



La seguridad en el marco del Estado de derecho

Sonia Alda Mejías

Carolina Sampó

Gerardo Rodríguez Sánchez Lara

(coordinadores)

Universidad de las Américas Puebla

UDLAP[®]



Instituto de
Relaciones
Internacionales



UNIVERSIDAD
NACIONAL
DE LA PLATA

Con la colaboración de:



Centro de Estudios
Estratégicos del
Ejército del Perú



FRIEDRICH NAUMANN
STIFTUNG Für die Freiheit.
Países Andinos

LA SEGURIDAD EN EL MARCO DEL ESTADO DE DERECHO

Sonia Alda Mejías

Carolina Sampó

Gerardo Rodríguez Sánchez Lara
(coordinadores)

Coeditores

Universidad de las Américas Puebla

Real Instituto Elcano

Centro de Estudios sobre Crimen Organizado Transnacional
(CeCOT)-Instituto de Relaciones Internacionales-Universidad
Nacional de La Plata

Con la colaboración de

Centro de Estudios Estratégicos del Ejército del Perú

Friedrich Naumann Stiftung (Oficina Andina)

Índice

Presentación

Embajador Eminentísimo Raphael Steger Cataño 11

Decano de la Escuela de Ciencias Sociales,
Universidad de las Américas Puebla, México

Dr. Charles Powell 13

Director del Real Instituto Elcano, España

Dr. Norberto Consani 15

Director del Instituto de Relaciones
Internacionales, Universidad Nacional de La
Plata, Argentina

**Introducción: los cambios de la
agenda de seguridad en el marco
del Estado de derecho** 17

Sonia Alda Mejías, Carolina Sampó y Gerardo
Rodríguez Sánchez Lara

**Parte I. Seguridad global y Estado
de derecho: retos a la seguridad
por área geográfica** 28

**La cultura de la legalidad como
motor dinamizador de la seguridad,
el desarrollo y la gobernabilidad** 29

Sonia Alda Mejías

Los cambios de la agenda de seguridad en el marco del Estado de derecho	60
Manuel Villoria	
El abordaje de la criminalidad organizada y su violencia conexas en América Latina, desde una perspectiva de seguridad nacional moderna y democrática	92
Mariano Bartolomé	
Retos a la seguridad y el Estado de derecho en la Unión Europea	106
David Vincent Henneberger y Sebastian Vagt	
Seguridad y Estado de derecho en África a través del caso del G5 Sahel	120
Mohamed Badine El Yattoui y Claudia Barona Castañeda	
Emergencia de Asia-Pacífico en Latinoamérica: retos para su seguridad	142
José Pardo de Santayana y Andrés González Martín	
Parte II. Problemas transnacionales que amenazan la seguridad	196
Estado de derecho en el ciberespacio: la actualidad en Latinoamérica y el Caribe	197
Boris Saavedra	

El vínculo entre seguridad y medio ambiente: una aproximación teórica y práctica en América Latina	226
Simone Lucatello	
La migración como un asunto de seguridad a veinte años de la Cumbre de Tampere	244
Ludmila Quirós	
Parte III. Exigencias del Estado de derecho a las instituciones de seguridad	262
¿Tiene sentido medir la impunidad? Comparando el diseño de índices y estudios sobre impunidad aplicados al caso mexicano	263
Juan Antonio Le Clercq Ortega	
El rol de la inteligencia y los mecanismos de control democráticos	300
Julia Pulido Gragera	
Flujos financieros ilícitos y buen gobierno	311
Aitor Pérez	

Parte IV: La transformación de las fuerzas armadas en el marco del Estado de derecho 330

Transparencia y cultura organizacional en las fuerzas armadas 331

Paul Eduardo Vera Delzo

En busca de la transparencia: los presupuestos de defensa del Ecuador 2006-2019 345

Bertha J. García Gallegos

La transformación de la inteligencia militar en el marco democrático: tareas y transparencia 370

Andrés Gómez de la Torre Rotta

Semblanzas

Coordinadores 401

Sonia Alda Mejías

Gerardo Rodríguez Sánchez Lara

Carolina Sampó

Autores 405

Mohamed Badine El Yattioui

Claudia Barona Castañeda

Mariano Bartolomé

Bertha Judith García Gallegos

Andrés Gómez de la Torre Rotta

Andrés González Martín
David Vincent Henneberger
Juan Antonio Le Clercq Ortega
Simone Lucatello
José Pardo de Santayana
Aitor Pérez
Julia Pulido Gragera
Ludmila Quirós
Boris Saavedra
Sebastian Vagt
Paul Eduardo Vera Delzo
Manuel Villoria Mendieta

ESTADO DE DERECHO EN EL CIBERESPACIO: LA ACTUALIDAD EN LATINOAMÉRICA Y EL CARIBE

Boris Saavedra

Estado de derecho

Con la finalidad de proporcionar claridad del marco teórico de los conceptos empleados en este ensayo conceptualizaremos el Estado de derecho con base en *The Origins of Political Order* (Fukuyama, 2011), es decir, como cuerpo abstracto de reglas de justicia fundamentadas en valores y no en la legislación como ejercicio de la función del poder político. Sin embargo, el empleo de la combinación del sistema civil y el derecho consuetudinario en el ciberespacio en la Unión Europea ha permitido un mejor desempeño del marco legal para el control y la aplicación del Estado de derecho.

Estado actual de las regulaciones del ciberespacio en América Latina y el Caribe

El desarrollo histórico de los sistemas legales en los países, enfocado en los tres sistemas existentes y utilizados en la región: sistema civil, común y la combinación de ambos, así como el contraste de los esfuerzos y los desafíos para los tres sistemas, se

consideran elementos contribuyentes a la actual falta de capacidades reguladoras.

La regulación de las funciones de ataque, defensa, resiliencia, privacidad y libertad de expresión, entre otras de los sectores público y privado, es esencial para ejercer la ciberseguridad nacional y global. El sector público, enfocado en el principio de proteger el bien común, y el sector privado, enfocado en la generación de ganancias comerciales, deben converger y unirse bajo un marco regulatorio común para cumplir sus objetivos de seguridad. Por ejemplo, podemos citar los esfuerzos exitosos de la Unión Europea (UE), específicamente en el área de la privacidad, que es una de las muchas áreas críticas de la ciberseguridad y que requiere una regulación efectiva del ciberespacio. El modelo regulatorio de la UE a menudo es seguido por países en diferentes partes del mundo, incluidos los de Latinoamérica y el Caribe. A manera de idea general del estado de la cuestión de las regulaciones de seguridad cibernética en la región, la tabla A describe cada país y el marco de legislación de seguridad cibernética o regulaciones relacionadas con: protección de datos, cibercrimen, gobierno electrónico, tecnología de la información (TI), comunicaciones, infraestructura crítica y varias áreas adicionales, así como el sistema legal empleado y la fecha de implantación.

