Regulations in Cyberspace in Latin America and the Caribbean: challenges and opportunities

By: Dr. Boris Saavedra with Emma Corcodilos [1]

If we continue to develop our technology without wisdom or prudence, our servant may prove to be our executioner.

Omar Bradley

Abstract

Cyberspace vulnerabilities constitute a major challenge to decision makers in Latin America and the Caribbean. There is a growing concern in the region for the lack of an effective legal framework to control this limitless environment. All legal systems used in the region present their own challenges, but within each one is a lack of capacity to efficiently regulate cyberspace. Additionally, while the public sector focuses on the common good and the private sector focuses on profit, both must be united under a common regulatory framework that facilitates the objectives of security for society. This essay addresses the current status of cyberspace regulations in Latin America and the Caribbean (LAC) and the challenges faced in implementing them.

Keywords: Regulations, Public-Private Partnership, civil and common law systems, resilience

Introduction

The growing speed of cyber capabilities resulted in a vast increase in security risks around the world. Countries therefore struggle to implement regulations to protect their societies quickly enough to keep up with cyber threats that emerge daily. While many other areas of security and defense are more easily regulated, cyberspace has one distinct characteristic: it is not constrained by boundaries. This limitless environment of

[1] Dr. Boris Saavedra Associate Professor at WJPC, National Defense University
Ms. Emma Corcodilos Research assistance at WJPC, National Defense University
Disclaimer. The views expressed in this testimony are my own and do not necessarily reflect the views of the William J. Perry Center for Hemispheric Defense Studies, National Defense University, or the Department of Defense.

cybersecurity also poses a challenge to the international community in containing and controlling such threats.

The objective of this essay is to provide the current status of cyberspace regulations in Latin America and the Caribbean (LAC) and the challenges faced in implementing them. This is done by examining the historical developments of regulations in various countries focusing on the three legal systems used in the region. Because all the countries discussed either utilize a civil legal system, a common legal system, or a mixture of both, the contrast in efforts and systematic challenges for all three systems will also be discussed as possible results of lacking regulatory abilities.

Above all, the resilience of the public and private sectors is essential to upholding national security around the world, especially regarding cyberspace. With the public sector focused on protecting the common good, and the private sector focused on strong business profits, both must come together under one regulatory framework in order to fulfill their security goals. This is seen most successfully through the efforts of the European Union (EU), specifically in the area of privacy, which is one of the many critical areas of cybersecurity that require an effective regulation for the security of cyberspace. The EU model is often followed by countries around the world, including those in LAC. For a general sense of cybersecurity regulations in LAC, **Table A** outlines each country in the region with cybersecurity legislation framework (such as those for data protection, cybercrime, e-government, information technology (IT), critical infrastructure, and various additional areas) as well as their legal system and the date of implantation.

Table A

Country	**Legal System**	**Cyberspace Legislation Title**	**Date**
Antigua & Barbuda	Common Law	Electronic Crimes Act	2013
		Data Protection Act	2013
Argentina	Civil Law	Personal Data Protection Law	2000
		Computer Crimes Law	2008
Bahamas	Common Law	Computer Misuse Act	2003
		Data Protection Act	2003
Barbados	Common Law	Computer Misuse Act	2005
Belize	Common Law	Telecommunications Act	2002
		Electronic Transactions Act	2003
		Interception of Communications Act	2010

		National ICT Strategy	2010
		National E-Government Policy	2015
Bolivia	Civil Law	General Law on Telecommunications, Information and Communication Technologies	2011
		eGovernment Implementation Plan	2017
Brazil	Civil Law	Information and Communications Security and Cyber Security Strategy	2015
		General Data Protection Law	2020
Cayman Islands	Common Law	Data Protection Law	2019
Chile	Civil Law	Law No. 18.168 (General Telecommunications Act)	1982
		Law No. 19.628 (Personal Data Protection Law)	1999
		National Cybersecurity Policy	2017
Colombia	Civil Law	Law 1237 (Protection Information and Data)	2009
		CONPES 3701 (Policy Guidelines on Cybersecurity and Cyberdefense	2011
		Law No. 8968 (Personal Data Protection Act)	2011
		Law 1581 (Data Protection Law)	2012
		CONPES 3854 (National Digital Security Policy)	2016
Costa Rica	Civil Law	National Cybersecurity Strategy	2017
Cuba	Civil Law	Safety Regulations for Information Technologies	2007
Dominican Republic	Civil Law	Law No. 53-07 (Against Crimes and High Technology Offenses)	2007
		Law No. 172-13 (Protection of Personal Data)	2013
		Decree No. 230-18 (Establishing and Regulating the National Cybersecurity Strategy)	2018
Ecuador	Civil Law	Law No. 2002-67 (E-commerce, Electronic Signatures and Data Messages)	2002
		National Plan for Electronic Governance	2017
El Salvador	Civil Law	Special Law Against Cybercrime and Related Offenses	2016
French Guiana	Civil Law	Information Systems Defense Strategy: France's Strategy	2011
		Cyber Defense Pact	2014
		National Digital Security Strategy	2015
		Transportation of the EU The Security of Network and Information Systems Directive	2018

