she will approach the issue from a technical point of view, focusing on which principles should guide legislations addressing personal data protection. In this regard, Cambronero notes that the Internet Society has developed a document referring to the guarantees that Internet policies should have and shares the views of ISOC on these issues. In particular, four values should be included in this kind of legislation: (1) user trust, (2) a technological perspective (3) a reliable network, and (4) a reliable ecosystem where users can continue to participate. These documents are uni-stakeholder, as only the authorities are involved, and they dictate which principles must guide legislation on the matter.

Laura Juanes (Facebook) begins by mentioning she is very excited to be in Panama and grateful for the invitation. From a regional perspective and with reference to privacy, Latin America is not the “far west”, i.e. there is no free for all, there are constitutional protections, the concept of *habeas data* was born in Latin America and more than 10 countries have adopted this legal instrument, among them Argentina, where these instruments are being reviewed for possible modifications. There are data protection authorities who are doing a great job, and participating in international forums such as APEC and other technical forums. Progress in issues of transparency in the region should be highlighted.

Irvin Halman notes that, in the case of Panama, there are two articles in the Constitution regarding personal data, but that data protection is not included in any supplementary legislation. Consultations were held last year with the help of the OAS, associations and civil society were consulted in order to draft a data protection bill. Based on Chilean legislation¹, taking also into consideration ARCO rights and the particular needs of certain sectors, a bill was presented to Congress. Halman points out that it is important to take this issue forward because we are moving towards digital economy and digital government, so it is necessary to generate trust among citizens regarding which data is in the hands of governments and companies; this is what prompted work with the transparency authority – the authority dealing with these issues by law – and to elaborate and work on a personal data protection bill.

3. Questions about personal data protection models in the Latin American context:

To Cédric Laurant: What kind of data protection models exist today?

¹ This refers to the Bill proposed by the Chilean government, not to the data protection Act currently in force, as the latter is outdated (1999).

Cédric Laurant points out that most of the models developed in Latin America are based on European models, with certain differences. For example, in Mexico, with a little more practicality, companies are not under the obligation to register their personal data, or they have co-regulation schemes which allow companies to flexibilize regulations so that they always self-regulate under the guidelines stipulated by law and the federal data protection authority. There are omnibus laws in Argentina, Colombia, Costa Rica, Mexico, Peru and Uruguay, there are laws more sector-specific laws, as is the case of Mexico, where a law applies to the collection of credit and loan record data. Similar laws exist in Colombia and Chile. Finally, there are countries with non-unique legal frameworks such as Panama, but which have bills underway, such as Panama itself, Honduras, Bermuda, or the Cayman Islands.

To Laura Juanes: What personal data protection models have been applied in the continent, under the international context, and what are your views on these models?

Laura Juanes points out that she will paraphrase Marisa Jimenes (Google) at the Ibero-American Congress on Data Protection held in Chile, stating that we take the personal data principles of the 80's which are now part of the Privacy Act or those of the FDE in 81' or the principles set out by APEC. If we put them all together, they are not so different from each other. They all speak of accountability, transparency, control, security, individual rights, etc. When these principles are translated and implemented, there are changes in the different countries where they are applied. Juanes points out the reasons for these changes, emphasizing that the reasons for these changes are the cultural, economic and geopolitical context; the relationship with other rights, for example, freedom of enterprise and expression, freedom of expression and privacy, etc.; and finally, the legal culture.

This translates into standards, legal traditions which are modified, pointing out what is acceptable and what is not, depending on where we are and how we have been brought up. An example is the European Right to Oblivion which has been adopted by some countries and not by others in the same way.

It is important to note that, when looking at models and implementations, we should not think that some models are better than others, as they are all different. It is not about making judgments, because they are all different. It is important to know what we have at our disposal, to see which tools have worked and which have not, for example, Danilo Doneda points out that models cannot be transplanted to other countries, as they do not necessarily adapt. It is necessary to study the models that have been adopted, not implement them directly in other countries. It is necessary to look at trends rather than models. Take Canada, for example. Canada has a hybrid model which is very interesting and flexible, based on legal

consent. Despite this, the Canadian authority is becoming aware of the limitations of consent. For example, at Facebook we have written a paper with the authority on this matter, the APEC model is very interested in this model. This also means we need to examine the European model and be careful with the data being collected there, because Latin America only receives the headlines. For example, there is no single legal basis in the European model but several ways of understanding issues such as consent, its adequacy based on data, etc.

Question to Fatima Cambronero: "Do you think that regulation is the way to set standards for the protection of personal data?"

