UNIVERSIDAD DE LA REPÚBLICA

FACULTAD DE CIENCIAS SOCIALES

DEPARTAMENTO DE CIENCIA POLÍTICA

Informe Final de Pasantía Licenciatura en Ciencia Política

Ciberseguridad en Uruguay

Hacia la adhesión al Convenio de Budapest

Victoria Calcaterra Dufour

Tutor: Adolfo Garcé

2022

Indice

Introducción

Reconocido como un líder regional[1] en lo que respecta a la ciberseguridad, Uruguay aún no se ha adherido al Convenio sobre la Ciberdelincuencia firmado en Budapest en noviembre de 2001. Convenio que al 21 de junio de 2022 cuenta con sesenta y seis Estados Parte, de los cuales ocho[2] son latinoamericanos y con quince Estados Observadores, de los cuales cuatro[3] son latinoamericanos.

Mediante este trabajo se busca hacer un breve informe que sintetice la situación de Uruguay respecto a la posible adhesión al Convenio de Budapest. En el primer apartado, el foco está en el Convenio. Se busca informar sobre este "Convenio de Budapest", los requisitos y procedimiento de ingreso y especialmente su relevancia en el mundo de la ciberseguridad. Se mencionan los beneficios que obtienen los Estados al adherirse, según el Consejo de Europa. También, a través del estudio de Derechos Digitales realizado por Martins dos Santos (2022), se hará énfasis en las cuestiones que requieren ser tomadas con cierto recaudo. Serán resaltadas aquellas discusiones que estuvieron presentes en países latinoamericanos.

En el segundo apartado el foco se traslada al camino que ha recorrido Uruguay en términos de ciberseguridad y el que aún queda por recorrer. En este apartado también se hace un breve resumen sobre lo que significa la ciberseguridad en la actualidad a partir de las exposiciones realizadas en el evento sobre Ciberseguridad realizado por la Embajada de los Estados Unidos, la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic) y el Ministerio de Relaciones Exteriores en octubre de 2022. Este evento demuestra que ambos países están trabajando en una estrategia de defensa cibernética coherente, coordinada e integral.

El tercer apartado se centra en el Proyecto de Ley presentado por el diputado Sebastián Cal, Tipificación del Ciberdelito. Se menciona el motivo, la temática que abarca y críticas de expertos.

Por último, se encuentra el apartado dónde se expresan las conclusiones que merece el informe acorde a la información presentada.

Convenio sobre la Ciberdelincuencia (2001)

[1] Según "Reporte sobre Ciberseguridad 2020" del BID y OEA, y César Moliné Rodríguez, representante regional del Centro de Competencia en Ciberseguridad y Ciberdelito en República Dominicana (LAC4)
[2] Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana.
[3] Brasil, Guatemala, México y Trinidad y Tobago.

El Convenio sobre la Ciberdelincuencia[4] de Budapest fue firmado en 2001 por los Estados Europeos[5]. Según el Consejo Europeo (2022), es considerada como la norma internacional más relevante y completa en cuanto a la ciberseguridad cuyo objetivo es servir como guía a los Estados al momento de legislar en esta materia y como marco para la cooperación internacional.

Desde su creación ha tenido dos protocolos adicionales, el primero (2003) tiene como objetivo incriminar los actos racistas y xenófobos; y el segundo (2021), y más reciente, potenciar la cooperación internacional entre Estados, entre autoridades competentes y con el sector privado y la divulgación de pruebas electrónicas. Cada Estado Parte es libre de adherir o no a cada nuevo Protocolo.

Además de ser un tratado entre Estados, organizaciones internacionales como lo son las Naciones Unidas, la OCDE[6], la Unión Europea y el G8[7] también se han comprometido a cooperar en términos de lucha en contra de la delincuencia cibernética (Convenio sobre la Ciberdelincuencia, 2001: 3).

En el Preámbulo del Convenio se aclara que se ha tenido presente la necesidad de garantizar el respeto de antiguos tratados sobre Derechos Humanos y libertades fundamentales.