Grenada	Common Law	ICT National Strategic Plan	2006
		Electronic Crimes Act	2013
Guatemala	Civil Law	National Cybersecurity Strategy	2018
Guyana	Mixed Law	Cybercrime Bill	2018
Honduras	Civil Law	Electronic Transactions Act	2006
		Cybercrimes Act	2010
		Digital Agenda of Honduras	2013
Jamaica	Common Law	National Cyber Security Strategy	2015
Mexico	Civil Law	Protection of Private Personal Data	2010
		National Cybersecurity Strategy	2017
Nicaragua	Civil Law	Data Protection Law No. 787	2012
Panama	Civil Law	National Strategy for Cyber Security and Critical Infrastructure	2013
Paraguay	Civil Law	Law No. 4439 (Amending the Penal Code)	2011
		Law No. 1962/02 (Data Protection Law)	2015
		National Cybersecurity Plan	2017
Perú	Civil Law	Law N. 29733 (Personal Data Protection Law)	2011
		National Policy on E-Government and Information Technology	2013
		Law N. 30096 (Computer Crimes Act	2014
Puerto Rico	Mixed Law	Act No. 111 (Citizen Information of Data Banks Security Act)	2005
		Act No. 234	2014
St. Kitts & Nevis	Common Law	National ICT Strategic Plan	2006
		Electronic Crimes Act	2009
St. Lucia	Mixed Law	Computer Misuse Act	2011
		National ICT Policy and Strategy	2013
		Data Protection (Amendment) Act	2015
St. Vincent and the Grenadines	Common Law	Privacy Act	2003
		Electronic Evidence Act	2004
		Electronic Transactions Act	2007
		National ICT Strategy and Action Plan	2010

Suriname	Civil Law	Telecommunications Facilities Act	2004
Trinidad and Tobago	Common Law	Data Protection Act	2011
		National Cyber Security Strategy	2012
Uruguay	Civil Law	Law No. 18.331 (Protection of Personal Data)	2008
		Presidential Decree 452/009	2009
		Presidential Decree 92/014	2014
		Digital Agenda 2020	2017
Venezuela	Civil Law	Special Law on Computer Crimes	2001
		Law on Electronic Signatures and Data Messages	2001
		Info government Law	2014

Legal Systems and Public Private Partnerships

Most countries in the world utilize a civil law system, a common law system, or a mixture of both. Much of Central and South America utilizes civil law, which finds its roots in the Roman legal system. There is almost always a written constitution in these countries based on specific legal codes (i.e. civil codes, constitutional law, etc.). Civil law systems only recognize laws passed through the legislative system to be binding law. Common law systems, on the other hand, are influenced by case law. While many of these countries utilize a constitutional and legislative process, they also consider judicial decisions to be binding law. Although many of these countries find a legal foundation in the doctrine of *stare decisis,*[2] courts have the ability to create new interpretations of the law when given different facts in a new case.[3] This allows for common law systems to be more malleable, as they do not always have to go through the lengthy legislative process in order to implement new regulations.

Regardless of the legal system, Public Private Partnerships (PPPs) are an essential element of cybersecurity, as the public and private sectors are the two most important actors in the race against cyber threats. Their resilience depends on cooperation, as practiced through PPPs. Before analyzing each country's challenges and regulations individually, it is first important to understand the challenges of creating PPPs through contracts given a country's legal system. Civil law countries do not have much freedom of contract, as parties to the contract are often unable to decide which provisions they want to contract out of, and many provisions are not expressly included, but rather implied through other underlying laws that make it unnecessary to repeat them contractually. This can be problematic because of the ambiguity of the contract's rules.

[2] *Stare decisis* is the principle that current cases should be decided in congruence with past precedent.

[3] PPLRC, "Key Features of Common Law or Civil Law Systems," *World Bank Group*, September 6, 2006, https://ppp.worldbank.org/public-private-partnership/legislation-regulation/framework-assessment/legal-systems/common-vs-civil-law#Common_Law_System

Contracts in civil law systems are shorter due to their omission of specific language, leaving disputes between parties to be resolved by operation of law after the creation of the contract. Regarding cybersecurity regulations, PPPs in a civil law system leave much room for error due to debatable language. For instance, legal language regarding the protection of "critical infrastructure" lacks clarity, as the definition of "critical infrastructure" may change through different legislation over time.[4] In addition, because civil law systems are set in codified law, many PPP agreements will be unenforceable if they are not in exact congruence with the country's laws. This will set PPPs back, as contracts often need to be rearranged in order to adapt to a country's laws. Common law systems, on the other hand, have much more freedom of contract. Unlike civil law systems, very few provisions are implied. While this requires a longer contract, it leaves less room for dispute in the long run. In addition, common law allows PPP contracts to be much more flexible because most provisions are permitted if they are not expressly prohibited by a country's laws or regulations. This allows for PPPs to be more easily established, and any question of legality is decided by the courts rather than by already established laws.[5]