Tabla 1. Regulaciones de seguridad cibernética en América Latina.

País	Sistema legal	Título de la legislación en ciberseguridad	Año
Argentina	Derecho civil	Ley de Protección de Datos Personales	2000
		Ley de Delitos Informáticos	2008
Bolivia	Derecho civil	Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación	2011
		Plan de Implementación de Gobierno Electrónico	2017
Brasil	Derecho civil	Estrategia Nacional de Seguridad de las Comunicaciones de Información y Seguridad Cibernética	2015
		Ley General de Protección de Datos	2020
Chile	Derecho civil	Ley General de Telecomunicaciones	1982
		Ley de Protección de la Vida Privada	1999
		Política Nacional de Ciberseguridad	2017
Colombia	Derecho civil	Ley de la Protección de la Información y de los Datos	2009
		Lineamientos de Política para la Ciberseguridad y Ciberdefensa	2011
		Acta de Protección de Datos Personales	2011
		Ley de Protección de Datos	2012
		Política Nacional de Seguridad Digital	2016

País	Sistema legal	Título de la legislación en ciberseguridad	Año
Costa Rica	Derecho civil	Estrategia Nacional de Ciberseguridad	2017
Cuba	Derecho civil	Reglamento de Seguridad para las Tecnologías de Información	2007
República Dominicana	Derecho civil	Ley sobre Crímenes y Delitos de Alta Tecnología.	2007
		Ley de Protección de Datos Personales	2013
		Estrategia Nacional de Ciberseguridad	2018
Ecuador	Derecho civil	Ley de Comercio Electrónico, Firmas y Mensajes de Datos	2002
		Plan Nacional de Gobierno Electrónico	2017
El Salvador	Derecho civil	Ley Especial Contra los Delitos Informáticos y Conexos	2016
Guatemala	Derecho civil	Estrategia Nacional de Seguridad Cibernética	2018
Guyana	Derecho mixto	Proyecto de Ley sobre Delitos Electrónicos	2018
Honduras	Derecho civil	Ley de Transacciones Electrónicas	2006
		Ley de Ciberseguridad	2010
		Agenda Digital de Honduras	2013
México	Derecho civil	Ley Federal de Protección de Datos Personales	2010
		Estrategia Nacional de Ciberseguridad	2017

País	Sistema legal	Título de la legislación en ciberseguridad	Año
Nicaragua	Derecho civil	Ley de Protección de Datos Personales	2012
Panamá	Derecho civil	Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas	2013
Paraguay	Derecho civil	Ley que modifica el Código Penal Ley de Protección de Datos Plan Nacional de Ciberseguridad	2011 2015 2017
Perú	Derecho civil	Ley de Protección de Datos Personales Política Nacional de Gobierno Electrónico Ley de Delitos Informáticos	2011 2013 2014
Puerto Rico	Derecho mixto	Ley de Información al Ciudadano sobre la Seguridad de Bancos de Información Ley para Descartar Información Personal de Consumidores.	2005 2014

País	Sistema legal	Título de la legislación en ciberseguridad	Año
Trinidad y Tobago	<i>Common law</i>	Ley de Protección de Datos Estrategia Nacional de Ciberseguridad	2011 2012
Uruguay	Derecho civil	Ley de Protección de Datos Decreto de Seguridad de la Información para Organismos de la Administración Pública Estandarización de los Nombres de Dominio de la Administración Central Agenda Digital 2020	2008 2009 2014 2017
Venezuela	Derecho civil	Ley Especial contra los Delitos Informáticos Ley sobre Mensaje de Datos y Firmas Electrónicas Ley de Infogobierno	2001 2011 2014

Sistemas legales y asociaciones público-privadas

La mayoría de los países del mundo utilizan el sistema de derecho civil, sistema de derecho consuetudinario o una combinación de ambos. Gran parte de Centro y Sudamérica utiliza el derecho civil, que tiene sus raíces en el sistema legal romano. La mayoría de ellos cuenta con una constitución basada en códigos legales específicos (es decir, códigos civiles, derecho constitucional, etcétera). Los sistemas de derecho civil sólo reconocen que las leyes aprobadas a través del sistema legislativo son leyes vinculantes. Los sistemas de derecho consuetudinario, por otro

lado, están influenciados por la jurisprudencia. Si bien muchos de estos países utilizan un proceso constitucional y legislativo, también consideran que las decisiones judiciales son leyes vinculantes. Aunque muchos de ellos con base legal en la doctrina de la *stare decisis* (Oyen, 2017) (principio legal para determinar puntos en litigios según el precedente), los tribunales tienen la capacidad de crear nuevas interpretaciones de la ley cuando se dan diferentes hechos en un nuevo caso (PPPLRC, 2006). Esto permite que los sistemas de derecho consuetudinario sean más maleables, ya que no siempre tienen que pasar por el largo y riguroso proceso legislativo para implementar nuevas regulaciones.

Independientemente del sistema legal, las asociaciones público-privadas (APP) son un elemento esencial de la seguridad cibernética, ya que estos sectores son los dos actores más importantes en la lucha contra las amenazas cibernéticas (la capacidad de recuperación depende de la cooperación entre ambos). Antes de analizar algunos ejemplos de regulaciones de país individualmente, primero es importante comprender los desafíos de crear APP a través de contratos dado el sistema legal del país. Los países de derecho civil no tienen mucha libertad de contrato, ya que las partes a menudo no pueden decidir qué disposiciones quieren contratar, y muchas disposiciones no se incluyen expresamente, sino que están implícitas en otras leyes subyacentes que hacen innecesario repetirlos contractualmente. Esto puede ser problemático debido a la ambigüedad de las reglas del contrato.

Los contratos en los sistemas de derecho civil son más cortos debido a la omisión de un lenguaje específico, lo que deja que las disputas entre las partes se resuelvan por lo establecido en la ley y no en el contrato. Con respecto a las regulaciones de seguridad cibernética, las APP en un sistema de derecho civil dejan mucho margen de error debido al lenguaje utilizado. Por ejemplo, el lenguaje legal con respecto a la protección de «infraestructura crítica» carece de claridad, ya que la definición de «infraestructura crítica» puede cambiar a través de diferentes legislaciones con el tiempo (Weaver, 2016). Además, debido a

que los sistemas de derecho civil están establecidos en la ley codificada, muchos acuerdos de APP no serán ejecutables si no están en congruencia exacta con las leyes del país. Esto retrasaría las APP, ya que los contratos a menudo deben reorganizarse para adaptarse a las leyes del país.