El documento consta de cuatro capítulos, (I) terminología, (II) medidas que deberían adoptarse a nivel nacional, (III) cooperación internacional y (IV) cláusulas finales. Los de mayor relevancia y controversia resultaron ser el segundo y el tercero. Es de común acuerdo la importancia de legislar en pos de combatir el cibercrimen, fortalecer la ciberseguridad de la población y cooperar internacionalmente, aún así, resulta difícil que una norma de tal generalidad logre armonizar con la legislación de cada uno de los Estados que pretenden adherirse. Por esta razón el principal requisito es la adecuación jurídica de los Estados al Convenio. A su vez, esta falta de especificidad en la norma genera cautela por parte de los Estados latinoamericanos al momento de tomar la decisión final, como lo es en el caso de Brasil (Martins dos Santos, 2022)

[4] La ONU (2020) define como ciberdelincuencia: *"Acto que infringe la ley y que se comete usando las tecnologías de la información y la comunicación (TIC) para atacar las redes, sistemas, datos, sitios web y la tecnología o para facilitar un delito (…). Se diferencia de los delitos comunes en que «no tiene barreras físicas o geográficas» y se puede cometer con menos esfuerzo y más facilidad y velocidad que los delitos comunes (aunque esto depende del tipo de ciberdelincuencia y del tipo de delito con el que se compare)"*

[5] Miembros del Consejo de Europa, Canadá, Japón, Sudáfrica y Estados Unidos.

[6] Organización para la cooperación y el Desarrollo Económico.

[7] Grupo de los 8 (Estados Unidos, Gran Bretaña, Italia, Francia, Alemania, Japón, Canadá y Rusia.)

Convenio europeo en Latinoamérica

Resulta una compleja labor para los países latinoamericanos adecuarse a una norma europea. Existe la necesidad de blindarse contra los delitos cibernéticos internacionales y también de actuar con prudencia frente a una posible pérdida de soberanía. Éste ha sido el principal argumento de los actores que cuestionaron la adhesión, entre ellos la sociedad civil y el mundo académico, así lo expresa Martins dos Santos (2022) en su análisis sobre la adhesión e implementación de este tratado en Argentina, Brasil, Chile, Colombia y México. Las discusiones en la región tuvieron como objetivo advertir sobre las tipificaciones genéricas; la ambigüedad y ambivalencia del texto; el aumento de la inseguridad jurídica penal; las posibles interpretaciones arbitrarias; los potenciales abusos de autoridades; la necesidad de la creación de leyes equilibradas; los límites de jurisdicción; la peligrosa línea de legitimación; el mayor control y la vigilancia; la protección de garantías de los derechos humanos y las libertades fundamentales (Martins dos Santos, 2022). En algunos países surgió la discusión de adhesión total o parcial. Algunos se adhirieron con reservas. Las reservas que menciona Martins dos Santos (2022) en su análisis están relacionadas a la tipificación de delitos relacionados a la pornografía infantil, a la jurisdicción, al derecho de rechazar las solicitudes de asistencia internacional en los casos en que la conducta no esté tipificada por el país, a la recolección de datos en tiempo real, a la normativa relacionada a los datos personales y protección del derecho a la privacidad.

Se puede destacar la advertencia por parte de la academia a actuar con cautela y evitar poner en riesgo el derecho a la intimidad, a la protección de datos, a libertad de expresión de los ciudadano (Martins dos Santos, 2022).

Los países latinoamericanos adheridos, si bien lo hicieron con cierto recaudo y algunos incluso con reservas, finalmente se adhirieron con convicción. Los gobernantes de los Estados Parte acuerdan en que "para prevenir y perseguir el delito cibernético es fundamental contar con mecanismos e instrumentos adecuados que permitan y faciliten la cooperación y asistencia internacional" como lo declaró el gobierno argentino en la reunión de Redacción del segundo Protocolo Adicional del Convenio (2021). Este sistema de cooperación internacional rápido, eficaz, que establece canales de intercambio de información resultó para Chile un medio adecuado para continuar con su política nacional de garantía de seguridad cibernética (Ministerio de Relaciones Exteriores, 2017).

Los beneficios para los Estados Parte son claros y contundentes (Consejo de Europa, 2022): se proporciona un marco legal para la cooperación internacional en materia de ciberdelito y evidencia digital, los miembros podrán ser parte del Comité del Convenio sobre la Ciberdelincuencia (T-CY) considerado el organismo intergubernamental más relevante en la temática, podrán participar en futuras negociaciones, existe un compromiso de cooperación confiable y eficiente, y además pueden convertirse en países prioritarios para los programas de creación de capacidad (facilita la aplicación del Convenio y mejora la cooperación).

En todos los casos la intención de adherir generó movimientos necesarios en la legislación nacional sobre ciberdelitos. Estos movimientos y discusiones se han mantenido, tal como expresó el director nacional de Ciberseguridad de Argentina, Gustavo Salín, "existe un proyecto para el diseño de una política de ciberseguridad nacional" (Diario Judicial, 2022).