Fatima Cambronero points out that in certain cases it is and in others it is not. I would like to share the principles that such regulation should have, regardless of how it they are implemented. For example: the principle of lawfulness, that data treatment is conducted within the current legal system; in some countries this is enshrined in legislation, but in others it is not. However, this can be redirected through the Constitution. Another principle is loyalty, whereby the processing of personal data must be done according to the reasonable privacy expectations of personal data holders. A third principle is consent: no personal data can be processed without the consent of the holder of the information, which must go hand in hand with information (privacy policies) about what treatment is going to be done, which data will be processed, for what purpose, where the data will be transferred, etc. Another principle is quality: treated data must be updated, correct and truthful. Another principle is proportionality, any data that is requested must be related to the purpose for which it is intended, and this needs to be made explicit in the privacy terms and conditions. Finally, the principle of responsibility is at the core of any legislation: data can only be treated in compliance with the legislative standards currently in force and applicable terms and conditions.

Some legislations speak of duties, as in the case of Mexico, while other countries establish principles such as that of security, where the technical aspects required for treating personal data are regulated.

Two final aspects should be taken into account: first, we must define what are the rights of the holders of the personal data, who, in principle, must be able to access information on such data and other ARCO rights; second, the need to have a personal data control authority that actually has power. In my opinion, this body should be independent from political power and focus on the person, the holder of the personal data.

Carlos Affonso Pereira de Souza is asked the same question: " Do you think that regulation is the way to set standards for the protection of personal data?"

Carlos Affonso points out that in the case of Brazil the Constitution includes a data protection regulation and that the protection of privacy appears in the Civil Code and in the Consumer Protection Act. He adds that they have the Brazilian Civil Rights Framework for the Internet (Internet Act) which has articles on privacy and data protection rights (Article 7). While this does not replace the need for a law on personal data protection, but it is a first step.

The situation in Brazil seems to be portrayed as a country with only two options: either reproduce the European model or reproduce the American model. However, it is important to note that we have many relevant experiences in Latin America. The Civil Rights Framework for the Internet was created, an innovative and pioneering experience which examined the strengths of each country. It is worth emphasizing that there are more than simply two options: there is space for creativity and for observing different ways used for dealing with the issue in the region.

Another point worth noting is technological change. It seems to me that we are living in a very special moment. Those of us working on personal data are used to discussing issues such as personal data, Cloud Computing, Big Data, IoT. I do not think these issues will change the discussion structurally, but the issue of Artificial Intelligence will.

Artificial Intelligence may even change the structure of law itself. To understand how privacy and data protection will evolve in this environment, it is very important to address the topic of artificial intelligence (it will be addressed tomorrow at the Conference). Another issue is Smart Cities: how to collect and process personal data in Smart Cities. We have an example in Brazil with the case of Sao Paulo: the mayor changed the way in which personal data were collected through public wi-fi serviced. This mayor acknowledged that data collection changes economic models. But technological innovations cannot be created at the expense of privacy and the protection of citizen's personal data. Finally, understanding how data collection will be conducted is a major problem with regard to how regulations will be created.

The final comment delivered by Carlos Affonso underlines that there are many examples in addition to public wi-fi. For example Uber, Cabify, etc. There is a regulation in Sao Paulo that forces these companies to share a lot of information, e.g. driver rating, which is very interesting. Why is the State interested in knowing and allowing people to share information about these drivers? All of us here know that personal data are interesting. The questions are how will data be protected and why is it being collected.

Question for Irvin Halman. What was the process for creating the Personal Data Protection Law in Panama?

Irvin Halman points out that European and regional legislation, such as that of Chile, were examined because that seemed to be most appropriate to what Panama was looking for. A pragmatic choice of legislation was made, considering that regulations too taxing for companies would prevent our agencies from receiving large amounts of work and they do not have the ability to collect the amount of data that would be required by more taxing regulations.

When a deviation from the standard promoted by the regulations is detected, the authority imposes fines, penalties, etc. in the event of serious and recurring offenses, data processing might even be suspended.

We try to make regulations general and applicable to both private companies and government agencies. When there are special laws in force, those will be applied. However, where there are no specific regulations in place, the general rule will apply. For example, a number of principles are applied: data collected should be used for the stated purposes, regulated subjects include both natural and legal persons (public or private) within the national territory.

Another principle: when collecting data in critical government structures, the data must be stored in national territory.