Cyberspace Regulations in Countries using Civil Law Systems

For the analysis of the LAC countries that use the civil legal system, we have selected Brazil and Colombia as the countries that have made the most progress in establishing legislation for cyberspace activities. Among various countries within the LAC region, Brazil is one of the most economically advanced that utilizes civil law. Given its mass adoption of information communications technology (ICT), Brazil is a top target for cyber-attacks.[6] The Brazilian Federal Constitution first guarantees privacy protection as a fundamental right of all people. Brazil's most recent piece of legislation dealing with cybersecurity issues is the Brazilian General Data Protection Law (LGPD, when translated to Portuguese), which focuses on regulating the use and protection of personal data by the public and private sectors.[7] The LGPD followed the EU's implementation of their General Data Protection Regulation (GDPR) and contains many similar provisions. The implementation within the Brazilian system was challenging, as it took six years to be passed by Congress and will not be implemented until 2020. In this case, regulations run the risk of being outdated due to the dynamic pace of cyber risks. This is one of

[4] Yana Weaver, "Basic Differences Between A Common Law System And A Civil Law System In Terms Of Contracts And Business," *LSL*, May 31, 2016, lslcpas.com/basic-differences-common-law-system-civil-law-system-terms-contracts-business/.

[5] PPLRC, "Legal and Regulatory Issues Concerning Public-Private Partnerships," *World Bank Group*, July 13, 2016, https://ppp.worldbank.org/public-private-partnership/legislation-regulation

[6] Robert Muggah, "Brazil Struggles with Effective Cyber-crime Response," *Jane's Military & Security Assessments Intelligence Centre,* 2017, https://www.janes.com/images/assets/518/73518/Brazil_struggles_with_effective_cyber-crime_response.pdf

[7] Alan Campos Elias Thomaz and Fabio Ferreira Kujawski, "The Privacy, Data Protection and Cybersecurity Law Review - Brazil," *The Law Reviews,* October 2018, https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175622/brazil

multiple laws that has been and will continue to be adopted through a bill that was designed to regulate issues from years before its implementation.[8] In addition to privacy concerns, Brazil faces cyber threats toward their supervisory control and data acquisition (SCADA) devices, which control most of the country's critical infrastructure.[9] The Brazilian government has taken steps to define its critical infrastructure as early as 2010, and recognizes the nexus between protecting that infrastructure and cyber risks.[10] Most recently, the Central Bank of Brazil has followed Resolution No. 4.658 as a cybersecurity policy framework to protect infrastructure related to cyber.[11] Brazil also works with the Organization of American States (OAS), which is a body that helps to facilitate projects with participation from both the public and private sectors. Although Brazil has taken small steps to protect and regulate its critical infrastructure through technical review and national guidelines for inspection by the National Telecommunications Agency (ANATEL), many efforts lack resources and capacity. ANATEL has even been criticized by Brazil's Federal Accountability Office for its inability to meet oversight commitments sufficiently.[12] Brazil is also lacking the necessary amount of coordination between all stakeholders deploying SCADA devices, both public and private. Additionally, because Brazil utilizes a system that allows for both the Federal Police of Brazil and the state police in the country to handle ICT offenses, there is often a risk of competing competencies and a lack of communication between the two.[13] This makes the utilization of a task force helpful in coordinating information and identifying critical cyber threats in relation to national security and critical infrastructure issues. Although Brazil is lacking this entity, they utilize the Computer Forensic Unit of the Federal Police to inform their congress during policy making processes, as recommended by the REMJA Working Group on Cybercrime.[14] Adding to the challenges of Brazil's ability to regulate cybersecurity, the country oversight structure allows for a long list of ministries and government entities to have influence over cybersecurity issues.[15] No single agency is tasked with the overall coordination among over seven different ministries and departments that control aspects

---

[8] Daniel Pitanga Bastos De Souza, "Brazil: Cybersecurity 2019," *Global Legal Group Limited*, October 16, 2018, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/brazil

[9] "Brazil's Critical Infrastructure Faces a Growing Risk of Cyberattacks," *Council on Foreign Relations*, April 10, 2018, https://www.cfr.org/blog/brazils-critical-infrastructure-faces-growing-risk-cyberattacks

[10] Amelia Meyer, "Brazil Infrastructure," 2010, *Brazil*, https://www.brazil.org.za/brazil-infrastructure.html

[11] "Resolution CMN 4,658," *Banco Central Do Brazil*, April 26, 2018, https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf

[12] Ordinance No. 50640, December 22, 2015, http://www.anatel.gov.br/legislacao/procedimentos-de-fiscalizacao/887-portaria-50640

[13] "Specialized Cybercrime Unites: Good Practice Study", *CryberCrime@IPA, November 9, 2011,* https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

[14] Inter-American Development Bank and Organization of American States, "Cybersecurity: Are We Ready in Latin America and the Caribbean?" *IADB*, March 2016, https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean

[15] Robert Muggah, "Brazil Struggles with Effective Cyber-Crime Response," *Jane's*, 2017, https://www.janes.com/images/assets/518/73518/Brazil_struggles_with_effective_cyber-crime_response.pdf

of privacy and security in the cyber sector. In terms of legislation to combat cybercrime, Brazil's Congress has been faced with many bills that if passed, would allow for access to personal data without a judicial order, prolonging public opposition due to privacy concerns.