Luego de que los Estados hayan legislado para armonizar con lo dispuesto en el Convenio, tal y como lo expresa el Consejo de Europa (2022): "se debe enviar una carta dirigida al secretario general del Consejo de Europa en la que manifieste el interés de su Estado en adherirse al Convenio de Budapest. Una vez que exista consenso entre los actuales Estados Parte del Convenio, se invitará al Estado a adherirse. Las autoridades de ese Estado deberán formalizar sus procedimientos internos similares a la ratificación de cualquier tratado internacional antes de depositar el instrumento de adhesión ante el Consejo de Europa". Se observa que, el requisito no solo es adecuar la legislación nacional, sino también ser aceptado por el Consejo de Europa. Si bien es un tratado internacional, hay una autoridad que mantiene el último veredicto, y ese es el Consejo de Europa.

Resulta interesante observar el fuerte empuje que se da en la región a partir de la publicación del primer reporte de ciberseguridad realizado por el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) en 2016 (Tabla 1). Como se expresa en la actualización del mismo reporte publicado en 2020, hasta la primera publicación la región no había tomado dimensión del problema. A su vez, el crecimiento en la cantidad de ciberataques también despertó la alarma, siendo el sistema financiero el principal objetivo de dichos ataques. Hasta la fecha en que se realiza el reporte, Uruguay no había demostrado intenciones de adherir al Convenio. En la actualidad, el Ministerio de Relaciones Exteriores lideró un proceso de consultas sobre la temática, Fiscalía ha mantenido reuniones con Ministerios de Justica Latinoamericanos y

Agesic mantiene contacto con la Embajada de Estados Unidos realizando encuentros para concientizar sobre la ciberseguridad. Uruguay ya mostró interés en adherir, existe una estrategia nacional de ciberseguridad en desarrollo.

Tabla 1.

Países latinoamericanos miembros y observadores del Convenio sobre la Ciberdelincuencia.

PAIS	Miembros y Observadores		Adheridos	
	Estrategia Nacional de Ciberseguridad	Estrategia Nacional de Ciberseguridad en Desarrollo	Parte	Invitados
Argentina	2019		2018	
Barbados		X		
Belize		X		
Brasil	2020			X
Chile	2017		2017	
Colombia	2016		2020	
Costa Rica	2017		2017	
Ecuador		X		
Guatemala	2018			X
Guyana		X		
Jamaica	2015			
Mexico	2017			X
Panama	2013		2014	
Paraguay	2017		2018	
Perú		X	2019	
Rep. Dominicana	2018		2013	
Suriname		X		
Trinidad y Tobago	2013			

Elaboración propia. Fuente: Reporte de Ciberseguridad BID-OEA. 2020.

A través de este reporte (2020: 16), y debido al aumento de ciberataques, las organizaciones responsables, implementan nuevamente el Modelo de Madurez de la Capacidad de Ciberseguridad (CMM por su sigla en inglés) para las Naciones que consta de cinco dimensiones (2020: 42): (I) política y estrategia en ciberseguridad; (II) cultura cibernética y sociedad; (III) educación, capacitación y habilidades en ciberseguridad; (IV) marcos legales y regulatorios; y (V) estándares, organizaciones y tecnologías. Estas dimensiones son evaluadas por cinco etapas de madurez: (I) inicial, (II) formativa, (III) consolidada, (IV) estrategia, y (V) dinámica. Luego de evaluar cada dimensión según la etapa en la que se encuentra se genera un nivel de madurez. La región mantiene un nivel bajo que prácticamente no ha avanzado desde la última medición en 2016. Uruguay se

posiciona como líder calificando con el nivel de madurez más alto en la región en cuatro de las cinco dimensiones, y con un nivel de madurez *Estratégico* en capacitación profesional (2020: 39). Si bien mantiene un muy buen nivel, especialmente respecto a la región, el nivel de madurez en la cuarta dimensión, marcos legales y regulatorios, se encuentra muy por debajo de su propio promedio.

Uruguay y la ciberseguridad

Ha habido cinco oleadas mundiales sobre tipificación de delitos cibernéticos. La primera fue en la década de 1970, protección de la privacidad; la segunda ocurrió en la primera mitad de 1980, delitos económicos; la siguiente fue en la segunda mitad de 1980, protección de la propiedad intelectual; luego en 1990 se procedió con las reformas procesales en cuanto a la prueba digital; por último, a partir del 2001 la lucha contra el terrorismo en el plano digital (Pecoy, 2021). Luego de la última oleada, comienza en Uruguay la transformación digital tan reconocida internacionalmente (El País, 2022).