Los sistemas legales de derecho consuetudinario, por otro lado, tienen mucha más libertad de contrato. A diferencia de los sistemas de derecho civil, muy pocas disposiciones están implícitas. Si bien esto requiere un contrato más largo, deja menos espacio para disputas a largo plazo. Además, el derecho consuetudinario permite que los contratos de APP sean mucho más flexibles porque la mayoría de las disposiciones están permitidas si no están expresamente prohibidas por las leyes o regulaciones del país. Esto permite que las APP se establezcan más fácilmente, y cualquier cuestión de legalidad es decidida por los tribunales y no por las leyes ya establecidas (Muggah, 2016).

Regulaciones del ciberespacio en países que utilizan sistemas de derecho civil

Para el análisis de los países de LAC que utilizan el sistema legal civil, hemos seleccionado a Brasil y Colombia como los países que más han avanzado en el establecimiento de legislación para las actividades del ciberespacio. Brasil es uno de los más avanzados económicamente que utiliza el derecho civil. Dada su adopción masiva de la tecnología de las comunicaciones e información (TCI), Brasil es un objetivo principal para los ataques cibernéticos (Muggah, 2017b).

La Constitución Federal brasileña garantiza primero la protección de la privacidad como un derecho fundamental de todas las personas. La legislación más reciente de Brasil que trata temas de ciberseguridad es la Ley General de Protección de Datos de Brasil (LGPD), que se centra en regular el uso y la protección de datos personales por parte de los sectores público y (Kujawski, 2018). La LGPD siguió la implementación de la UE del Reglamento General de Protección de Datos (GDPR) ya que contiene

muchas disposiciones similares. La implementación dentro del sistema brasileño fue un desafío, ya que el Congreso tardó seis años en aprobarlo y se implementará en 2020. En este caso, las regulaciones corren el riesgo de quedar desactualizadas debido al lento proceso burocrático para la aprobación de la ley y el ritmo dinámico de la evolución tecnológica y con ella los riesgos cibernéticos.

Este es un ejemplo de las múltiples leyes que han sido y seguirán siendo adoptadas a través de un proyecto de ley diseñado para regular problemas de vieja data antes de su implementación (Souza, 2019). Además de las preocupaciones de privacidad, Brasil enfrenta amenazas cibernéticas a sus dispositivos de control de supervisión y adquisición de datos (SCADA), que controlan la mayor parte de la infraestructura crítica del país (Muggah, 2018). El Gobierno brasileño ha tomado medidas para definir su infraestructura crítica ya en 2010, y reconoce el nexo entre la protección de esa infraestructura y los riesgos cibernéticos (Meyer, 2010).

Más recientemente, el Banco Central de Brasil ha seguido la resolución número 4.658 como un marco de política de seguridad cibernética para proteger la infraestructura relacionada con la ciberseguridad (Goldfajn, 2018). Brasil también trabaja con la Organización de Estados Americanos (OEA), organismo que ayuda a facilitar proyectos con participación de los sectores público y privado. Aunque Brasil ha dado pasos para proteger y regular su infraestructura crítica a través de una revisión técnica y pautas nacionales para la inspección por parte de la Agencia Nacional de Telecomunicaciones (ANATEL), muchos esfuerzos carecen de recursos y capacidad (50540, 2017). ANATEL incluso ha sido cuestionada por la Oficina Federal de Responsabilidad de Brasil por su incapacidad para cumplir suficientemente los compromisos de supervisión. Brasil también carece de la coordinación necesaria y suficiente entre todas las partes interesadas que implementan dispositivos SCADA, tanto públicos como privados. Además, debido a que Brasil utiliza un sistema que permite que la policía federal y estatal del país manejen los delitos relacionados con las TCI, a menudo existe el riesgo de deli-

mitación clara de competencias y falta de comunicación entre ambas (CyberCrime@IPA, 2011).

Esto hace que el empleo de una fuerza de trabajo sea útil para coordinar información e identificar amenazas cibernéticas críticas en relación con la seguridad nacional y los problemas de infraestructura crítica. Brasil carece de esta entidad, utilizan la Unidad Forense Informática de la policía federal para informar al congreso durante los procesos de formulación de políticas, según lo recomendado por el grupo de trabajo de REMJA sobre cibercrimen (Bank, IDB, 2016). Además de los desafíos antes mencionados para regular la ciberseguridad, la estructura de supervisión del país cuenta con una larga lista de ministerios y entidades gubernamentales que tienen influencia sobre los problemas de ciberseguridad (Muggah, 2017a). Ninguna agencia está encargada de la coordinación general entre más de siete ministerios y departamentos diferentes que controlan aspectos de privacidad y seguridad en el sector cibernético. En términos de legislación para combatir el delito cibernético, el Congreso de Brasil ha presentado muchos proyectos de ley que, de aprobarse, permitirían el acceso a datos personales sin una orden judicial, lo cual es materia muy sensible y cuenta con el rechazo público debido a las preocupaciones por la privacidad.

Al igual que Brasil, el derecho civil de Colombia garantiza la privacidad en su Constitución e incluye un derecho de *habeas data*, que permite a los ciudadanos conocer y controlar la información personal que se ha recopilado en bases de datos públicas o privadas. El enfoque de la legislación de seguridad cibernética de Colombia se ha centrado en la protección de datos. Existen dos leyes principales al respecto, la más reciente es la Ley 1581 de 2012, que se ocupa de los requisitos de presentación de informes y las regulaciones generales, sin embargo, los casos de violaciones de seguridad a menudo no se informan a pesar de esta regulación (Bank y IDB, 2016). Esta ley, entre otras, está inspirada en las regulaciones de datos europeas con un enfoque en el consentimiento. La ley designa a la Superintendencia de Industria y Comercio (SIC) como la principal autoridad de protección de datos con la capacidad de hacer cumplir las regulaciones

mediante auditorías, redadas e investigaciones sin previo aviso, así como la capacidad de penalizar por incumplimiento de la ley (Silva, 2018). Además, se han creado leyes que promueven aún más el cumplimiento de las regulaciones cibernéticas de Colombia, como la Ley 1273 de 2009 que otorga penas de hasta cuatro años de prisión (Colombia, 2016).

Con respecto a la lucha de Colombia contra el cibercrimen, su Consejo Nacional de Política Económica y Social (CONPES) dirige la política de ciberseguridad y defensa cibernética en el país, lanzando CONPES 3701 en 2011 (García, 2016). Este documento sirvió de guía para el Gobierno en la formación de ciberseguridad y ciberdefensa política, y sus recomendaciones impulsaron al establecimiento de un sistema de defensa cibernética que tiene como objetivo proteger las instituciones estatales y la información del Gobierno (García, 2016). Además, el nuevo documento CONPES estableció grupos de trabajo compuestos por entidades gubernamentales y organizaciones privadas para proteger la infraestructura crítica del país (Organization of American States, 2015).

