Session 1: Surveillance and Privacy: Concerns Regarding Cybersecurity and Trust in the Digital Environment

Moderator: Maricarmen Sequera - TEDIC, Paraguay /
CédricLaurant - Son tus Datos, Mexico

Panelists:

Civil Society: Katitza Rodríguez - Electronic Frontier Foundation, Peru
Gisela Pérez de Acha - Derechos Digitales, Mexico
Private Sector: Ana Lucía Lenis - Google
Fernando López - ASIET
Technical Community: Julián Dunayevich - NIC Argentina, Argentina

Remote participation moderator: Daniela Viteri - Universidad San Francisco de Quito, Ecuador

Rapporteur: Leandro Ucciferri - Association for Civil Rights, Argentina

---

Part I

Maricarmen Sequera opened the session. Panelists were divided into groups. First, the panel focused on explaining the context, where we are positioned, the definition of cybersecurity, the growing digitalization of various aspects of social, economic, political and cultural life, and the growing interests of the different actors (government, civil society, academia, the technical community and the private sector). They also commented on cybersecurity, noting that the complexity of threats to the data circulating over the Internet has increased and mentioning legal responses to these challenges.

How to preserve the free, secure and open nature of the Internet. Why many believe that Human Rights need to be sacrificed in order to achieve cybersecurity. What public policies need to be developed to guarantee cybersecurity without affecting Human Rights.

Ana Lucía Lenis: Ana Lucía Lenis started by answering the first question: how to preserve the free, secure and open nature of the Internet. She highlighted that cybersecurity should be seen as a multistakeholder issue. Google is of the opinion that, in many cases, regional debates confuse cybersecurity with cybercrime, i.e., address the strictly criminal part of the issue and the legal definition of the offenses. Cybersecurity is seen as a conversation between industry and government, not as a space where the voices of all actors must be heard. It is an area that requires more work. It is not a matter strictly between two actors, but an open matter that involves fundamental citizen rights. The matter is very relevant for academia and civil society.

In legislative debates, there is a clear lack of knowledge regarding these issues. Thus, legislators need advice from the technical and academic communities.

User security is a shared responsibility that needs to start with education. Many of the attacks suffered by citizens are due to a lack of knowledge of the measures they can take to protect themselves.

Regarding cybercrime, territoriality is clearly a factor, as these crimes do not recognize national borders. They must be correctly defined to avoid certain activities being declared illegal because of legislators' lack of knowledge.

Katitza Rodríguez: The big issue with cybersecurity is that there are no clear priorities in the definition of digital security. The concept is too nebulous and has different meanings for different people. It combines different issues that require different solutions and treats them as a monolithic concept. Measures are needed to strengthen the economy. Clear policies with clear risk analyses and are needed. The proportionality of any actions must also be measured. One way of protecting digital security is by means of secure infrastructure and the use of strong point-to-point encryption. It seems ironic that, although there is a permanent quest to protect digital security, public policies undermine security by creating backdoors. Therefore, instead of promoting encryption, public policies that minimize encryption are being promoted.

How to protect the free and open nature of the Internet? Criminal legislation and public policies seek to guarantee that adopted measures are necessary, proportional, appropriate and reasonable. Civil society has developed 13 international principles to promote respect for Human Rights in the interception of communications in order to meet international Human Rights and due diligence standards. Electronic Frontier Foundation and Derechos Digitales have issued a report analyzing these principles within the framework of international Human Rights standards.

Gisela Pérez de Acha: Gisela Pérez de Acha agreed that the definition of cybersecurity is quite vague. The term “cyber” is used with less and less meaning. This brings sensationalism to the issue of cybersecurity, which has been used within the region to undermine Human Rights. She suggested addressing how cybersecurity affects gender issues. The proposed definition is to preserve the underlying critical infrastructure both online and offline through policies and education. The aim is to protect personal integrity.

There are two categories: on the one hand, cybercrimes and content-related crimes (copyright issues should not be included in cybersecurity debates); on the other hand, national security, a concept which is also abused and where emphasis must be placed on how it is used.

She mentioned the case of Sepúlveda, the hacker who rigged elections in Colombia.

How to preserve critical infrastructure: we need to consider which body will be in charge of investigating these actions.

The case of a database containing information on Mexican individuals that was uploaded to an Amazon Cloud server and then leaked was discussed, as well as the Company's response to the request to remove it.

What happens when victims are part of vulnerable groups, LGBT or women due to gender issues?