Los inicios de Uruguay en las políticas digitales remontan a la segunda mitad de la década de los 2000. Hasta la fecha se distinguen cuatro grandes hitos relacionados a la ciberseguridad: en el año 2005, la creación de la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic), como una unidad ejecutora del gobierno; en el año 2008, la creación del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) dentro de Agesic; en el año 2015, la creación del Equipo de Respuesta a Incidentes de Seguridad Cibernéticos del Ministerio de Defensa (D-CSIRT); y en agosto del año 2021, la creación de la Unidad de Cibercrimen en el Ministerio del Interior. El Ministerio del Interior se encarga de los ciberdelitos, de las denuncias de privados, de individuos, por ejemplo, un intento de estafa. Las denuncias a mayor escala corresponden al CERTuy y al D-CSIRT, las unidades de mayor jerarquía en el país en esta temática. La primera se encarga de la ciberseguridad, del "monitoreo, prevención, coordinación y respuesta a incidentes de ciberseguridad" (Agesic, 2008). Por otro lado, el D-CSIRT se encarga de la ciberdefensa y tiene como misión "participar de forma eficaz y eficiente en la respuesta a incidentes cibernéticos sobre infraestructuras críticas[8] y servicios esenciales de la comunidad objetivo, así como desarrollar capacidades de prevención y detección temprana de incidentes de seguridad informática en dicha comunidad" (MDN, 2015). CERTuy es miembro de la red CSIRT Américas,

[8] Todos los sistemas físicos o virtuales, que ofrecen servicios esenciales para dar apoyo a los sistemas básicos a nivel social, económico, medioambiental y político.

esto significa que puede hacer uso de la naturaleza colaborativa de la red (Reporte BID-OEA).

En el año 2006 se lanza la primera Agenda Digital Uruguay (ADU). Hasta la fecha han habido cinco versiones, siendo la más reciente la Agenda 2025. En esta última versión se expresan los deseos y voluntades de lograr una conectividad universal de calidad del Estado con la ciudadanía. Esta meta de "Gobierno como plataforma" se verá automáticamente traducida en una mayor cantidad de datos para lo cual es necesario un entorno seguro y controlado. En función de lo mencionado anteriormente, la Agenda expresa en sus objetivos de Ciberseguridad adoptar el Marco de Ciberseguridad creado por Agesic, en servicios, infraestructura y redes críticas; educar sobre la ciberseguridad; implementar nuevas tecnologías de análisis predictivos y automatización de respuestas (AUD 2025, 2020). Esta agenda ignora la cooperación internacional, fundamental para prevenir y responder a ataques. La única mención que se observa es en el apartado de seguridad jurídica: "promover la adhesión a estándares y convenciones internacionales" (2020: 20), pero es una frase inespecífica que carece de contenido, es genérica y no expresa medios para lograrlo. Como expresó Heber Paguas[9] en la Comisión de innovación, ciencia y tecnología (2021: 2), "[Uruguay carece de] legislación específica en cuanto a ciberdelitos, [...] salvo por algunas excepciones que la analogía permite, excepcionalmente, ya que en el derecho penal no es una herramienta de uso". La especialista en seguridad de la información, Dra. Jimena Hernández[10], enfatiza en la desactualización del Código Penal uruguayo, si bien ha tenido cambios, mantiene las figuras tradicionales por lo que, en cuanto a los ciberdelitos, se amparan "en lo que tiene que ver con los accesos indebidos a sistemas o los daños que se pueden generar a un sistema" (Comisión, 2021:2).

Ciberdelincuencia

"Uruguay debe estar listo para un ataque de *ransomware*[11]. Ningún país está libre de los ciberataques" expresó Karl Ríos, Encargado de Negocios de la Embajada de los Estados Unidos en Uruguay, en el discurso inicial del evento sobre Ciberseguridad organizado por la Embajada y Agesic la última semana de octubre de 2022. Dicho evento

[9] Director Ejecutivo de Agesic

[10] Asesora Letrada de Agesic

[11] Tipo de software malicioso (*malware*) que cifra los datos de un sistema haciéndolos inutilizables para luego pedir rescate económico a cambio de la liberación de los datos.

fue realizado con el fin de generar conciencia en el país sobre la gran amenaza que significan los ciberataques y para demostrar la cooperación existente entre Uruguay y Estados Unidos. Kemba Walden[12] (Ciberseguridad, 2022) expresó las iniciativas actuales de sus oficinas: generar resiliencia[13] en el presente y futuro, medir el riesgo y las oportunidades. Para ser resiliente y robusto, es necesaria la cooperación.

El ransomware se está convirtiendo en una práctica frecuente que va en aumento y nunca va a acabar. Busca información sensible que directa o indirectamente pone en riesgo la seguridad nacional. Ya no sólo se atenta contra empresas sino también contra organismos dependientes del Estado. En los últimos años los mayores ciberataques detectados han sido motivados por intereses geopolíticos.

