Session 1: Data Protection Alternatives in Latin America and the Caribbean from a Rights Perspective. Use of Data by the Private and Public Sectors.

1. Presentation by the moderator (María Paz Canales)

We would like to discuss a legal framework for the protection of personal data that is compatible with the exercise of fundamental human rights. Most Latin American countries do not yet have a personal data protection framework. This framework is important for the digital economy, innovation and the protection of human rights. Data protection plays a key role due to changes in technology. Today, personal data can be generated based on other data, and even metadata have become increasingly important.

The business model favors the cross-border flow of personal data, but different actors must act to protect personal data from misuse and possible security incidents. The participation of governments, the private sector, civil society, academia and users is very important. Unilateral actions are not effective and may have negative effects on this ecosystem.

2. Panelists' interventions regarding the first question: **Which principles and rights should guide the protection of personal data? How can the multistakeholder model contribute to the effective protection of user privacy, personal data and other human rights?**

- Pedro Less (Google)

Information security and transparency are the two basic pillars supporting data protection, as the biggest problems have to do with these two aspects. Another issue is data portability, on which we have been working with the Data Liberation Front so that the information downloaded by a user can be easily exported to another player. This will become an additional competitive advantage for the private sector, as those who offer greater protection will have a greater number of users, and portability will increase competition. As for security, the region must discuss this topic. The existing approach is very territorial, and we believe it is important to focus on where the information is located, rather than on the processes to which it is subject. For small and medium-sized companies, it is very difficult to keep the information in each country; this also goes against Internet infrastructure. For this, we need binding self-regulation mechanisms that are developed through participatory processes.

Multistakeholder models can contribute to the protection of rights, for example, academia and civil society have condemned the right to be forgotten because it goes against the human rights system and infringes upon freedom of expression. The technical community can say what is and what is not possible in terms of regulation. If a group of companies are the only ones who can comply with the terms and conditions set forth in the regulation, this regulation will promote concentration. Users also have a role to play, as they are the digital migrants who regulate the digital ecosystem. We must bear in mind new behaviors considering behavioral insights and economics.

- Eduardo Bertoni (Director of the Agency for Access to Public Information and Data Protection, Argentina)

First question: The organization of the Latin American IGF has become increasingly professional. It would be important for what is discussed here to have an impact on the global IGF. The region is undergoing a significant change in terms of personal data, given the development of technology and the influence of European legislation, which has promoted the need for better regulations. All such regulations include a chapter on principles — you would be bored if I told you about them because you already know them.

The difficulty in regulating based on this model is that technology changes very quickly, so it is often difficult to effectively implement some of these rights (e.g., the right to information vs. Big Data). There is now a tendency to monetize user data collection, which is an issue that we will have to sort beyond the principles that have already been established. We will have to be creative to make sure that regulations are enforced and that their enforcement does not hinder innovation, investments and data exchange.

Data security is also a huge challenge, particularly, determining how regulations can increase the efficiency of said protection, as not all sectors think alike and not all data can be treated equally.

- Juan Manuel Haddad (Telefónica Argentina)

At Telefónica, we like to say that we are going through a change of era — we are moving to a digital economy where data plays the leading role. The business model of this digital economy is supported on a basic pillar: people should trust how their personal data are processed and handled. Creating trust involves transparency, data security, and empowering people so they can choose how to handle their data.

Publishing terms and conditions on a website no longer appears to be enough, as nobody reads or understands them. It is necessary to go beyond this, so that users can understand what is being done with their data.

- Iria Puyosa (Researcher at Universidad de los Andes, Quito)

There is very little civil society participation in these discussions. Likewise, users are not incorporated into the process of discussing and developing regulations and legislation. Discussions often take place when the foundations of the model have already been established. National regulations are also emphasized, particularly when data processing takes place across borders. In different countries, different bodies are responsible for data protection, but who oversees these bodies? It is important to make sure they are independent from the various regulatory agencies and that they are based on the multistakeholder model. Educating citizens and the public in general is also important, as people do not realize that they are constantly generating data, particularly when using mobile and biometric devices.