The Internet is not only about money. Information is also a major asset, particularly if it relates to nude images, dissidents, etc. For certain attackers, these are extremely valuable assets. Examples include “sextortion,” where criminal hackers access a victim’s webcam, take photographs or record videos of everything they see, and then request a monetary ransom. A large part of the victims are underage.

How to change the focus of cybersecurity, understood as cybercrime, to include users’ bodies and identities.

Fernando López: Public policies are not in line with the issues at hand. This is why these governance forums are so important.

From the perspective of a public policy analysis, the first issue is that regulations are always behind public issues. When we realize we have a problem, it has already become evident to all and exceeds the way we understand problems.

Our current reality is very different from the one we once knew. Regulatory models are being transformed but have yet to fulfill users' needs.

The role each actor must play remains unclear. Governments try to take over these roles, but sometimes become a part of the problem. In this sense, the main concern is which alternative would best promote the ecosystem's development.

He believes there is agreement regarding the fact that the focus should be on the user. How to guarantee user rights and their trust when using technology. Increased user trust will translate into innovation and access for more individuals. This requires a clear understanding of what is going on and how users interact with new technologies.

Governments must be capable of assessing the measures that have been adopted and how to provide the certainty needed for people to continue receiving information and fueling development in the field of telecommunications.

Today, society has greater awareness and is gradually demanding stronger guarantees that authorities will allow conducting online activities in secure manner. Here education is key. Strengthen users so that they will be aware of their rights and empower them to claim these rights.

Telecos have traditionally been required to protect personal data and a procedure exists in case these rights are violated. As new services are launched, however, there is no criteria for protecting user security.

Within the digital ecosystem, all actors must be held to the same standards; otherwise, the risk will remain. It is essential for the industry to rethink the value of personal data and the services offered free of charge that have a specific cost for users who must surrender their personal data. Users might be willing to share their data, but in most cases they are not aware they are doing so.

It is important to consider the way we, as experts, can help users make informed decisions. People should be at the center of regulatory policies. What is more, people should be conscious of their possibilities. It is not clear who users can turn to or how they can avoid the use of their data. Sometimes it is unclear which regulations apply to global services. Debates among ordinary citizens are needed.

Alternatives should be taken into consideration in order to have an open Internet that is respectful of Human Rights and public policies to support it.

Julián Dunayevich: Julián Dunayevich addressed cybersecurity challenges from the point of view of a ccTLD. Tools, guidelines and methods are needed to defend users from attacks and third-party accusations. Internet infrastructure is as critical as that of other sectors (energy, water). Different areas are responsible for and must manage their own infrastructure, as a failure of their systems would have a major impact on the Internet and on national services.

He highlighted different projects and approaches to infrastructure resiliency. LACTLD is implementing a project for sharing infrastructure among different countries of the LAC region in order to work collaboratively and achieve greater robustness.

Clients are also a target (server queries). Work is being carried out so that there will be greater certainty for browsers looking up non-malicious URLs.

Given the resiliency of their infrastructure, they are prepared to perform “disaster recovery.”

Cybersecurity requires working with multiple stakeholders. Each actor can help find a solution. Therefore, it is essential to work in coordination with the various sectors at both national and regional level.

There is a need to work with each of the areas that act based on third-party accusations and define the steps to be followed in such cases. To be successful, protocols must be established.

ccTLDs have teams that receive many complaints and must act in case of cybersecurity incidents. They have the chance to communicate with other regional groups and this allows them to build a knowledge base on how to manage incidents. ccTLDs have an advantage in that they already have certain elements that allow them to decide the best course of action upon receiving a complaint (e.g., contact details for each domain name) and this allows them to quickly contact the holder and provide a solution, not unilaterally but within the legal framework in force.

They have protocols and mechanisms for determining jurisdiction and competence (e.g., whether an IP belongs to another country or whether the domain submitting the claim has nothing to do with the specific ccTLD, in which case the incident must be forwarded to whoever is responsible), incident categorization, notification and reporting channels, scope and actions.

Incidents are categorized. This allows transferring information to the courts so they can continue the process.

Protecting its infrastructure, collaborating and sharing experiences, implementing common policies, having a regional cybersecurity model, agreeing on how to manage these situations, and having reliable information systems that will allow faster response times are essential for a ccTLD.

Cédric Laurant: Cédric Laurant posed questions to the panelists and then gave the floor to the audience.

He began by asking a question to Ana Lucía. The private sector should encourage trust among users. In Mexico, Uruguay, Colombia and Costa Rica, the organization in charge of protection should promote trust by proving that companies know how to act in case of data breaches. What measures should be implemented?