Anthony Frazier[14] explica que en este tipo de delito se toman los datos como rehenes a través de tácticas como, por ejemplo, el *email phishing*[15]. Se busca ingresar a un sistema, luego se procede a descargar el *malware*[16], se cifran datos, piden rescate y demandan el pago. Luego de efectuado el pago, entregan una "llave" que libera los datos. Una vez infectado el sistema y congeladas las bases de datos, el *malware* puede generar pérdida de productividad. Este delito puede realizarse a través de diferentes tipos de ataque y cada organización ciberdelictiva tiene sus preferencias. También tienen preferencias en la elección de objetivos de ataque, por esta razón, dependiendo del sistema que se vea afectado, el grupo ciberdelictivo que convierte en sospechoso. El grupo organizado REvil Sodinokibi[17] es un ejemplo de organización de ransomeware. Suele optar por la táctica de algoritmo cifrado y sus objetivos suelen ser sistemas financieros, tecnologías de la información e instituciones sanitarias (Anthony Frazier). Se

[12] Subdirectora Nacional de la Oficina "Cyber"

[13] Resiliencia en el ámbito de la tecnología de la información (TI) se entiende como la capacidad de la infraestructura, ya sea de servidores, comunicación o de seguridad, de proveer y mantener una continuidad operacional, a pesar de las fallas, tales como: problemas de sobrecarga, fallas en el datacenter, ancho de banda saturada, tráfico malicioso en la organización, amenazas avanzadas al descubierto, filtración de información confidencial y de ataque de secuestro digital de información (ransomware), etc. Esta capacidad adquiere especial importancia en la administración pública y los sistemas de información y telecomunicaciones. (Barrios, 2018: 3)

[14] Agente de la Oficina Internacional de Piratería Informática y Propiedad Intelectual (ICHIP), Departamento de Justicia, Consulado de EE.UU. en Sao Paulo.

[15] Conjunto de técnicas que persiguen el engaño a una víctima ganándose su confianza para manipularla y hacer que realice acciones que no debería hacer.

[16] Software malicioso

[17] Su procedencia no se conoce con certeza, se sospecha que podría ser rusa por ser el ruso el idioma principal de la organización.

suele atacar sistemas viejos, no actualizados. Es necesario cambiar la "higiene" de los sistemas, mantener los softwares actualizados contantemente.

Hay sectores de infraestructura crítica cuyos activos, sistemas y redes se consideran tan vitales que su incapacitación o destrucción tendría un efecto debilitante en la seguridad nacional, ellos son: sanidad y salud pública, servicios financieros, transporte, tecnología, gobierno, instalaciones comerciales. Todos los oradores hicieron mucho énfasis en que los eventos van a suceder, no se pueden evitar, si se puede tomar las medidas para lograr reponerse lo antes posible. Para esto es necesario estar preparado para detectar el ataque de manera temprana y así reducir el daño. La demora en pedir ayuda da ventajas al atacante. El intercambio de información entre Estados toma un rol significativo. Este intercambio ayudará a prevenir ataques, identificar organizaciones, brindar apoyo durante ataques y sobre todo a la recuperación de los (muy probables) futuros ataques.

Es imprescindible la cooperación entre Estados y también entre disciplinas para responder a tiempo y de manera efectiva. La formación de quienes están a cargo es tan importante como la respuesta. Hoy en día hay déficit profesional en esta área. Y aún así, como expresó Paula Brenes[18] desde Costa Rica[19], es un error considerar estos problemas como exclusivamente técnicos. Es necesaria la variedad de profesionales para crear la herramienta de solución. Diferentes personas, con diferentes especialidades, que brindan diferentes puntos de vista, resuelven problemas. Es necesario crear un sistema a través de una estrategia integral, sin parches. Esta nueva estrategia de ciberseguridad debe poner a la persona en el centro. La Sra. Brenes expresó que "hay que volver a la raíz, no hay que perder el foco de a quién estamos protegiendo: a las personas. Hay que hacer una pausa y volver a la esencia. Se debe volver a la raíz, a la política pública". Como se también se menciona en el reporte de ciberseguridad (BID, OEA: 2020, 17): *"*Contar con profesionales más capacitados se ha vuelto fundamental para diseñar e implementar las políticas y medidas de seguridad cibernética que son necesarias para garantizar la resiliencia del país frente a ciberataques cada vez más sofisticados y complejos*"*.

Luego de explicar los daños y la magnitud del mayor ataque detectado en diciembre de 2020, que penetró varios sistemas entre los más importantes los de La Casa

[18] Jefa en Governanza Digital, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), Gobierno de Costa Rica.
[19] Victima del último gran ciberataque.

Blanca y el Pentágono, el capitán Claudio López[20] destaca tres lecciones aprendidas: (I) la colaboración es vital en la ciberseguridad; (II) medir el riesgo e invertir en control; (III) estar pronto para la batalla.

