Cybersecurity, Privacy and Trust: Trends in Latin America and the Caribbean

FGV | **Fundação Getúlio Vargas**
Marília Maciel, Nathalia Foditsch, Luca Belli and Nicolas Castellon

Introduction: key issues at stake

The goals of cybersecurity strategies are usually twofold: i) To protect society against cyber threats; and ii) to foster economic and social prosperity, in a context in which key activities are based on the use of Information and Communication Technologies (ICTs). In order to fully achieve these goals, national cybersecurity strategies should be harmonized with fundamental values and rights, such as privacy, freedom of expression and due process, as well as with key technical principles that have allowed innovation on the Internet, such as openness, universality and interoperability.[1] The respect for human rights and these architectural principles is key to strengthening trust and fostering economic growth.

The respect for human rights and these architectural principles is key to strengthening trust and fostering economic growth.

In developed regions of the world, cybersecurity strategies have a holistic approach, encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects.[2] Sovereignty considerations in cybersecurity policy making are increasingly relevant and more involvement from the military and the intelligence branches of the government are evident.[3] When cybersecurity strategies are exclusively centered on military and intelligence concerns, however, they may not encompass the adequate balance between security and rights, such as privacy and freedom of expression and association.

The more data that is exchanged with the use of ICT, the more that cybersecurity and privacy concerns will rise. Moreover, a growing trend of mandatory data retention requirements justified under security reasons may conflict with privacy, anonymity, and freedom of expression, if the limits of data retention and the use of retained data are not grounded on principles, such as necessity, proportionality and due process.

Tendencies at the Latin American and Caribbean level

Awareness of the importance of developing cybersecurity strategies is increasing among countries in the Latin American and Caribbean (LAC) region. Some of them already have a strategy in place, such as Colombia, Jamaica, Panama, and Trinidad and Tobago. Other countries are in the process of developing one, such as Costa Rica, Dominica, Peru, Paraguay and Suriname. The level of maturity of these strategies varies, including in terms of providing a framework for cooperation among governmental agencies and with external actors.

In the LAC region, the army and the national security agencies have not been widely established as coordinators of cybersecurity policy development. This provides a positive window of opportunity to develop cybersecurity policies in multi-stakeholder platforms, including different governmental branches, academia, the technical community, civil society, and the private sector. LAC countries will be able to advance a new notion of cybersecurity that is not derived only from the military and defense domains, but also from human rights.

Multi-stakeholder cooperation is noticeable in many LAC countries. It can be found, for example, in the creation of Computer Security Incident Response Teams (CSIRT), which are widespread across the region. The collaboration among national CSIRTs has allowed the exchange of knowledge and good practices, leading to more secure and robust communications systems. Improvement of national capabilities is important to boost confidence in private and public digital services, which paves the way for an emerging digital economy and reliable e-governance.

One of the main concerns raised in LAC countries has been defining and penalizing cybercrimes, by either creating new laws or updating existing ones.[4] Brazil offers an interesting case. A draconian bill containing cybercrime provisions was proposed before Congress and met strong opposition from academics and civil society.[5] The government was convinced that, rather than a criminal law, Brazil needed to define the rights and responsibilities of Internet users. This culminated in the approval of the Civil Rights Framework for the Internet (Marco Civil), relating to issues such as the protection of fundamental rights online, network neutrality, intermediary liability, responsibilities of the public sector and data retention.

Another regulatory trend in the LAC region is an increasing concern about the protection of online privacy and personal data. After the Snowden revelations in 2013, the awareness of the intersection between cybersecurity and personal data has become clearer, as it involved daily electronic communications. As the Internet has become essential for Latin American and Caribbean socio-economic development, the consequences of failing to protect it can impact trust in online activities, and potentially have negative consequences on the Internet economy and society as a whole.

In his 2014 study entitled, "Latin America and protection of personal data: Facts and figures (1985–2014)", Nelson Remolina Angarita found that 70% of LAC countries have some type of data protection within their constitutions.[6] Moreover, different countries have already enacted (e.g., Argentina, Antigua and Barbuda, Colombia, Costa Rica, Mexico, Peru and Uruguay) or are currently drafting data protection laws (e.g., Brazil).[7] In spite of this, mandatory data retention is a growing practice in the region and, in many cases, stored data can be obtained without a court order.