For example, the example of free connectivity will apply. Information is requested to confirm that personal data will not be used unless such data are dissociated. To generate trust among users, within the application, the authority shall request that users validate their identity. For processes carried out by public entities, data are dissociated from the identity of their holders, although the electoral court does know that such persons exist. This creates trust, security and is what the law seeks. There was an earlier effort to have a law of this type, but it caused doubts and suspicions among the citizenship, which caused the initiative to fail. We hope that trust and the public consultation that was held will allow government authorities and companies to have better personal data protection and privacy regulations.

Cédric Laurant was asked about the legislative processes for the approval of personal data legislation as well as user perspectives in Panama and other countries of the region. The idea was for Cedric to share his experiences in this regard.

Cédric Laurant: In Mexico we have followed cases of consumer complaints against companies that violate consumer rights and we have encountered obstacles. What was most surprising was the lack of knowledge on the part of INAI (Mexico's Federal Institute for Access to Public Information and Data Protection) staff, for

example, of what a cookie or behavioral advertising were – they had no idea how the legal system applied in these situations. This poses a major issue, as there is also a lack of knowledge among users and consumers on how to protect themselves and their rights. In addition, when INAI imposes sanctions, there is no compensation for the holder who filed the complaint, but rather for the Public Treasury. INAI has fined the equivalent of 14-15 million dollars since 2012, only 2 or 3 fines (one of them a fine for \$ 40,000 pesos imposed on a doctor) have been paid so far, and this does not appear in INAI's annual reports.

Since July 2010, the law requires notification of violations to the Personal Data Act. This is a worldwide trend, including places such as Europe, 46 states of the United States, Uruguay, Costa Rica, Colombia and Mexico. I think Panama is thinking of including it on their Bill, as is Argentina. Other countries are also considering similar initiatives. This is a major obstacle: in Mexico, no company has notified their treatment of personal data. The only companies that comply with this requirement are publicly listed companies, which are required to do so under the Stock Exchange Act.

Many companies have been asked to respond on these issues and have not done so, whether in bad faith or for reputational issues. The last point is that, despite having physical facilities, they conceal the location of their offices. In October, a criminal lawyer received a court ruling which said that Google Mexico had committed perjury by stating before notary that they were not domiciled in Mexico (something done by many companies in Mexico), implying that users can't report infractions to those companies in Mexico.

The moderator points out that there are only two questions remaining.

Laura Juanes (Facebook) is asked about users' perspectives on their actions on Facebook. Laura Juanes points out that the issue of privacy is a matter of trust and that there are two billion users who trust Facebook. It is essential to promote user trust through education, reactive measures and transparent privacy policies. I think we are at that point.

Laura Juanes extends an invitation to Desing Jumbs in Sao Paulo. We are trying to respond with technologies to provide control and transparency to users. The idea is to bring together different professionals to create working groups and assign them privacy challenges. We believe that it is possible to combine privacy and technologies. Everyone is invited.

Fatima Cambronero is asked how the issue of data protection is addressed in international organizations.

Fatima points out that ISOC's perspective is focused on user trust, in other words, on the fact that users should be able to rely on legislation. This means that the protection of personal data is considered as a Human Right. Respect for telecommunications is essential. The Internet Society recommends encrypting communications. Privacy policies or terms and conditions must be read. In our countries with legislation based on Roman law, consumer protection and data protection laws are treated differently. In other Common Law countries, they are dealt with together. In our countries there should be protection for consumers when they contract online: Mexico's PROFECO closely monitors those behind e-commerce companies, so that users can submit a claim in case of incidents. It should also be taken into account that users must always have control over the information, including the possibility of accessing, correcting, rectifying and deleting such information. One innovative aspect stemming from European data protection standards is the right to digital data portability and the possibility of transferring data to others if the owner wishes to do so.

To conclude, transparency: those responsible for gathering and processing personal data must be accountable to the owners of such data, thus promoting legal certainty.

4. Questions from the audience

4.1 Osvaldo, from Dominican Republic: There are two general trends. One is by sector and the other is omnibus. In DR, prior to implementation of the Data Protection Act, credit regulations were used. Somehow, this evolved from *habeas data* to specific regulations, as there were international pressures to legislate in that regard. As a consequence of the above, the Superintendency of Banks is the regulator. Companies with global presence such as Facebook are often not established in one particular country. How do they ensure the general public can access personal data and how can they protect that information?

Facebook (Laura Juanes) points out that the way to know your right and what information you have shared on Facebook is through the 'Download your information' which allows users to download all the personal information Facebook has gathered. We offer this tool globally. This information is what you have provided through our company's platform.