Ana Lucía: Each country's databases should be delimited. All notices must be given under strict compliance with the law. Many databases are located outside national borders. As regards the publishing of incidents, in many cases Google recommends collaboration between private companies and sharing information with government agencies. However, work is still needed for governments to share perceived risks with the private sector so that they can be better prepared for future incidents. Each case should be considered separately, taking into account national regulations.

Question to Katitza: What would be the most effective measure for promoting the use of point-to-point encryption?

We are not asking for legislation. Instead, we are asking for education so that people will understand the risks of using technology. People must use technology, but they must also understand the risks involved. Encryption is a way to avoid such risks. Encryption enables secure communications. The use of this type of encryption must be promoted by means of public education and public policies. Cybersecurity Day campaigns did not include any comments regarding the use of encryption.

Cédric: A recent campaign recommended avoiding sexting. However, this practice will not disappear and should not be regarded negatively. There was no talk of encrypting cell phone contents or messages.

Gisela: Consensual sexting should be differentiated from sextortion or revenge porn and image abuse. Encryption would avoid or make it more difficult for third parties to access

such content. Above all, encrypting communications should not be forbidden, as this helps protect against cybercrime.

Question from the floor:

Renata Aquino (Brazil): Renata Aquino asked about cases in Latin America and finding a solution.

Katitza: Electronic Frontier Foundation published a surveillance self-defense guide that teaches how to use secure technology and careful practices so that teachers, activists and common citizens can defend themselves against cybercriminals. The guide shows how to perform a risk analysis and how to protect information in specific cases. Not everything can be protected from everyone, so a case-by-case analysis should be conducted. The guide is available at https://ssd.eff.org

Part II

Eduardo Rojas (Fundación Redes): What can you tell us about current trends and what are your recommendations on how to face the wave of legal reforms in different countries, cybersecurity, the regulation of social networks, grooming, etc.? There seems to be confusion between the protection of assets and the protection of individuals.

Ana Lucía Lenis: There are multiple legislative processes going on throughout the region. The private sector is trying to take advantage of Internet governance forums to guide the debates regarding these legislative projects. These issues should be addressed by multiple stakeholders. Local governance forums are a good example of this (Mexico, Colombia). Multiply these local debates, inviting universities and other actors, so that they can have an impact in each country.

Katitza: Comparing experiences and sharing best practices is very useful. Regarding cybersecurity, the OECD published a report – an example of a multistakeholder paper – that promotes conducting a risk analysis of what needs to be protected, against whom and how, for the purpose of developing public policy that provides a proportional and reasonable solution to each specific risk.

Gisela: Keep criminal law to a minimum. Particularly in the case of Latin American jails, adding fuel to the fire would be excessive.

Fernando: Mention of the Mexican Cybercrime Bill, also known as the Fayad Law. An open consultation process driven by civil society led to the withdrawal of the bill.

Question from **Manuel Alcántara**: Manuel highlighted the confusion between cybersecurity and cybercrime. He asked Ana Lucía to share a definition that will clearly differentiate the two terms or to provide examples to help specify the thin line that separates the two. He asked Julian to share recommendations on how to create an incident response team and which method or protocol is used by NIC Argentina to submit evidence to the courts.

Ana Lucía: The private sector notices that cybersecurity debates focus on cybercrime (the penalization and criminalization of various behaviors) and believes that multistakeholder debate should be encouraged. Other points of view are not taken into account, beginning with education. Particularly taking into account fundamental rights and due process.

Julián: As for building a CSIRT, understanding the role of each actor and defining agreements between them is key. Discussions must involve the highest possible number of people. In many cases, lack of proper procedures can spoil evidence, which is why procedures must be defined for each case. As a ccTLD, their service area is very specific, so it is essential to articulate with all parties and even create national CSIRTs that can respond as quickly as possible.

Salvador Camacho (ISCO Mexico): Question for Julian: What is NIC Argentina doing to lower cybersquatting rates? How knowledgeable are the prosecutors handling these cases in Argentina?

Julián: There are specific areas and policies at local and national level and it is possible to work with each of these. Sometimes we work on this type of policies (preventing the creation of domain names for the purpose of perpetrating attacks), but generating lists of names that cannot be justified means walking a very fine line.

Question: Is it true that users are responsible for vulnerabilities?

Ana Lucía: Users are precisely the challenge companies must face: providing users with greater control so they can decide what they want to do with their data. This has more to do with education than with blocking access to innovation. The discussion about protecting user data privacy is not a discussion among telcos, OTT, etc. Many regulations and companies were created before *habeas data* and data protection laws. The industry should deal with this together. Ana Lucía also highlighted the security measures introduced by Google for Android to provide users with greater control over app permissions. Seeking to solve user issues, the information that is collected has been minimized.