Se proyecta que Colombia lanzará una estrategia de defensa nacional para infraestructura crítica basada en el trabajo de los grupos. Sin embargo, después del escándalo que involucró abusos de escuchas telefónicas por parte de los jefes de las fuerzas armadas y del Departamento de Seguridad Administrativa (DAS) a principios de 2014, el presidente Santos buscó ayuda de la OEA, lo que resultó en la creación de la Misión Nacional de Asistencia Técnica en Seguridad Cibernética (Colombia Freedom on the net, 2018). El objetivo es generar recomendaciones que le darían al Gobierno una base más sólida para implementar este nuevo sistema. La misión también incluyó perspectivas internacionales de funcionarios gubernamentales de varios países, así como representantes del Consejo de Europa (COE), Interpol, la ONU y la Organización para la Economía, Cooperación y Desarrollo (OCDE).

La principal recomendación de la misión fue armonizar el nuevo sistema con la convención internacional sobre cibercrimen, también conocida como la Convención de Budapest, para

permitir que el país considere las mejores prácticas en materia de legislación sobre delitos digitales. En 2016, se redactó CONPES 3854, en sustitución de CONPES 3701, centrándose más en la gestión de riesgos y la promoción de campañas de sensibilización pública. Colombia es un buen ejemplo por ser el primer país de LAC en reconocer plenamente las recomendaciones de la OCDE, ambos informes de CONPES no lograron generar políticas duras por adelantado.

CONPES 3854 evaluó las secuelas de los objetivos establecidos en 3701, uno de los cuales fue «fortalecer la legislación sobre seguridad y defensa cibernética», sin embargo, el documento sólo desarrolla una regulación estricta dirigida a la protección de los derechos y datos personales. Si bien menciona una política nacional de seguridad digital, en sí, sólo proyecta la construcción de un «plan» a ejecutar entre 2016 y 2019 para diseñar la política, con la esperanza de su implementación, utilizando CONPES 3854 como guía, en 2020.

Entonces, si bien CONPES 3854 reconoce la necesidad de adaptar la legislación a las amenazas de rápido movimiento en el ciberespacio, las políticas de Colombia aún están a la zaga de las nuevas amenazas. Ambos informes de CONPES definieron la infraestructura crítica cibernética, pero las regulaciones de protección aún no se han implementado. El Equipo de Respuesta de Seguridad de Emergencia de Colombia (COLCERT) es el principal responsable de proteger la infraestructura crítica nacional contra incidentes cibernéticos que amenazan la seguridad nacional, pero carece de APP para ayudar a reforzar esta protección. A pesar de la cooperación internacional y las pautas de la Convención de Budapest, aún no se ha implementado una política para el país con respecto a la ciberseguridad y la defensa, y los grupos de la sociedad civil tienen muchas reacciones negativas con respecto al enfoque de CONPES 8354 por experiencias nega-

tivas en asuntos militares, económicos y de derechos humanos, como la privacidad (Colombia, Freedom on the Net, 2018).

Regulaciones del ciberespacio en países que utilizan sistemas de derecho consuetudinario

Para analizar países con sistemas legales comunes, hemos seleccionado Belice y Trinidad y Tobago. Hasta la fecha, la legislación sobre transacciones electrónicas es lo más cerca que Belice ha estado de la legislación cibernética, la Ley de Intercepción de Comunicaciones de 2010 (disposiciones relacionadas con la interceptación y la autorización), la Ley de Transacciones Electrónicas de 2003 (facilita el uso y la protección adecuados de transacciones), y la Ley de Telecomunicaciones de 2002 (protege las telecomunicaciones y describe los delitos y las sanciones por incumplimiento) (UNODC, United Nations Office on Drug and Crime, s. f.). Belice es uno de los países de la región que no tiene reglamentaciones relacionadas con la protección de datos, ciberseguridad y el delito en el ciberespacio, hay una ley de libertad de información (2000) que protege la información personal de los ciudadanos, pero no menciona los datos electrónicos (Belice, 2000). La estrategia de desarrollo a mediano plazo de Belice 2010-2013 sirvió como marco para la creación de una legislación que, entre otras cosas, abordaría cuestiones de «protección de datos y privacidad, cibercrimen y seguridad de la red».

La estrategia también destaca el nombramiento de un grupo de trabajo sobre TIC que creará y actualizará la política nacional de TIC; sin embargo, sólo parece haber una estrategia nacional de TIC (2011), y no menciona problemas cibernéticos ni protección de datos (Flowers, 2011). La Estrategia Nacional de Gobierno Electrónico y el Plan de Trabajo 2015-2018 es otro marco creado por Belice para guiar a su Oficina Central de Tecnología

de la Información (CITO) para producir el marco del gobierno electrónico.

Aunque la estrategia no se centra mucho en la seguridad cibernética, uno de sus pilares es mejorar la seguridad nacional, con uno de los muchos objetivos destinados a «construir capacidad técnica y legislativa para responder, mitigar y proteger del cibercrimen y los delitos dentro del sector público». La estrategia también recomienda la creación de un equipo de respuesta a incidentes de seguridad informática (CSIRT) para producir información de seguridad cibernética, apoyo en caso de un incidente cibernético y colaboración. Sin embargo, no se ha creado el CSIRT, aunque la policía nacional a menudo colabora con CSIRT internacionales cuando se trata de problemas cibernéticos. Belice no cuenta con legislación sobre seguridad cibernética, mencionan en su estrategia la importancia de proteger la infraestructura crítica y la necesidad de proteger las redes de información, aunque no definen qué es infraestructura crítica en el país.

Por último, la estrategia afirma que el CITO trabajará con la agencia responsable del cibercrimen y la ciberseguridad para producir una política y estrategia, así como un plan de acción nacional de ciberseguridad, y asegura que el gobierno de Belice se centrará en la creación de políticas y legislación que respalden la estrategia. En 2017, se organizó un Simposio de Seguridad Cibernética nacional con el objetivo de la colaboración y el desarrollo entre los sectores público y privado que se ocupe de cuestiones de seguridad cibernética. Si bien es cierto que se han desarrollado eventos como simposios, y se han creado varias estrategias que se ocupan de las futuras regulaciones de seguridad cibernética, el país no ha implementado completamente ninguna de las pautas que abordan cuestiones cibernéticas y carece de la AAP para la cooperación.