Much like Brazil, Colombia's civil law groundings guarantee the right to privacy in its Constitution, and includes a "habeas data" right, allowing citizens the right to know about and control personal information that has been collected in public or private databases. Colombia's cybersecurity legislation focus has been on data protection. There are two main data protection laws in Colombia, the most recent being Law 1581 of 2012, which deals with reporting requirements and general regulations; however, instances of security breaches often go unreported despite this regulation.[16] This law, among others, is inspired by European data regulations with a focus on consent. The law designates the Superintendence of Industry and Commerce (SIC) as the main data protection authority with the ability to enforce regulations by conducting unannounced audits, raids, and investigations, as well as the ability to penalize for non-compliance to the law.[17] Additionally, laws have been created that further promote adherence to Colombia's cyber regulations, such as Law 1273 of 2009 that hands out penalties of as much as four years in prison.[18] In regards to Colombia's fight against cybercrime, their National Council for Economic and Social Policy (CONPES) directs cybersecurity and cyber defense policy in the country, releasing CONPES 3701 in 2011.[19] This document acted as a guide for the government in forming cybersecurity and cyber defense policy, and its recommendations pushed Colombia to set up a cyber defense system that aimed to protect state institutions and government information.[20] In addition, the new CONPES document established working groups consisting of government entities and private organizations to protect the country's critical infrastructure.[21] Colombia is projected to release a National Defense Strategy for Critical Infrastructure based on the groups' work. Following a scandal involving wiretapping abuses by heads of the military and of the Administrative Security Department (DAS) in early 2014, President Santos sought help from the OAS, resulting in the creation of the National Mission of Technical Assistance on Cyber Security.[22] The objective was to generate further recommendations that would give the government a more solid base when implementing its systems. The mission also included international perspectives from government officials of various countries, as well as representatives from the Council of Europe (COE), Interpol, the UN, and the Organization for Economic

---

[16] Inter-American Development Bank and Organization of American States, "Cybersecurity: Are We Ready in Latin America and the Caribbean?" *IADB*, March 2016, https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean

[17] Natalia Barrera Silva , "Colombia", *The Law Reviews*, October 2018, https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175627/colombia

[18] "Colombia Cuenta Con Una Política Nacional de Seguridad Digital," *Mintic*, April 15, 2016, https://www.mintic.gov.co/portal/604/w3-article-15033.html

[19] Jairo Andrés Cáceres García, "Cyberdefense and Cybersecurity in Colombia," *DialogoI*, September 22, 2016, https://dialogo-americas.com/en/articles/cyberdefense-and-cybersecurity-colombia

[20] Ibid.

[21] Organization of American States, "Report on Cybersecurity and Critical Infrastructure in the Americas," *OAS*, 2015, https://www.sites.oas.org/cyber/Documents/2015%20-%20OAS%20Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf

[22] "Colombia Country Report," *Freedomhouse*, 2018, https://freedomhouse.org/report/freedom-net/2018/colombia

Cooperation and Development (OECD). Its main recommendation of the mission was to harmonize the new system with the international Convention on Cybercrime, otherwise known as the Budapest Convention, to allow for the country to consider best practices on digital crime legislation. In 2016, CONPES 3854 was drafted, replacing CONPES 3701, focusing more on risk management and the promotion of public awareness campaigns. While Colombia sets a good example for being the first LAC country to fully recognize recommendations of the OECD, both CONPES reports failed to produce hard policy upfront. CONPES 3854 evaluated the aftermath of goals made in 3701, one of which being to "strengthen legislation on cybersecurity and cyber defense", but the document admitted to only developing hard regulation aimed at the protection of personal rights and data. Although the document mentions a National Digital Security Policy, the document itself is only projecting the construction of a "plan" that will be executed sometime between 2016 and 2019 to form their policy, with the hope of its implementation, using CONPES 3854 as a guideline, by 2020. So, while CONPES 3854 acknowledges the need to adapt legislation to fast moving threats in cyberspace, Colombia's policies still lag behind new threats. Both CONPES reports defined cyber critical infrastructure but protective regulations have yet to be implemented. The Emergency Security Response Team of Colombia (COLCERT) is mainly responsible for protecting national infrastructure against cyber incidents that threaten national security, but they do not have any PPPs to help bolster this protection. Despite the country's utilization of international cooperation and guidelines from the Budapest Convention, a policy has not yet been implemented for the country regarding cybersecurity and defense, and there is much backlash from civil society groups regarding CONPES 8354's focus on military and economic issues at the expense of broader social and human rights concerns, such as privacy.[23]

Cyberspace Regulations in Countries using Common Law Systems

When analyzing countries with common legal systems, we have chosen Belize and Trinidad and Tobago as examples of countries exerting the most effort to combat cyber issues. To date, electronic transaction legislation is the closest Belize has come to cyber legislation as seen in the Interception of Communications Act of 2010 (provisions relating to interception and when it is allowed), the Electronic Transactions Act of 2003 (facilitates the appropriate use and protection of transactions), and the Telecommunications Act of 2002 (protects telecommunications and outlines offences and penalties of noncompliance).[24] Belize is one of the only countries in the LAC region that does not have any regulations pertaining to data protection or overall cybersecurity or crime. Belize has a Freedom of Information Act (2000), which protects personal information of citizens, but does not mention electronic data.[25] Belize's Medium Term Development Strategy 2010-2013 serves as a framework to the government for the creation of legislation to, among other things, address issues of "data protection and privacy, cybercrime, and network security." The strategy also highlights the appointment of an ICT Task Force that is to

[23] Ibid.