- Raquel Gatto (ISOC)

Thinking about the future, what forces of change will allow us to maintain an open Internet? One such force is user empowerment, but also keeping human beings in mind at all times, from the moment a technology is created up until its regulation. Internet of Things devices allow collecting increasing amounts of data. Big Data allows organizing and handling this data, and Artificial Intelligence can organize these data into products and services. There is an incentive for collecting and processing data. In the case of automobile insurance, for example, it is possible to see if a person is a good driver,

whether they are driving under the influence, or if the car is parked on the street. Insurance companies use this information to set their prices. Users, however, are missing from this equation. Are users aware that their data is being analyzed when calculating the cost of their insurance policy? Is this a technology-related problem? No, the problem is related to the use of technology and the business model. This is why every legal framework must hear the voice of each actor. Users, technology, networks and collaborative governance are the four aspects that should be taken into consideration.

At a global level, the OECD has issued privacy guidelines, which were developed using the multistakeholder model. In the African Union, a process on cybersecurity and data protection was initiated, and members agreed on a guide for these two topics. The Brazilian law is another example, as it went through eight years of public consultations and drafts.

2. Round of specific questions to panelists:

- Pedro Less: ***How can personal data protection favor innovation and the development of digital services in the region?***

In reference to how data protection can increase innovation in the region: In the past, cars drove at a speed of three kilometers per hour as a precaution, not because their engines were slow. Regulations must allow the permissionless development of new technologies, placing users at their center. For example, there is a major ongoing debate on ethical principles for Artificial Intelligence. We have launched seven principles with a focus on privacy. This is why we will never use artificial intelligence for illegal surveillance or for any other activity that infringes upon human rights. The principles seek to guarantee that artificial intelligence will not be used to discriminate or to deliver fewer services to certain users (denying credits, insurance, health services, etc.). Innovation exists and there are ways to achieve innovation in a responsible manner.

Question from the audience on existing regulatory standards: Our criticism of GDPR is that many of the resolutions are expensive for companies, yet they do not protect people. The European Union strongly promotes its system by paying for its dissemination or through its free-trade agreements. Latin America, however, has its own characteristics. Therefore, we should not copy-paste the European model, especially if it is promoted through free-trade agreements.

Question from the audience on informational self-determination: The priority is to provide tools that will allow people to control their information. Offering users a control panel where they can control the information stored by the system and teach them how to use it.

- Eduardo Bertoni - **Beyond the enforcement of general regulations, how can authorities ensure the effectiveness of personal data protection?**

The data protection bill, which is now in the hands of the executive branch, was drafted through a multistakeholder process. The process generated much interest and support. As for other efforts striving for the effectiveness of data protection, even without a new regulatory framework, the Agency has published suggested security measures for databases. We have also made progress in terms of public databases and have guidelines for data collection and processing, particularly as regards the right to information. These things do not require changes to existing legislation. This specific initiative seeks to guide public agencies.

Question from the audience on the independence of data agencies and regulatory compliance by public agencies. In Argentina, the bill created an independent data protection authority, as those paragraphs had been vetoed in 2000. What was supposed to be the regulatory body was established by decree, failing to comply with international standards. The agency in charge of transparency was created in 2016. It had a high level of autonomy, both in terms of budgeting and in the way its authorities were appointed. In addition, the term of office is countercyclical: it begins during one presidency and ends during the next.

- Juan Manuel Haddad - **What are the main challenges for a sustainable digital economy in terms of personal data?**

The priority is to ensure an inclusive Internet for everyone. With regards to personal data, I believe the focus should be on how to increase data security, how to empower people so they will learn how to handle their data, and how to provide alternatives to terms and conditions to make them more transparent. How do we get people to benefit from the data we process? We can also consider data as an asset with a real value. Personal data should be taken into account in free competition processes as well as in the merger of certain companies.

- Iria Puyosa: **How can participation spaces for civil society and the technical community be created within the agencies responsible for data protection oversight and regulation design?**

In the case of Ecuador, there were discussions behind closed doors and no media coverage. We need a participation mechanism that does not rely on the decision of a public official. This is not only due to a lack of education: there is no awareness of the daily impact of data protection. We need to work on educating the general public as a whole.

- Raquel Gatto - **How does the application of data protection regulations affect the founding principles of the Internet? What are the challenges posed by their extra-territorial application or scope?**

The GDPR has extra-territorial effects. The Internet has certain principles known as Internet invariants, which include interoperability and global reach. Each time regulations are applied in a specific jurisdiction, there is a fear of Internet fragmentation. Any regulation must take these principles into consideration.