Al igual que muchos otros países de LAC, el enfoque de Trinidad y Tobago con respecto a la ciberseguridad ha estado en la protección de datos. La regulación más reciente del país es la Ley de Protección de Datos (DPA) de 2011, que brinda protección a la privacidad personal y la información que es

recopilada por organismos públicos y privados; sin embargo, la DPA funciona como si no se hubiese implementado, ya que el organismo de aplicación de la ley, la Oficina del Comisionado de Información, aún no se ha establecido, y muchas de las disposiciones de la DPA no se han puesto en ejecución (Tobago, 2012). El comisionado de información, al establecerse, tendría la capacidad de ingresar a las bases de datos e interrogar a los ciudadanos, así como buscar y recopilar sus datos sin una orden judicial (Lyn-der-say, 2019). Esto, junto con el hecho de que ciertas disposiciones del proyecto de ley aún no se han ejecutado (como las que protegen los derechos de los periodistas), ha generado preocupaciones sobre el equilibrio correcto de la privacidad y los derechos constitucionales a la libertad. En 2016, el Ministerio de Administración Pública y Comunicaciones acordó revisar y potencialmente modificar la ley, pero hasta la fecha, no se han implementado los cambios.

El Gobierno también ha creado una APP que incluye los operadores públicos y privados y los propietarios de infraestructura energética crítica, que se enfoca en prevenir, anticipar y responder a todas las amenazas al sector energético del país. Con respecto al delito cibernético, Trinidad y Tobago elaboró una estrategia nacional de seguridad cibernética en 2012, que tuvo como objetivo proporcionar pautas para toda la legislación al respecto. Algunas de las cosas más importantes que hace este documento es definir la infraestructura crítica en la nación, y centrarse en la interdependencia de la protección de la infraestructura de información crítica (CIIP) y la protección de la infraestructura crítica (CIP), utilizando el marco y la asociación internacional para implementar la legislación y crear la conciencia educativa y de formación. Si bien el marco presenta buenas ideas, aún no ha cumplido todas sus potencialidades.

El Proyecto de Ley de Delitos Cibernéticos de 2017 aún no se ha promulgado y enfrenta una gran reacción social. Al igual que el DPA, el proyecto de ley penaliza a periodistas y denunciantes que filtren datos obtenidos ilegalmente, incluidos documentos del Gobierno. Éste es un problema para los ciudadanos porque este tipo de filtraciones son algunas de las únicas formas en que

puede responsabilizar al Gobierno, y la falta de leyes establecidas impide la capacidad del país para avanzar en esta materia. Además, hay un retraso en la conciencia y los avances en seguridad cibernética debido a la falta de voluntad política para asignar los recursos financieros y humanos.

Regulaciones del ciberespacio en países que utilizan una combinación de sistemas de derecho civil y común

Con respecto a los países de la región que utilizan una combinación de ambos sistemas legales, hemos optado por analizar los esfuerzos legislativos de Guyana y Puerto Rico. Guyana actualmente no tiene legislación sobre protección de datos. En 2015, el Gobierno modificó su proyecto de ley de las instituciones financieras para permitir que la autoridad de recaudación de ingresos de Guyana (GRA) acceda a los datos de todos los ciudadanos para diversos fines de investigación, lo que suplantó el requisito del proyecto de ley anterior para que el GRA haga una solicitud legal antes de obtener acceso a dichos datos (Paul, 2015). Esto recibió críticas de la Comisión del Sector Privado (PSC) debido a la falta de legislación que proteja la información confidencial en el país. Aunque el PSC recomendó la adopción a corto plazo del marco legal aplicado en Estados Unidos por el fiscal general, no se ha logrado nada en este sentido (*Guyana Times*, 2015).

Desde entonces, el Gobierno ha declarado públicamente que la necesidad de dicha regulación de privacidad aún no es necesaria debido a las obligaciones de los tratados internacionales con EE. UU. (Paul, 2015). Como la Ley de Cumplimiento Fiscal de Cuentas Extranjeras (FACTA) la cual exige que las personas que viven fuera de EE. UU. produzcan informes anuales de sus cuentas financieras no estadounidenses, que para Guyana proviene del GRA. En términos de entidades gubernamentales, Guyana tiene una Agencia Nacional de Gestión de Datos que no se enfoca en aspectos de protección de datos (Telecommunica-

tions, 2016). En 2018, se aprobó un proyecto de ley de cibercrimen que fue originalmente criticado por el Partido Progresista Popular de la oposición (PPP) por cláusulas que restringían los derechos de la prensa y amenazaba a los denunciantes al criminalizar a los usuarios de computadoras que promuevan el descontento hacia el Gobierno.

En este sentido, el Gobierno produjo enmiendas que eliminaron los obstáculos a la prensa libre y definió de manera más rígida el tipo de datos electrónicos que se prohibirían. Incluso con estas enmiendas vigentes, el congreso continuó en desacuerdo sobre varias disposiciones y se negó a asumir la responsabilidad de incluir ciertas cláusulas, ya que el PPP no estuvo presente para votar en ciertos momentos del proceso de enmienda del proyecto de ley o careció de los poderes para votar. Todavía se carece del apoyo de ciertos miembros del Gobierno (Reporter, 2018). Una ventaja del proyecto de ley es que es un requisito para los funcionarios encargados de hacer cumplir la ley, incluidos los fiscales estatales y la capacitación obligatoria en seguridad cibernética, sin embargo, los profesionales del derecho aún no han recibido dicha capacitación.

Además, muchos abogados han argumentado que el proyecto de ley no está alineado con la Convención de Budapest y carece de disposiciones que permitan la cooperación internacional, sin embargo, Guyana no ha firmado ni ratificado la convención y, por lo tanto, no está legalmente vinculada a ella (COE, 2018). Además, Guyana está atrasada en la evaluación de sus activos y vulnerabilidades de infraestructura crítica (CNI), y los propietarios de CNI rara vez se adhieren a los estándares de seguridad o informan de incidencias debido a la falta de legislación sobre la identificación de CNI (Bank e IDB, 2016). En 2015, Guyana colaboró con expertos del Comité Interamericano contra el Terrorismo (OEA / CICTE) de la OEA en un taller para identificar las mejores prácticas de otros países en el desarrollo de un marco de política nacional de ciberseguridad, como en Trinidad y Tobago (StabroekNews, 2015).

Otro objetivo del taller fue establecer una fuerza de tarea nacional para abordar las necesidades cibernéticas del país, lo que

aún no se ha logrado. Aunque el país ha establecido un CIRT nacional para proporcionar análisis y respuesta a incidentes de los problemas de seguridad cibernética, sus capacidades son limitadas debido a la ausencia de una estrategia o política nacional de seguridad cibernética y la falta de conciencia sobre los problemas relacionados con la ciberseguridad en el Gobierno. El CIRT tampoco se rige por la legislación, sino por la aprobación del gabinete, y actualmente no existe un requisito legal para que el sector privado denuncie los incidentes cibernéticos al Gobierno. Los principales desafíos para el futuro en materia de regulación de la seguridad cibernética de Guyana son la falta de personal con las habilidades requeridas, la ausencia de regulaciones nacionales, la capacitación inadecuada y el hecho de que las amenazas de seguridad cibernética actualmente no son vistas por el Gobierno como prioridad (OAS y Symantec, 2014).