Proyecto de Ley – Tipificación del Ciberdelito[21]

El tema de la ciberseguridad en Uruguay aparece en agenda a partir de que el diputado Sebastián Cal presentó el proyecto de Tipificación del Ciberdelito. Si bien es el quinto proyecto que se presenta sobre delitos informáticos, esta vez parecería haber cobrado mayor fuerza y estar más cercano a su aprobación. Hay un conjunto de razones que explican el fenómeno: la presión generada por actores internacionales como el BID y la OEA a través de su informe, delegación de la Unión Europea en Uruguay, Embajada de los EE.UU. en conjunto con actores nacionales como lo es Agesic; el aumento de los ciberataques[22] y especialmente aquellos con motivación geopolítica. No es un detalle menor que el proyecto comenzara a escribirse en plena pandemia, cuando el teletrabajo llegó a su pico máximo hasta el momento, significando vulnerabilidad en los sistemas de las empresas debido a que habían sido trasladados a las computadoras personales de sus empleados.

La presentación de este proyecto tiene como objetivo *aggiornar* la legislación nacional al Convenio de Budapest. En la exposición de motivos se expresa la necesidad de crear una Ley específica sobre la materia y a su vez se reconoce la dificultad de contemplar todos los posibles escenarios.

Como lo describe su nombre, este proyecto de Ley se basa en la tipificación de diferentes actos[23]: acoso telemático, acercamiento físico o virtual, estafa informática, daños informáticos, acceso ilícito a datos informáticos, vulneración de datos, suplantación de identidad, terrorismo digital, abuso de los dispositivos. A su vez, el último artículo sugiere una "Campaña Nacional Educativa".

Ha sido un proyecto muy debatido. La Comisión especial de innovación, ciencia y tecnología, ha recibido múltiples actores del Estado, invitados a brindar sus opiniones y recomendaciones desde la perspectiva en la que se encuentra cada uno. Las principales

[20] Jefe del Departamento de Ciberdefensa del Estado Mayor de la Defensa (ESMADE), Ministerio de Defensa Nacional, Uruguay.
[21] Ver Anexo 1
[22] Ciberataque al Ministerio de Defensa Nacional en enero de 2021 (El Observador, 2021)
[23] Ver en Anexo 1

comparecencias han sido de Agesic, del Banco Central del Uruguay (BCU) y de la Fiscalía General de la Nación. Todos ellos acuerdan en que la cooperación internacional resulta imprescindible. Los representantes de Agesic y de la Fiscalía mantienen una línea argumentativa respecto a los aspectos procesales. Jimena Hernández (Comisión Especial, 2021) sugiere crear un protocolo a seguir en las investigaciones con evidencias digitales, ya que resultan ser altamente volátiles y se necesitan herramientas efectivas. Esta sugerencia va acorde al segundo Protocolo presentado recientemente. Los representantes del BCU por su parte establecen diferencias entre la competencia administrativa que atañe al Banco y aquellas relacionadas a la tipificación del delito que corresponden a la Justicia. En las comparecencias surgieron cuestiones respecto a si los términos delictivos debían estar en inglés o en español. Especulando que quizás el uso del inglés podría generar una interpretación más amplia de la norma y que si el término estuviese en español podría ser más específico; a su vez el diputado Cal menciona que fueron utilizados los términos en inglés debido a ser requisito por parte del Convenio. En la comparecencia de Fiscalía, el diputado Cal también expresó que considera a Uruguay como "el más atrasado de la región con respecto a temas de ciberseguridad" (Comisión Especial, 2022: 5), declaración cuestionable si tenemos en cuenta los reportes realizados por el BID y la OEA.

Martín Pecoy hace un análisis comparativo muy detallado entre el proyecto de Ley y el Convenio de Budapest. Lo analiza como conjunto y luego estudia cada artículo en comparación al Convenio. Su primera puntualización refiere a la falta de justificación criminológica sobre la necesidad de crear en Uruguay las figuras mencionadas. Aún así, son delitos que Uruguay ya se había comprometido a tipificar en documentos internacionales (Pecoy, 2021), por lo que parecería ser de conveniencia su aprobación. El artículo que más apoyo ha obtenido tanto por Pecoy como por los comparecientes en la comisión parlamentaria es el No. 7; que tipifica la suplantación de identidad[24] resultando ser la gran novedad legislativa incluso respecto a Budapest. Por otro lado, Pecoy hace un análisis profundo con el objetivo de plantear futuros debates. Varios artículos del proyecto (Art. 1; 2; 6) ya están tipificados en Uruguay por lo que se podría generar conflictos de derogación tácita. Utilizando el término elegido por el Fiscal de Corte, Juan Gómez[25] (Comisión Especial, 2022), hay que evitar la *superfetación* de normas. Para Pecoy, sólo castigar no soluciona el problema (Art. 3); así como tampoco elevar el

[24] Ver Anexo 1
[25] Fiscal de Corte y procurador General de la Nación

castigo, en caso de ser ya existente, sin justificación (Art. 4, 5, 9). Respecto al Art. 8, Budapest no sugiere esta tipificación, aún así la redacción, según Pecoy, coincide parcialmente con "PARIOT" de Estados Unidos. Limita la definición de ciberterrorismo a los actos de espionaje y sabotaje.