The Panamanian authority points out that, according to the pragmatic logic of the bill, they anticipate that global companies will have the standards for citizens to act, including both consumer rights and enforcement of local competition. Panama is an open country that tends to regulate to ensure this issue is respected. With regard to credit legislation, a benefit for consumers is

that data can be shared with banks if the person gives consent, this consent cannot be withdrawn, but it cannot be used for other purposes.

4.2 Question for Cedric Laurant from Lia Hernandez. A good thing and a bad thing about a personal data protection act. What is good and what would you change about the Panama bill? Answer: The bill I have seen has several confusing elements. It includes the fundamental principles of a legal framework applicable to private companies. The bill has exceptions for private companies, which would be able to justify having to treat data for purposes a little different than the owner consented to. More than analyzing a specific detail of the bill, the bill itself is not enough for the holder to be protected, as other factors should also be considered. For example, authorities must be independent of any political party, as is the case in Mexico. They must have sufficient budgetary autonomy and be well acquainted with regulations, because in Mexico there is no real authority capable of properly deciding specific cases. It is also important that this law includes training and education measures regarding the bill for both users and companies. Companies often do not comply with the regulation because owners lack the means and incentives to defend themselves.

Laura Juanes adds that for laws to be understood and become rooted they need to be relatively simple and easy to implement at all levels, both large companies which can afford law firms and small businesses. Laws mustn't be made for firms.

4.3 Question from Renata Aquino from Brazil regarding advertising and political content. In polarized political situations people only view news and content according to their political profile. The question is how much of the data is taken into consideration for political profiling by social networks like Facebook, where one can be deceived by false news and political content. Laura Juanes points out that Facebook is very concerned about the issue of misinformation. "We want our platforms to facilitate information. We will gladly put you in touch with the technicians working on this issue, especially on trying to eliminate the economic incentives that encourage this kind of information. But I do not want to get into trouble because it is not a topic in which I am directly involved, so I'll be delighted to put you in contact with the specialists.

4.4 Carlos Affonso adds that social networks need to be a window to the world and not just a mirror that reproduces what people like. The issue of fake news requires an inclusive and multisectoral debate; actions by these platforms and the commitment of civil society are needed to clarify this issue. It is necessary

that all agents, particularly platforms, identify the contents which may be considered by the community as fake news.

4.5 Question: Is the sale of personal data through the Deep or Dark Web contemplated? Laura Juanes: Facebook does not sell the personal data of our users. Facebook does not sell personal data.

4.6 Question from Usuarios Digitales, Humberto Artos: Artificial Intelligence seems to take the issue of personal data to a new version of data protection. Understanding that companies such as Facebook or IBM are working on it, what are your thoughts with regard to advancing and drafting data protection policies that contemplate Artificial Intelligence?

Carlos Affonso: it is important not to create an opposition between privacy and the protection of personal data vs. innovation and Artificial Intelligence. Further in-depth discussion of these issues is needed, discussions on automated individual decisions that are emerging in the European debate and also appearing in Argentina and Chile but only for public agencies. The issue of automated individual decisions is key to the discussion on Artificial Intelligence and this topic should be discussed.

5. Final words:

a) Carlos Affonso: Regarding Brazil, three years ago we passed a Civil Internet Framework, yet when we talk about Brazil everyone remembers the Whatsapp shutdown. That was a very bad solution, due to poor management of access to privacy and personal data. When this was used, it was to protect personal data and privacy, both of citizens and businesses. A data protection act creates legal security for all, companies and citizens alike.

b) Cédric Laurant: My final question is for Laura Juanes. In Europe, express consent is required for biometric recognition in Facebook tagging. In Latin America, it is sensitive data in many cases, Mexico, for example. Why is this not required in Latin America? Answer by Laura Juanes: Facial recognition is a matter of context and perception rather than regulation. In this case, I think it is more important to know about the need to tag a photo before uploading it, which is a service not offered in Europe. It is a question of context and about how one relates to technology.

c) Laura Juanes: We need to talk about opportunity, about what we can learn from each other, what we can contribute in the region and what we can export.

d) Fátima Cambroneró: Perhaps regulation is needed to protect personal data. The recommendation is that this regulation should be based on a

multistakeholder approach and that all stakeholders should participate on an equal footing.

- e) Irvin Halman: The development of digital economy and the opportunities that interoperability presents require the regulation of a constitutional right. Standards are welcome for Panama to regulate this matter.

Thank you very much, everyone.

End of the session.