Data retention may be necessary in some cases to collect evidence and to enable the investigation of cybercrimes. However, the collection of personal data for investigation purposes should be limited to what is necessary for the prevention of a real danger or the suppression of a specific criminal offense.[8] Therefore, bulk data collection is at odds with this provision. Although national legislations further regulate special cases, this should be done in a way that does not undermine these core principles. Data processing should also be adequate, relevant and not excessive in relation to the purpose for which they were stored.[9] Without establishing the limits for data retention, privacy rules will continue to be curtailed and this may seriously jeopardize the fundamental rights of Internet users. Moreover, this might represent a costly regulatory burden for companies, especially those that are of small and medium size. These are some examples of how these provisions are applied in the region.

In Argentina, a law[10] was challenged before the Supreme Court as it authorized the interception of phone and electronic communications without proper guidelines for the applicability of the provisions.[11] Moreover, it required that data be stored for 10 years. The law was declared unconstitutional by the Supreme Court in 2009.

In Brazil, the Civil Rights Framework for the Internet (Marco Civil)[12], enacted in 2014, is perceived as a progressive document protecting citizens' interests. Nevertheless, its provisions relating to mandatory data retention might arguably tip the balance towards security concerns over privacy and civil liberties. According to the Marco Civil, service and application logs should be stored for six months, whereas connection logs should be stored for one year.[13]

It is also necessary to balance the costs and benefits of data retention provisions

In Mexico, a telecommunications law[14] with different data retention provisions was enacted in 2014. Retained data can be accessed by public authorities without a court order. Moreover, some data should be stored up to 24 months, which corresponds to a 12-month increase compared to the standard that was already in place.

In Paraguay, a proposed bill known as "pyraweb"[15] required Internet service providers to store metadata for one year.[16] Moreover, no court order was needed for public authorities to request the data. After facing political pressure from civil society groups, the bill was rejected by the Senate.

The way forward

Considering the trends described in this document as well as the necessity to protect the full enjoyment of Internet users' human rights, some recommendations can be made. These recommendations do not encompass the wide range of issues pertaining to the balance between security and the protection of human rights. However, they address some fundamental points to be considered by countries willing to safeguard rights while tackling important security concerns.

Defining and enforcing sound privacy and data protection regulatory frameworks

It is essential to balance the provision of security with the need to properly safeguard the rights of individuals. The approval and implementation of sound privacy and data protection frameworks help to achieve this goal. It is also necessary to balance the costs and benefits of having data retention provisions. While civil society groups are worried about privacy issues, industry is concerned with the regulatory burden they would have to face, which translates into higher costs to operate their businesses. Principles such as necessity and proportionality should be used to assess the adequacy of these provisions.

Creating national sustainable multi-stakeholder platforms

It is important to consider the different aspects and implications, as well as the technical feasibility of enacting new regulations. Civil society groups, the academic and technical communities, as well as industry representatives are able to provide valuable expertise from their perspectives, and help design sound regulatory frameworks in a sustainable fashion. These multi-

stakeholder networks could help to develop a forward-looking approach to cybersecurity in the region, which takes into account technological developments, such as datafication, big data and the Internet of Things, and considers the impacts of these technologies on security and privacy.

Strengthening international cooperation

Cybersecurity has been increasingly mainstreamed at the international level.[17] It is important to create channels for multi-level cooperation between national governments and the regional and global international organizations working in the field. Strengthening regional cooperation can also facilitate a meaningful inclusion of countries from the region in ongoing global discussions. The borderless nature of the Internet enhances the importance of international cooperation and the harmonization of legal frameworks.

Conclusion

This document provided a brief overview of how LAC countries have tackled the interplay between cybersecurity and fundamental rights, focusing particularly on the right to privacy and to the protection of personal data. It also offered suggestions on the way forward, such as the development of sound privacy and data protection frameworks, the strengthening of international cooperation and the creation of clear frameworks for collaboration amongst interested stakeholders. It is essential to encourage the development of appropriate democratic governance mechanisms—at the national and international levels—based on a multi-stakeholder effort. ■