Llama la atención la ausencia de propuestas relativas a la aprobación de la cooperación internacional. Pecoy tiene esperanzas de que Uruguay se adhiera al Convenio de Budapest, no sin un riguroso análisis previo.

Conclusión

Uruguay se encuentra muy bien posicionado en la región y en las Américas respecto a la ciberseguridad por lo que no era congruente a los ojos de los actores internacionales el hecho de no tener una Estrategia Nacional de Ciberseguridad en desarrollo. Actualmente contamos con dicha estrategia en desarrollo, el Ministerio de Relaciones Exteriores ya expresó su interés en ser miembro del Convenio de Budapest, se han mantenido las reuniones correspondientes durante el último año, y a través de la aprobación del proyecto de Ley que tipifica el ciberdelito estaremos dando un paso hacia la membresía.

El proyecto de Ley claramente es una herramienta que juega un papel importante por ser lo que podría considerarse como el "primer paso" en la legislatura nacional necesaria para adherir al Convenio. Existe una base en términos de ciberseguridad en Uruguay, ello se ve reflejado en la valoración que obtuvo el país en el "Modelo de Madurez de la Capacidad de Ciberseguridad", también en el hecho de que varios artículos del proyecto ya estaban siendo contemplados en la normativa vigente. De esta situación obtengo dos conclusiones, la primera es que Uruguay no está tan mal como el Diputado Cal considera, y la segunda que parecería haber existido un descuido al estudiar la normativa vigente. Que exista una base no es razón para mantenerse al margen de la oleada de la región. Sin duda queda mucho por hacer, empezando por la cooperación internacional que en el proyecto no se menciona, tampoco en la Agenda Uruguay Digital de 2025 que además carece de especificidad. Es necesaria la legislación adecuada para adherir al Convenio. Aún así, los actores convocados a la Comisión también presentaron sugerencias que no son requeridas por el Convenio, pero si para un mejor desempeño de su trabajo. Los actores encargados de legislar deberían involucrarse más en la temática,

para así brindarles el respaldo necesario a quienes trabajan para defender a las personas. Como dijo Paula Brenes, no hay que perder el foco: defender y cuidar a la ciudadanía. Esto está comenzando, mucho queda por hacer, el camino parece no tener fin.

Gran énfasis se hizo en el Evento sobre Ciberseguridad en el hecho de que los ataques van a ocurrir. Incluso si un Estado contara con el mejor sistema de seguridad, los ataques suceden igual y van en aumento. Como expresó David Britain[26] en el Evento de Ciberseguridad, "el nivel máximo de seguridad es igual al link más débil del sistema". Es necesario instruir en la temática. Brindar educación general en prevención, mantenimiento y actualización de los sistemas. Educación específica a las autoridades encargadas de la ciberseguridad. Es necesario crear un protocolo específico de respuesta.

Es urgente adherir al Convenio, es más importante hacerlo bien. Teniendo definiciones claras, sin ambigüedades. Las penas de los delitos deben ser acordes. Aprender de las experiencias de los países de la región, no desconocer sus discusiones y su camino hacia la adhesión. Tener en cuenta sus planteos, especialmente cuando hacen referencia a la soberanía del país y a los derechos de la ciudadanía.

Por último y no lo menos importante, debo resaltar la importancia de las diferentes disciplinas y como cada una de ellas es relevante en la solución de problemas. Es un problema en sí considerar que la ciberseguridad se resuelve solamente con técnicos de software. Paula Brenes resalta la importancia de volver a la raíz, a la política pública. Las políticas públicas atraviesan transversalmente todas las solucionas a las que se pueden llegar. En la mesa de discusión es verdad que deben estar representadas múltiples disciplinas, pero no debe faltar la Ciencia Política.

[26] Jefe de LATAC Cyber Network, Embajada Británica en Brasilia.