Katitza: Civil society is not suggesting that people stop using technology. We are telling companies that people should be in control of their data, that it should be possible to delete data, that a process is needed to anonymize data, how long data is stored, etc. It is very easy to identify a person in an anonymized database.

Fernando: Expressed concern with the language that is being used. People do not question whether they are vulnerable or whether they can decide. People should be able to make conscious, informed and practical decisions. Some people are not aware of how their data is being used. Users must be aware of and understand privacy policies and their right to be properly informed in order to make proper decisions.

Ana Lucía: We depend on one another, so we should not be attacking ourselves within the same ecosystem. All things can be improved. All parties are responsible for privacy policies and terms and conditions. There are teams working so that people can have access to clearer information.

Katitza: The private sector tries to protect privacy. The major problem concerns massive data collection. Once this data exists, it may fall into government hands and this represents a risk. The larger the amount of data collected and maintained, the more information that can be provided to the government.

Question: What actions should telecommunication companies and governments implement? When does this become a gender issue affecting women?

Gisela: First, victims should never be blamed (the "mini-skirt effect"). As to sexting, initiatives that consider sexuality as "bad" or "terrible" should not be supported and should be banned off-line. The risk of sexting is that a third-part might publish your information without your prior consent. Authorities don't know how to react when faced with these situations. Instead of banning sexuality, the priority should be to educate on the risks involved. Gender issues should be included in all of these agendas, as they are currently being left aside.

Jessica (Intermundi): Money still decides what is important on the Internet. There is hypocrisy in the way words are managed and in the fact that the companies that own the information have the same responsibility as governments, users, etc. Also, what type of policies should be developed so that companies are unable to harass citizens who don't read or understand privacy policies. What can they do if they are aware of this harassment?

Katitza: There are many tools. For instance, data protection laws seek to place companies and individuals/users at the same level. This is not a trend within the region. There are also tools that can be used to block information on the Internet. For example, PrivacyBadger, tools that allow browsing the Internet in a secure and anonymous manner, and guides that teach users how to take control of their data. Two strategies: a legal strategy and a personal strategy.

Question: In addition to raising awareness and trying to affect policy development, how can civil society have an impact on these issues?

Katitza: People – not only organizations – should be able to campaign for the protection of individual rights. Not everything is about education.

Oscar Robles (LACNIC): The challenge of generating trust should be addressed in a multistakeholder fashion. Each group has its own responsibility in the matter. For example, the technical community creates encryption protocols. Each sector has its own role. What can we do as a multistakeholder organization to help end users, the most vulnerable party to this relationship?

Julián: Training and educating each actor involved in developing legislation is key. Typically, judges don't know how to deal with these topics – even certain government agencies don't know how do it. Their lack of knowledge stems from the fact that all they see is what the court system shows them.

Question: Considering the entire civil framework as a reference, what can be done other than educating users and the court system?

Fernando: More transversal policies are needed.

Katitza: Many organizations prepare reports containing specific results.

Monica Arroyo (Observatorio de la Juventud): Question focused on the right to information. Has any though been given to avoiding page upon page of terms and conditions?

Katitza: No company will say it is against privacy policies. What they try to do is explain their contracts in simple terms. When one asks a company what it is doing with one's data, many do not provide a clear and direct answer. In Peru, the data protection law is used to censor citizens.

Gisela: Consent needs to be free and informed; otherwise, it cannot be regarded as actual consent. Term and condition agreements are neither free nor informed.

Presentation by Gisela – Hacking Team in Latin America

Galileo is the name of the software sold by Hacking Team. It is similar to having a public official watching and copying what we do on our personal devices.

In Ecuador, there is evidence that the software was used to spy on Carlos Figueroa.

In Colombia, the DEA was intercepting all Internet traffic.

In Mexico, those who bought the software had no difficulties using it. It was the Latin American country that spent the most on purchasing the software.

In Chile, the investigative police claimed they needed this software to advance their criminal investigations.

With the exception of Mexico and Colombia, the software goes against national legal standards in the region.

PackRat and FinFisher are also used.

We need to ask ourselves how malware affects cybersecurity and what role the private sector should play. We need to define what the term "surveillance capitalism" means and start predicting where we would like to go, what we are looking for, and how this helps major companies and governments.

Also, given that our laws do not allow the use of this type of software, to what extent are Hacking Team, PackRat and FinFisher responsible?

Malware is one of the main tools used to silence dissidence.