Antes de explicar los esfuerzos regulatorios en Puerto Rico, es importante comprender el sistema legal como territorio asociado de Estados Unidos, la región de LAC, así como que la mayoría de los puertorriqueños ven el territorio como parte de América Latina. Antes de su afiliación con los EE. UU., se utilizaba el código civil español. Debido a que EE. UU. utiliza un sistema de derecho consuetudinario basado en la doctrina del precedente judicial, Puerto Rico adoptó un sistema legal mixto que incorpora aspectos de derecho consuetudinario y civil (Zorilla y Law, 2019). En este sentido, tiene la capacidad de crear y enmendar su propia constitución, el título 48 del Código de EE. UU., «Territorios y posesiones insulares», requiere que Puerto Rico adopte todas las leyes estatutarias de EE. UU., que no son «localmente inaplicables» (Institute, 2012). El país tiene su propia Corte Suprema y aplica nuevas leyes basadas en precedentes de jurisprudencia (Institute, 2010); sin embargo, la Corte Suprema de EE. UU. puede revisar las decisiones de la Corte Suprema de Puerto Rico en un *writ of certiorari* (capacidad de revisión de las decisiones de la corte).

Puerto Rico adoptó la legislación de seguridad cibernética de EE. UU., y ha implementado sus propias regulaciones, a saber, de protección de datos (Seda-Fernandez y Haack, 2019). Actual-

mente no tiene una autoridad general o una ley única que describa amplias regulaciones de protección de los datos de los ciudadanos. Sin embargo, existen algunas leyes individuales que regulan aspectos de la información de identificación personal de los ciudadanos. Una de las primeras piezas de la legislación relativa a la protección de datos personales es la ley 111 de 2005 (Ley de Seguridad de la Información Ciudadana de los Bancos de Datos), que establece requisitos para que las entidades comerciales protejan la información personal de los consumidores que actualmente están bajo la custodia de dichas entidades.

La ley 234 se implementó en 2014 para exigir a las entidades comerciales que descarten todos los datos para proteger la privacidad del consumidor al eliminar la información personal, y que sea ilegible o indescifrable por cualquier método (Yordán, 2019). Recientemente, se ha presentado el proyecto de ley 607 a la Cámara de Representantes que modifica la ley 234 para exigir a los titulares de información de identificación personal que notifiquen a los consumidores sobre violaciones o acceso no autorizado a su información personal dentro de las 24 horas posteriores de darse cuenta (States, 2017). Esta enmienda tiene por objeto proteger aún más los datos personales de los ciudadanos y ampliar las protecciones contra el robo de identidad.

Reconociendo la falta de legislación que establezca parámetros para proteger las crecientes acumulaciones de datos personales por parte de las empresas, también ha propuesto el proyecto de ley 1231 del Senado, que crearía la Ley de Protección de Privacidad Digital para garantizar los derechos a la privacidad al incluir regulaciones de protección para la información contenida en bases de datos automatizadas y manuales de negocios del sector privado. El objetivo principal del proyecto de ley es permitir que los ciudadanos exijan a una empresa que se abstenga de vender su información personal a terceros, lo que actualmente no está restringido. Además, los ciudadanos podrían solicitar a una empresa que elimine su información personal de sus bases de datos o registros y avisar a terceros con los que se

han compartido los datos para que hagan lo mismo (Miranda, 2019).

Hasta ahora, los intentos de adaptar leyes obsoletas muestran su compromiso de abordar las nuevas amenazas que surgen del acceso mejorado a la información personal. El problema principal que se enfrenta es la falta de una autoridad global de protección de datos o ciberseguridad para abordar los problemas de privacidad y seguridad. Además, se carece de una ley de protección de datos que abarque todos los aspectos de los problemas de seguridad de los ciudadanos, así como la ausencia de cualquier regulación de seguridad cibernética, específicamente con respecto a la infraestructura crítica, ya que el Gobierno aún no ha comenzado su discusión.

Conclusiones

Los países de la región de América Latina y el Caribe enfrentan muchos desafíos de seguridad cibernética dado el rápido ritmo de las amenazas. La mayoría de los obstáculos provienen de la falta de coordinación entre los sectores público y privado, los recursos y la capacidad mínimas, la ausencia de un marco legal y la incapacidad para implementar regulaciones lo suficientemente rápido como para mantenerse al día con las nuevas amenazas, especialmente en los países que utilizan sistemas de derecho civil.

Los países que se centran en la protección de datos y la privacidad, a menudo descuidan la definición y protección de su infraestructura crítica, y los países que forman una legislación sobre delitos informáticos se centran en acceder a la información de los ciudadanos y, por esta razón, se ha generado rechazo público debido a preocupaciones de privacidad; los países de derecho civil también pueden tener dificultades para establecer APP útiles debido a la falta de libertad de contratación. Los países de LAC que utilizan el derecho consuetudinario aún no han creado jurisprudencia sobre estos temas, la naturaleza fluida de EE. UU. ha demostrado la flexibilidad del sistema, especialmen-

te cuando se trata de cuestiones de privacidad. Por ejemplo, en 2018 *Carpintera vs. Estados Unidos* creó un precedente declarando un requisito de orden legal para obtener datos de teléfonos celulares de ciudadanos estadounidenses (Wessler, 2018).

Si bien la jurisprudencia en EE. UU. es útil, la UE sirve como pionera en los esfuerzos cibernéticos, y a menudo influye en las acciones de regiones como EE. UU. y LAC. Es probable que a la UE le resulte más fácil lidiar con los problemas de ciberseguridad porque utilizan un sistema legal mixto, que incorpora aspectos tanto del derecho civil como del derecho consuetudinario. Esto les permite gobernar sobre ciertos aspectos de la ley, ya que no se mezclan los intereses políticos y la competencia en el mercado y han aumentado sus capacidades debido a su libertad de contrato a través de las APP y la cooperación internacional para implementar el compromiso general con la seguridad cibernética. La UE también se centra en algunos de los aspectos más importantes de la ciberseguridad: privacidad de datos, infraestructura crítica y cibercrimen.