[24] Repository Cybercrime, Database of Legislation, *UNODC*, https://sherloc.unodc.org/

[25] Freedom of Information Act, December 31, 2000, http://unpan1.un.org/intradoc/groups/public/documents/tasf/unpan025201.pdf

create and update the National ICT Policy; however, there only seems to be a National ICT Strategy (2011), and it neither mentions cyber issues nor data protection.[26] The National e-Government Strategy and Work Plan 2015-2018 is another framework created by Belize to guide its Central Information Technology Office (CITO) to produce further e-government frameworks. Although the strategy does not focus much on cybersecurity, one of its pillars is to enhance national security, with one of the many objectives aimed at "build[ing] technical and legislative capacity to respond to, mitigate, and protect against cybercrime and offences within the public sector." The strategy also recommends the creation of a Computer Security Incident Response Team (CSIRT) to produce cybersecurity information, support in the event of a cyber incident, and collaboration. However, no CSIRT has been created, though the national police often collaborate with international CSIRTs when dealing with cyber issues. While Belize does not have any cybersecurity legislation on the topic, they do mention in their strategy the importance of protecting critical infrastructure and the need to secure information networks, though they do not define what critical infrastructure is in their own country. Lastly, the strategy claims that the CITO will work with the agency responsible for cybercrime and cybersecurity in order to produce a cybersecurity national policy, strategy, and action plan and ensures the government of Belize will focus more on creating policies and legislation that supports the strategy overall, one of which being data protection regulations.[27] In 2017, Belize hosted a Cyber Security Symposium with the goal of collaboration and development among both the public and private sectors of a national framework dealing with cybersecurity issues. Although Belize conducts helpful collaborative events such as their symposium and has created various strategies dealing with future cybersecurity regulations, the country has failed to fully implement any of the guidelines dealing with cyber issues and lacks the cooperation of PPPs.

Like many other LAC countries, the focus of Trinidad and Tobago regarding cybersecurity focus has been on data protection. The country's most recent regulation is the Data Protection Act (DPA) of 2011, which provides protections to personal privacy and information that is collected by private and public bodies; however, the DPA functions as if it is not implemented, as the enforcement body of the act, The Office of the Information Commissioner, has not yet been established, and many of the DPA's provisions have not yet been enacted.[28] The Information Commissioner, if established, would have the ability to enter premises and question citizens, as well as to search for and collect their data without a court order or warrant.[29] This, along with the fact that

[26] Belize National ICT Strategy, 2011, http://lincompany.kz/pdf/Africa/Beliz2011.pdf
[27] Belize National E-Government Strategy, 2015, http://cdn.gov.bz/cito.gov.bz/egovstrategy/BelizeNatleGovStrategyWorkPlan2015.pdf
[28] "Data Protection Laws of the World: Trinidad and Tobago," *DLA Piper*, January 28, 2019, https://www.dlapiperdataprotection.com/index.html?t=law&c=TT
[29] Mark Lyn-der-say, "The Challenges of the Data Protection Bill," *Trinidad and Tobago Guardian*, October 24, 2016, http://www.guardian.co.tt/lifestyle/challenges-data-protection-bill-6.2.359349.b246c2daff

certain provisions of the bill have not yet been enacted into law (such as those protecting the rights of journalists), has raised concerns over the correct balance of privacy and constitutional rights to freedom. In 2016 the Public Administration and Communications Ministry agreed to review and potentially amend the act, but to date, no changes have been implemented. The government has also created a PPP between Trinidad and Tobago and public and private operators and owners of critical energy infrastructure, which focuses on preventing, anticipating, and responding to all threats to the country's energy sector.[30] With regards to cybercrime, Trinidad and Tobago produced a National Cyber Security Strategy of 2012, which is meant to provide guidelines for all legislation that follows.[31] Some of the most important things this document does is define critical infrastructure in the nation, pledge to focus on the interdependence of critical information infrastructure protection (CIIP) and critical infrastructure protection (CIP), uses international frameworks and partnerships to guide legislation, and implements education awareness and training.[32] While the framework lays out good ideas, it has not yet delivered on all of its promises. The Cybercrime Bill of 2017 has not yet been enacted into law and faces much social backlash. Like the DPA, the bill criminalizes journalists and whistleblowers who leak illegally obtained data, including government documents. This is an issue for the public because these types of leaks are some of the only ways that many actors can hold their government accountable, and the lack of set law impedes Trinidad and Tobago's ability to move forward. Additionally, there is a lag in cybersecurity awareness and advancements due to a lack of financial and human resources.