Referencias

Agenda Uruguay Digital 2025. (2020). “Agenda Uruguay Digital 2025”. Recuperado de: https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025

Agesic. (2005). *Creación y evolución histórica.* Recuperado de: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/institucional/creacion-evolucion-historica

Agesic. (2008). CERTuy. Recuperado de: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/tramites-y-servicios/servicios/certuy

Banco Interamericano de Desarrollo (BID). Organización de los Estados Americanos (OEA). (2020). *Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe.*

Recuperado de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Barrios, Verónica (2018). *Política Nacional de Ciberseguridad 2017-2022.* Asesoría Técnica Parlamentaria. Biblioteca del Congreso Nacional de Chile.
Recuperado de: https://www.bcn.cl/asesoriasparlamentarias/detalle_documento.html?id=74111

Ciberseguridad. (2022). *Event: Ransomware: The U.S. experience, the Costa Rica case, lessons learned, and how to protect ourselves.* Alianza, Montevideo, Uruguay. 27 de octubre de 2022.

Comisión Especial de innovación, ciencia y tecnología. (2021). Carpeta No. 972 de 2016 y 1734 de 2021. Proyecto de Ley: Tipificación de Ciberdelito. Versión taquigráfica 777, 04 de noviembre de 2021.
Recuperado de: https://parlamento.gub.uy/documentosyleyes/ficha-asunto/151908/tramite

Comisión Especial de innovación, ciencia y tecnología. (2022). Carpeta No. 1734 de 2021. Proyecto de Ley: Tipificación de Ciberdelito. Versión taquigráfica 861, 05 de mayo de 2022.
Recuperado de: https://parlamento.gub.uy/documentosyleyes/ficha-asunto/151908/tramite

Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia.*
Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo de Europa. (2003). *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.*
Traducción al español por Ministerio de Asuntos Exteriores y de Cooperación, Oficina de Interpretación de Lenguas. España, 2005. Recuperado de:

https://www.plataformaong.org/conferencia/wp-content/uploads/2014/10/Protocolo_adicional_convencion_cibercrimen.pdf

Consejo de Europa. (2022). *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: Beneficios.*
Recuperado de: https://rm.coe.int/cyber-buda-benefits-junio2022-es-final/1680a6f9f4

Consejo de Europa. (2022). *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*.
Recuperado de: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224
Última versión traducida al español (2021): https://rm.coe.int/0900001680a27dbe

Diario Judicial. (2022). *Existe un proyecto para el diseño de una política de ciberseguridad.*
Recuperado de: https://www.diariojudicial.com/nota/92613

El Observador. (Enero, 2021). *Información extraída a la Armada en ciberataque de criminal ruso se vende a US$ 500.000.*
Recuperado de: https://www.elobservador.com.uy/nota/informacion-extraida-a-la-armada-en-ciberataque-de-criminal-ruso-se-vende-a-us-500-000--202111921426

El País. (Marzo, 2022). *Proyectan a Uruguay como un Hub regional de tecnología.*
Recuperado de: https://www.elpais.com.uy/negocios/empresas/proyectan-uruguay-hub-regional-tecnologia.html

Martins dos Santos, Bruna (2022). *Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México.*
Recuperado de: https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

Ministerio de Defensa Nacional, Gobierno de Uruguay. (2015). *Equipo de Respuesta a Incidentes de Seguridad Informática de Defensa (D-CSIRT).*

Recuperado de: https://www.gub.uy/ministerio-defensa-nacional/tramites-y-servicios/servicios/equipo-respuesta-incidentes-seguridad-informatica-defensa-d-csirt

Ministerio de Relaciones Exteriores, Gobierno de Chile. (2017). *Chile deposita el instrumento de adhesión al Convenio de Budapest sobre la Ciberdelincuencia.* Recuperado de: https://www.minrel.gob.cl/chile-deposita-el-instrumento-de-adhesion-al-convenio-de-budapest-sobre/minrel_old/2017-04-21/175923.html

Ministerio de Seguridad Argentina. (2021). *Ciberdelito: Se aprobó el texto del 2° Protocolo Adicional del Convenio de Budapest.* Recuperado de: https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest

Organización de las Naciones Unidad. (2020). *La ciberdelincuencia en resumen.* Recuperado de: https://www.unodc.org/e4j/es/cybercrime/module-1/key-issues/cybercrime-in-brief.html

Parlamento del Uruguay. (2021). *Proyecto de Ley: Tipificación del Ciberdelito*. Ficha asunto: 151908. CRR. Carpeta 1734/2021. 03 de agosto de 2021. Recuperado de: https://parlamento.gub.uy/documentosyleyes/ficha-asunto/151908/tramite

Pecoy Taque, Martín. (2021). *El Proyecto de Ley uruguayo del año 2021 que pretende la tipificación delos ciberdelitos en Uruguay.* Montevideo Legal Hackers, 03 de agosto de 2021. Recuperado de: https://montevideolegalhac.wixsite.com/website/post/el-proyecto-de-ley-uruguayo-de-2021-sobre-delitos-informáticos