Notes

1. DAIGLE, Leslie. "On the Nature of the Internet". Global Commission on Internet Governance Paper Series nº 7. March, 2015. **https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf**
2. OECD. "Cybersecurity policy making at a turning point: Analyzing a new generation of national cybersecurity strategies for the Internet economy". OECD, 2012, p. 12.
3. Id, p. 14.
4. OAS; Symantec. "Tendencias de Seguridad Cibernética en América Latina y El Caribe". 2014. **http://www.symantec.com/content/es/mx/enterprise/other_resources/b-cybersecurity-trends-report-lamc.pdf**
5. Bill 84/99.
6. Remolina Angarita, Nelson. Aproximación constitucional de la protección de datos personales en Latinoamérica. Universidad de los Andes, 2014. **http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf**
7. See **http://participacao.mj.gov.br/dadospessoais/**
8. Council of Europe Committee of Ministers. Recommendation no. R (87) 15 regulating the use of personal data in the police sector.
9. Council of Europe. Convention for the Protection of Individuals with regard to Aumotatic Processing of Personal Data. ETS 108, Article 5.
10. Law 25.873 and Decree 1563/04.
11. Supreme Court of the Republic of Argentina. Halabi, Ernesto c/PEN ley 25.873 y decreto 1563/04 s/amparo. Available at **http://defensoria.jusbaires.gov.ar/attachments/1126_escuchas%20telefonicas%20-%20Ley%20Espia.pdf**
12. Law 12.965/14.
13. See articles 13 to 15 of Law 12.965/14.
14. Ley de Telecomunicaciones y Radiodifusión, 2014.
15. The word "pyraweb" alludes to the informers of dictatorship times (pyrague, in guaraní—an indigenous language).
16. The bill is available at **http://odd.senado.gov.py/archivos/file/Proyecto%20de%20Ley8.pdf**
17. Cybersecurity is among the priorities identified in the ten-year review process of the outcomes of the World Summit on the Information Society. The WSIS+10 Vision reflected the complementarity between security and privacy and defined that "building confidence and security in the use of ICTs, notably on topics such as personal data protection, privacy, security and robustness of networks", should be one of the priorities beyond 2015. In December 2013, the UN General Assembly adopted Resolution 68/167, which expresses deep concern at the negative impact that surveillance and interception of communications may have on human rights. Resolution 69/166, approved in 2014, builds on the previous one, calling for access to effective remedy for individuals whose right to privacy has been violated. On March 26, 2015, the Human Rights Council created the mandate of a Special Rapporteur on the right to privacy. However, intergovernmental cooperation on cybersecurity is still fragmented across different organizations and fora in the United Nations. In parallel, a yearly Global Conference on Cyberspace (GCCS), known as the "London Process", has brought together governments and other stakeholders to discuss issues on a broad range of topics related to cybersecurity.

Marília Maciel

Researcher and coordinator of the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. She serves as a counselor at the Generic Names Supporting Organization of the Internet Corporation for Assigned Names and Numbers (ICANN) representing the Non-commercial Stakeholder Group. She is a member of the Advisory Board on Internet security, created under the Brazilian Internet Steering Committee. Marília is a PhD candidate in International Relations at the Pontifical Catholic University (PUC – Rio de Janeiro).

Nathalia Foditsch

Researcher at the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. She has worked for international organizations, the Brazilian Federal Government, as well as law firms and think tanks on communications law and policy matters. Foditsch is a licensed attorney and holds a Master's degree in Law and another in Public Policy, both from the American University.

Luca Belli

Researcher at the Center for Technology and Society of the Getúlio Vargas Foundation School of Law in Rio de Janeiro. He holds a PhD in Public Law from the Université Panthéon Assas (Paris II) and is a founder and coordinator of the Dynamic Coalition on Network Neutrality, as well as of the Dynamic Coalition on Platform Responsibility, multi-stakeholder components of the United Nations' Internet Governance Forum.

Nicolás Castellón

Visiting researcher at the Center for Technology and Society of the Foundation School of Law in Rio de Janeiro. He specializes in cybersecurity governance, focusing on critical infrastructures and humanitarian uses for Big Data. He holds a Master's degree in Crisis and Security Management from Leiden University's Faculty of Governance and Global Affairs.

FGV DIREITO RIO
CENTRO DE TECNOLOGIA E SOCIEDADE

FGV | Fundação Getúlio Vargas
www.portal.fgv.br
marilia.maciel@fgv.br