Cyberspace Regulations in Countries Using a Mixture of Common and Civil Law Systems

Regarding countries in the LAC region utilizing a mixture of both legal systems, we have chosen to analyze the legislative efforts of Guyana and Puerto Rico. Guyana currently has no legislation or framework regarding data protection. In 2015, the government amended its Financial Institutions Bill to allow the Guyana Revenue Authority (GRA) to access data of all citizens for various investigative purposes, which drew back the previous bill's requirement for the GRA to make a lawful request before gaining access to such information.[33] This received criticism by the Private Sector Commission (PSC) due to the lack of legislation that protects confidential information in the country. Although the PSC recommended a short-term adoption of U.S. frameworks to the Attorney

[30] Inter-American Development Bank and Organization of American States, "Report on Cybersecurity and Critical Infrastructure in the Americas," 2015, https://www.sites.oas.org/cyber/Documents/2015%20-%20OAS%20Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf

[31] Trinidad and Tobago Cyber Security Strategy, February 3, 2015, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/trinidad-and-tobago-cyber-security-strategy

[32] Organization of American States, "Latin American and Caribbean Cyber Security Trends," *Symantec*, June 2014, https://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

[33] Jomo Paul, "No Immediate Need for Data Protection Laws - Finance Minister," *iNewsGuyana*, November 18, 2015, https://www.inewsguyana.com/no-immediate-need-for-data-protection-laws-finance-minister/

General, nothing on this front has been accomplished.[34] Since then, the government has publicly stated that the need for such privacy regulation is not yet needed due to international treaty obligations to the U.S.[35], such as The Foreign Account Tax Compliance Act (FACTA) requiring those living outside of the U.S. to produce yearly reports of their non-U.S. financial accounts, which for Guyana comes from the GRA.[36] In terms of government entities, Guyana has a National Data Management Agency that does not focus on aspects of data protection.[37] In 2018 the country passed a cybercrime bill that was originally criticized by the Opposition People's Progressive Party (PPP) for clauses that restricted the rights of the press and threatened whistleblowers by criminalizing computer users who promote discontent towards the government. In response, the government produced amendments that removed obstacles to a free press and more rigidly defined the type of electronic data that was to be prohibited. Even with these amendments in place, the House continues to disagree on various provisions and refuses to take responsibility for inclusion of certain clauses, as the PPP either were not present to vote at certain times of the bill's amendment process or lacked the voting powers to do so without major support of certain government members.[38] An upside of the bill is a requirement to expose law enforcement officials, including state prosecutors, to cybersecurity training; however, legal professionals have not yet undergone such training. In addition, many attorneys have argued that the bill is not in alignment with the Budapest Convention and lacks provisions allowing for international cooperation; however, Guyana has neither signed nor ratified the convention and is therefore not legally bound to it.[39] Additionally, Guyana is behind in assessing its Critical National Infrastructure (CNI) assets and vulnerabilities, and owners of CNI rarely adhere to security standards or report incidences due to a lack of legislation regarding and identifying CNI.[40] In 2015 Guyana collaborated with experts from the OAS' Inter-American Committee Against Terrorism (OAS/CICTE) in a two-day workshop to identify other countries' best practices in developing a National Cybersecurity Policy Framework, such

---

[34] GuyanaTimes, "Govt to Address Concerns on Data Protection Laws," *Mola*, November 12, 2015, https://mola.gov.gy/15-news-/319-govt-to-address-concerns-on-data-protection-laws

[35] Jomo Paul, "No Immediate Need for Data Protection Laws - Finance Minister," *iNewsGuyana*, November 18, 2015, https://www.inewsguyana.com/no-immediate-need-for-data-protection-laws-finance-minister/

[36] Ibid.

[37] For more on The National Data Management Agency: https://mopt.gov.gy/agencies/national-data-management-agency/

[38] Staff Reporter, "Cybercrime Bill Passed," *Guyana Chronicle*, July 21, 2018, http://guyanachronicle.com/2018/07/21/cybercrime-bill-passed

[39] Cybercrime Programme Office of the Council of Europe (C-PROC), "Cybercrime Digest," *COE*, May 1, 2018, https://www.coe.int/documents/9252320/19115368/CPROC+Digest+2018-05-01.pdf/bcef7798-011b-92b4-def8-4ed13dd03b4c

[40] Inter-American Development Bank and Organization of American States, "Cybersecurity: Are We Ready in Latin America and the Caribbean?" *IADB*, March 2016, https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean

as that in Trinidad and Tobago.[41] Another goal of the workshop was to establish a National Task Force to address the country's cyber needs, which has not yet been accomplished. Although the country has established a National CIRT to provide analysis and incident response to cybersecurity issues, its capabilities are limited due to the absence of a national cybersecurity strategy or policy and a lack of awareness of cyber-related issues in the government. The CIRT is also not governed by legislation, but rather by cabinet approval, and there is currently no legal requirement for private sector entities to report cyber incidents to the government. The main challenges to the future of Guyana's cybersecurity advancement and regulation is a lack of personnel with required skill sets, the absence of national regulations or frameworks, inadequate training, and the fact that cybersecurity threats are not currently viewed by the government as a top priority.[42]

Before explaining regulatory efforts in Puerto Rico, it is first important to understand Puerto Rico's legal system. Although Puerto Rico is a United States unincorporated territory, the LAC region, as well as a majority of Puerto Ricans, view the territory as a part of Latin America. Before its affiliation with the U.S., Puerto Rico utilized the Spanish civil code. Because the U.S. uses a common law system based on the doctrine of judicial precedent, Puerto Rico adopted a mixed legal system that incorporated both common and civil law aspects.[43] Although Puerto Rico has the ability to create and amend its own constitution, U.S. Code Title 48, "Territories and Insular Possessions" requires Puerto Rico to adopt all U.S. statutory laws that are not "locally inapplicable".[44] Puerto Rico has its own Supreme Court and applies new laws based on case law precedent;[45] however, the U.S. Supreme Court, although independent of that in Puerto Rico, can review Puerto Rico's Supreme Court decisions on a *writ of certiorari*.[46]