En 2018, la UE aprobó un Reglamento General de Protección de Datos (GDPR) con el objetivo de actualizar las leyes que protegen la información personal de los ciudadanos. El GDPR no sólo otorga control a los ciudadanos sobre sus datos, sino que también regula cómo los actores públicos y privados manejan la información personal (EUGDPR, 2018). Además, a diferencia de EE. UU, la UE se toma muy en serio la competencia en el mercado y la protección de datos. Actualmente, la región está buscando combinar los dos en un conjunto de restricciones que promuevan el valor de mercado de las compañías más pequeñas mientras regulan las compañías con gran poder de mercado que tienen acceso ilimitado a los datos de los usuarios.

En Estados Unidos, el poder del mercado en línea se mide por la cantidad de datos que un usuario está dispuesto a ceder a una empresa, y aquellos que acceden a la mayoría de los datos, como Facebook y Twitter, a menudo absorben los valores de los competidores menores, en otras palabras, monopolizan el mercado. Los tribunales a menudo sólo ven los monopolios comerciales en línea como un problema si claramente perjudican a los

consumidores. En este sentido, a la UE le resulta más fácil regular estas empresas, ya que los debates antimonopolio en Estados Unidos generalmente se procesan ante un juez, mientras que, en la UE, la propia Comisión Europea tiene el poder de decidir casos sin la aprobación de los Gobiernos nacionales. En Estados Unidos, sólo las agencias federales pueden imponer este tipo de leyes federales (Economist, 2019). Además, la privacidad es un derecho fundamental en la Carta de la UE, como la libertad de expresión que también está en la Constitución de Estados Unidos.

Debido a la postura dura de la UE sobre la privacidad, los reglamentos aquí a menudo son discutidos por sus mismos tribunales para determinar si las leyes estadounidenses son lo suficientemente protectoras como para permitir que los datos europeos fluyan a través de EE. UU. Si las regulaciones no están a la par con las de la UE, el funcionamiento de las compañías de internet de otros países, como las de Estados Unidos, podrían verse comprometidas (Economist, 2019). Además de las preocupaciones de privacidad, el Parlamento Europeo aprobó una ley de ciberseguridad (2019) que se centra en la experiencia de la Agencia de la Ciberseguridad de la Unión Europea (ENISA) y en el desarrollo de legislación, considerando las mejores prácticas, mejorando el desarrollo de capacidades en los Estados miembros, proporcionando educación y capacitación, y mejora de la cooperación con las APP para combatir los problemas de ciberseguridad y proteger la infraestructura crítica (Kurth, 2019).

Si bien la ciberdelincuencia se incorpora a la ley, también hay otros organismos que trabajan para combatir los ataques contra la infraestructura crítica, como el Centro Europeo de Ciberdelincuencia de Europol, junto con los esfuerzos de ENISA (EUR-LEX, 2013). En línea con los estándares de la UE, muchos países de LAC han seguido estas prácticas y adoptado regulaciones en congruencia con el GDPR. Brasil, por ejemplo, basó su ley de privacidad de datos en la UE, y muchos Estados de LAC han

aceptado las normas para la protección de datos, que utilizan el GDPR como una guía de política (Day, 2018).

Además, muchos países de LAC han acordado adherirse a la Convención de Budapest, que es un acuerdo internacional que establece los requisitos del marco de seguridad cibernética para cada miembro. Sin embargo, aún faltan acuerdos internacionales. Muchos países que han firmado y ratificado la Convención de Budapest aún no han implementado sus recomendaciones, y la convención no tendrá suficiente efecto sin la ratificación de miembros más grandes de la comunidad, como Rusia y China. Además, debido a que el ciberespacio no tiene límites, el derecho internacional vinculante es demasiado difícil de aprobar. Si bien las Naciones Unidas (ONU) han intentado trabajar para aliviar las amenazas internacionales de ciberseguridad, no se ha hecho mucho en lo referente a la adhesión internacional.

Los actos de delito cibernético son casi imposibles de identificar, y ningún tribunal de la comunidad internacional escucha casos relacionados con delitos informáticos internacionales, ya que no existe una ley internacional establecida que los prohíba y que sea vinculante para todos los Estados miembros de la ONU, y no existe una definición acordada de lo que constituye un cibercrimen (Chang, Chung, Chen y Chou, 2003). Realizar investigaciones para probar un ataque también es difícil sin infringir la soberanía de otra nación (UNODC, 2013). Es probable que el Consejo de Seguridad de las Naciones Unidas no presente una resolución sobre el delito cibernético debido a su composición actual, que incluye a Rusia y China, dos países que no se beneficiarían de tal resolución. Debido a estos problemas, así como a los mencionados anteriormente, es probable que la región continúe siguiendo a la UE para establecer sus propias regulaciones, y la utilización de la cooperación internacional y el establecimiento de APP como mecanismos más factibles para aumentar las posibilidades de regulación estaría dependiendo de la implementación de una legislación sólida a fin de combatir los problemas de ciberseguridad.

Referencias bibliográficas

- Anatel (2017). Agencia Nacional de Telecomunicaciones. Recuperado de <https://www.anatel.gov.br/legislacao/procedimentos-de-fiscalizacao/887-portaria-50640>
- Bank, I. A. D. (2016a). IDB. Cybersecurity: Are We Ready in Latin America and the Caribbean. Recuperado de <https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean>
- Bank, I. A. D. (2016b). IDB. Recuperado de <https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean>
- Belize, Government (2000). Government of Belize. Recuperado de <http://unpan1.un.org/intradoc/groups/public/documents/tasf/unpan025201.pdf>
- Chang, W., Chung, W., Chen, H. y Chou, S. (2003). An International Perspective on Fighting Cybercrime. *Intelligence and Security Informatics*, (2665), 379-384.
- COE. (2018). Cybercrime Digest. Cybercrime Programme Office of the Council of Europe (C-PROC). Recuperado de <https://www.coe.int/documents/9252320/19115368/CPROC+Digest+2018-05-01.pdf/bcef7798-011b-92b4-def8-4ed13dd03b4c>
- Colombia (2016). El futuro digital es de todos. Colombia cuenta con una política nacional de seguridad digital. Recuperado de <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/Noticias/15033:Colombia-cuenta-con-una-Politica-Nacional-de-Seguridad-Digital>
- Colombia (2018). Freedom on the Net 2018. Freedom House. Recuperado de <https://freedomhouse.org/report/freedom-net/2018/colombia>
- CyberCrime@IPA. (2011). CyberCrime@IPA. CyberCrime@IPA project of the Council of Europe and the European Union. Recuperado de <https://rm.coe.int/2467-htcu-study-v30->