Although Puerto Rico adopts cybersecurity legislation from the U.S., the territory has implemented its own regulations, namely dealing with data protection. Puerto Rico currently has no overarching authority or single law that outlines broad protective regulations of citizens' data.[47] There are, however, a few individual laws that regulate aspects of a citizens' personally identifiable information.[48] One of the first pieces of

---

[41] Staff Writer, "Gov't to Hold Cyber Security Workshop," *Stabroek News*, August 5, 2015, https://www.stabroeknews.com/2015/news/guyana/08/05/govt-to-hold-cyber-security-workshop/

[42] Organization of American States, "Latin American and Caribbean Cyber Security Trends," *Symantec*, June 2014, https://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

[43] Zorilla and Silverstrini Attorneys at Law, "Puerto Rico Legal System," *Zspalaw*, 2019, https://www.zspalaw.com/puerto-rico-legal-system.html

[44] 48 USC 734, *Cornell Law*, January 4, 2012, https://www.law.cornell.edu/uscode/pdf/uscode48/lii_usc_TI_48_CH_4_SC_I_SE_734.pdf

[45] 28 U.S. Code § 1258, *Cornell Law*, https://www.law.cornell.edu/uscode/text/28/1258

[46] In other words, the U.S. can review decisions when it deems necessary.

[47] Edwin J. Seda-Fernandez and Mariel Y. Haack, "Data Privacy Law," March 8, 2019, https://practiceguides.chambers.com/practice-guides/employment-2019/puerto-rico/3-data-privacy-law

[48] Ibid.

legislation regarding the protection of personal data is Act No. 111 of 2005 (Citizen Information of Data Banks Security Act), which provides requirements for commercial entities to protect personal information of consumers who are currently in the custody of said entities. Because this act does not address the handling of such information after the termination of that custody, Act No. 234 was implemented in 2014 to require commercial entities to discard all data in a way that protects consumer privacy, such as by "shredding, deleting, or modifying" it to render the personal information unreadable or indecipherable by any method.[49] As of recent, Puerto Rico has produced House Bill 607 amending Act No. 234 to require the holders of personally identifiable information to notify consumers of violations, compromises, or unauthorized access to their personal information within 24 hours of becoming aware of a breach.[50] This amendment is meant to further protect citizens' personal data and expand protections against things like identity theft. Recognizing the lack of legislation establishing parameters to protect growing accumulations of personal data by companies, Puerto Rico has also proposed Senate Bill 1231 which would create the Digital Privacy Protection Act in order to guarantee rights to privacy by including protective regulations for information held in automated databases and private sector business manuals. The main goal of the bill is to allow for citizens to demand a company to refrain from selling their personal information to third parties, which is currently not restricted in Puerto Rico. Additionally, citizens would be able to request a company to terminate their personal information from its databases or records and advise third parties who the data had been shared with to do the same.[51] So far, Puerto Rico's attempts to adapt outdated laws shows their commitment to addressing new threats that emerge from enhanced access to personal information. The main issue Puerto Rico faces is a lack of an overarching data protection or cybersecurity authority to deal with both privacy and security issues. In addition, there is a lack of a data protection law that encompasses all aspects of citizens' security issues, as well as an absence of any cybersecurity regulation, specifically regarding Puerto Rican critical infrastructure, which is not often discussed by the government.

Conclusion

Countries in the Latin American and Caribbean region face many cybersecurity challenges given the fast pace of cyber threats. Most obstacles for these countries come from a lack of coordination between the public and private sectors, minimal resources and capacity, the absence of a legal framework, and the inability for many countries to implement regulations quickly enough to keep up with new threats, which is especially true for countries utilizing civil law systems. Countries that focus on data protection and

[49]Medida P C1484, *OSLPR*, May 7, 2019, oslpr.org/legislatura/tl2013/tl_busca_avanzada.asp?rcs=P%20C1484
[50] Puerto Rico House Bill 607, *Open States*, January 14, 2017, https://openstates.org/pr/bills/2017-2020/PC607/
[51] Maria Miranda, "Bill Introduced to Protect, Regulate, Personal Data in Puerto Rico," *Caribbean Business,* March 25, 2019, https://caribbeanbusiness.com/bill-introduced-to-protect-regulate-personal-data-in-puerto-rico/

privacy often neglect defining and protecting their critical infrastructure, and countries forming cybercrime legislation focus on accessing citizen's information and have received public backlash due to privacy concerns. Many civil law countries may also struggle with establishing helpful PPPs due to a lack of freedom of contract. Although many LAC countries utilizing common law have not yet created case law on these issues, the fluid nature of such a system in regions such as the U.S. has proven to allow for a more flexible legal environment, especially when regarding issue of privacy. For instance, in 2018 *Carpenter v. United States* created precedent declaring a lawful warrant requirement in order to obtain cell phone data of U.S. citizens.[52] While case law in the U.S. is helpful, the EU serves as a frontrunner in cyber efforts, and often influences the actions of both the U.S. and LAC regions. The EU likely has an easier time dealing with cybersecurity issues because they utilize a mixed legal system, incorporating aspects of both civil and common law. Their judicial system allows for them to rule over certain aspects of the law, they have a non-political interest in market competition, and they have grown their capacities due to their freedom of contract through PPPs and international cooperation to implement their overall commitment to cybersecurity. The EU also focuses on some of the most important aspects of cybersecurity: data privacy, critical infrastructure, and cybercrime.