9nov11/16802f6a33

- Day, J. (2018). Privacy and Cybersecurity Developments in Latin America. JDSUPRA. Recuperado de <https://www.jdsupra.com/legalnews/privacy-and-cybersecurity-developments-13277/>
- Economist, T. (2019a). The Cambridge Analytica Bill.
- Economist, T. (2019b). The Power of Privacy.
- EUGDPR. (2018). GDPR Key Changes. Recuperado de <https://eugdpr.org/the-regulation/>
- EUR-LEX. (2013). Directive 2013/40/EU. Recuperado de <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PD>
- Flowers, G. (2011). Government of Belize. E Belize Accelerating Development. Recuperado de <http://lincompany.kz/pdf/Africa/Beliz2011.pdf>
- Fukuyama, F. (2011). *The origin of political order*. Nueva York: Farrar, Straus and Giroux.
- García, C. J. (2016). Diálogo digital. Military Magazine. Cyberdefense and Cybersecurity in Colombia. Recuperado de <https://dialogo-americas.com/en/articles/cyberdefense-and-cybersecurity-colombia>
- García, J. A. (2016). Diálogo digital. Military Magazine. Cyberdefense and cybersecurity in Colombia. Recuperado de <https://dialogo-americas.com/en/articles/cyberdefense-and-cybersecurity-colombia>
- Goldfajn, I. (2018). Banco Central Do Brasil. Resolucion CMN 4,658. Recuperado de <https://www.bcb.gov.br/ingles/norms/Resolution%204658.pdf>
- GuyanaTimes. (2015). Govt to Address Concerns on Data Protection Laws. Ministry of Global Affairs.
- Institute, L. I. (2010). 28 U. S. 734. Cornell Law.
- Institute, L. I. (2012). Cornell Law. 48 YSC 734.

- Kujawski, A. C. (2018). Law Reviews. Recuperado de <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175622/brazil>
- Kurth, H. A. (2019). EU Parliament Approves the Proposal for Cybersecurity Act. Hunton Security Blog. Recuperado de <https://www.huntonprivacyblog.com/2019/03/28/eu-parliament-approves-the-proposal-for-cybersecurity-act/>
- Lyn-der-say, M. (2019). The Challenge of the Data Protection Bill. Trinidad and Tobago DLA Piper. Recuperado de <https://www.dlapiperdataprotection.com/index.html?t=law&c=TT>
- Meyer, A. (2010). Brazil Infrastructure. Recuperado de <https://www.brazil.org.za/brazil-infrastructure.html>
- Miranda, M. (2019). Bill Introduced to protect, regulate, personal data in Puerto Rico. Caribbean Business. Recuperado de <https://caribbeanbusiness.com/bill-introduced-to-protect-regulate-personal-data-in-puerto-rico/>
- Muggah, R. (2016). Legal and Regulatory issues Concerning Public-Private Partnership. World Bank Group. Recuperado de <https://ppp.worldbank.org/public-private-partnership/legislation-regulation>
- Muggah, R. (2017a). Jane's by IHS Markit. Recuperado de https://www.janes.com/images/assets/518/73518/Brazil_struggles_with_effective_cyber-crime_response.pdf
- Muggah, R. (2017b). Jane's Military & Security Assessment Intelligence Center 2017. Jane's by IHS Markit. Recuperado de https://www.janes.com/images/assets/518/73518/Brazil_struggles_with_effective_cyber-crime_response.pdf
- Muggah, R. (2018). Council of Foreign Relations. Brazil's Critical Infrastructure Faces a Growing Risk of Cyberattacks. Recuperado de <https://www.cfr.org/blog/brazils-critical-infrastructure-faces-growing-risk-cyberattacks>

- OAS y Symantec. (2014). Latin America and Caribbean Security Trends. Organization of American States. Recuperado de https://www.symantec.com/content/en/us/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf
- Organization of American States (2015). Organization of American States. Trend Micro. Recuperado de <https://www.sites.oas.org/cyber/Documents/2015%20-%20OAS%20Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf>
- Oyen, T. (2017). Cornell Law School. Legal Information Institute. Recuperado de https://www.law.cornell.edu/wex/stare_decisis
- Paul, J. (2015). iNewsGuyana. No Immediate Need for Data Protection Laws-Finance Minister. Recuperado de <https://www.inewsguyana.com/no-immediate-need-for-data-protection-laws-finance-minister/>
- PPPLRC (2006). World Bank Group. World Bank. Recuperado de <https://ppp.worldbank.org/public-private-partnership/legislation-regulation/framework-assessment/legal-systems/common-vs-civil-law>
- Reporter, S. (2018). Cybercrime Bill Passed. Guyana Chronicle. Recuperado de <http://guyanachronicle.com/2018/07/21/cybercrime-bill-passed>
- Seda-Fernández, E. J. y Haack, M. Y. (2019). Data Privacy Law. Recuperado de <https://practiceguides.chambers.com/practice-guides/employment-2019/puerto-rico/3-data-privacy-law>
- Silva, N. B. (2018). LawReviews. The privacy, Data protection and cybersecurity law review. Recuperado de <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-5/1175627/colombia>
- Souza, D. P. (2019). ICLG.com. Brazil: Cybersecurity 2019. Recuperado de <https://iclg.com/practice-areas/>

- cybersecurity-laws-and-regulations/brazil
- StabroekNews. (2015). Gov't to Hold Cyber Security Workshop. Recuperado de www.stabroeknews.com/2015/news/guyana/08/05/govt-to-hold-cyber-security-workshop/
- States, O. (2017). Puerto Rico House Bill 607. Recuperado de <https://openstates.org/pr/bills/2017-2020/PC607/>
- Telecommunications (2016). For more on The National Data Management Agency. Recuperado de <https://mopt.gov.gy/agencies/national-data-management-agency/>
- Tobago, G. O. (2012). DLA PIPER. Data Protection Laws of the World. Recuperado de <https://www.dlapiperdataprotection.com/index.html?t=law&c=TT>
- UNODC. (2013). Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime (UNODC). Recuperado de https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf
- UNODC (s. f.). United Nations Office on Drug and Crime. SHERLOC Sharing Electronic Resources and Laws Crime. Recuperado de <https://sherloc.unodc.org/>
- Valeriano, J. y M. (2017). *Cyber Strategy the evolving character of power and coercion*. Nueva York: Oxford University Press.
- Weaver, Y. (2016). LSL CPAs and Advisors. Recuperado de <https://lslcpas.com/basic-differences-common-law-system-civil-law-system-terms-contracts-business/>
- Wessler, N. F. (2018). The Supreme Court's Groundbreaking Privacy Victory for the Digital Age. ACLU. Recuperado de <https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age>
- Yordán, N. T. (2019). Medida P C1484. Recuperado de oslpr.org/legislatura/tl2013/tl_busca_avanzada.asp?rcs=P%20C1484

Zorilla y Law, S. A. (2019). Puerto Rico Legal System.
Recuperado de <https://www.zspalaw.com/puerto-rico-legal-system.html>