In 2018, the EU passed a General Data Protection Regulation (GDPR) with the goal of updating laws that protect citizens' personal information. Not only does the GDPR give control to citizens over their data, but it also regulates how public and private actors handle personal information.[53] In addition, unlike the U.S., the EU takes market competition and data protection very seriously. The region is currently looking to combine the two in a set of constraints that would promote the market value of smaller companies while regulating companies with large market power that have unlimited access to user data. In the U.S., online market power is measured by how much data a user is willing to give up to a company, and those accessing the most data, such as Facebook and Twitter, often swallow competitors' values. Courts often only view online business monopolies as an issue if they are clearly harming consumers. In this sense, the EU has an easier time regulating these companies, as antitrust debates in the U.S. are usually prosecuted in front of a judge, while in the EU, the European Commission itself has the power to decide cases without approval of national governments. In the U.S., only federal agencies can impose these types of federal laws.[54] In addition, privacy is a fundamental right in the EU Charter the way that freedom of speech is in the U.S. Constitution. Because of the EU's hard stance on privacy, U.S. regulations are often discussed by EU courts to determine whether American laws are protective enough as to allow for European data to flow through the U.S. If regulations are not up to par with those in the EU, the functioning of

[52] Nathan Freed Wessler, "The Supreme Court's Groundbreaking Privacy Victory for the Digital Age," *ACLU*, June 22, 2018, https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age

[53] "GDPR Key Changes," *EU GDPR*, 2018, https://eugdpr.org/the-regulation/

[54] "The Power of Privacy," *The Economist*, March 23th-29th 2019, p. 19-20

other country's internet companies, such as those in the U.S., could be compromised.[55] In addition to privacy concerns, the European Parliament approved a Cybersecurity Act this year, which focuses on the expertise of the European Union Agency for Cybersecurity (ENISA) in developing legislation, considering best practices, enhancing capacity-building in Member States, providing education and training, and enhancing cooperation with PPPs to combat cybersecurity issues and protect critical infrastructure.[56] While cybercrime is incorporated into the act, there are also other bodies that work to combat attacks against critical infrastructure, such as Europol's European Cybercrime Center, along with efforts of ENISA.[57]

In line with EU standards, many LAC countries have followed suite and adopted regulations in congruence with the GDPR. Brazil, for instance, based its data privacy law off of that in the EU, and many Ibero-American Member States, which are mostly from LAC countries, have agreed to the Standards for Data Protection, which uses the GDPR as a policy guideline.[58] In addition, many LAC countries have agreed to adhere to the Budapest Convention, which is an international agreement laying out cybersecurity framework requirements for each member. Agreements on the international level, however, continue to be lacking. Many countries that have signed and ratified the Budapest Convention have not yet implemented its recommendations, and the convention will not have enough effect without ratification by larger members of the community, such as Russia and China. In addition, because cyberspace has no boundaries, a binding international law is too difficult to pass. While the United Nations (UN) has attempted to work toward alleviating international cybersecurity threats, not much has been done on the front of international adherence. Acts of cybercrime are nearly impossible to identify, and no court in the international community hears cases regarding international cybercrimes, as there is no set international law prohibiting them that is binding on all UN Member States, and there is no agreed upon definition of what constitutes a "cybercrime".[59] Conducting investigations to prove an attack is also difficult without infringing on another nation's sovereignty.[60] The United Nations Security Council will not likely produce a resolution dealing with cybercrime due to its current makeup, which includes Russia and China, two countries that would not benefit from such a

---

[55] "The Cambridge Analytica Bill", *The Economist*, March 2th-8th, 2019, p. 22

[56] "EU Parliament Approves the Proposal for Cybersecurity Act," *Hunton Security Blog,* March 28, 2019, https://www.huntonprivacyblog.com/2019/03/28/eu-parliament-approves-the-proposal-for-cybersecurity-act/

[57] Directive 2013/40/EU, *Eur-Lex* August 12, 2013, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

[58]Jones Day, "Privacy and Cybersecurity Developments in Latin America," *JDSUPRA*, June 25, 2018, https://www.jdsupra.com/legalnews/privacy-and-cybersecurity-developments-13277/

[59] Weiping Chang, Wingyan Chung, Hsinchun Chen, and Shihchieh Chou, "An International Perspective on Fighting Cybercrime," *Intelligence and Security Informatics*, no. 2665, (2003): 379-384.

[60] United Nations Office on Drugs and Crime (UNODC), "Comprehensive Study on Cybercrime," *UNODC*, February 2013: pp. 185, https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf

resolution. Due to these issues, as well as those aforementioned, the LAC region is likely to continue to follow the EU in setting up their own regulations, and the utilization of international cooperation and the establishment of PPPs are the most feasible mechanisms to boost their chances of implementing strong legislation to combat cybersecurity issues.