SOBRE CIBERDELITOS O DELITOS INFORMÁTICOS

ON CYBERCRIME OR COMPUTER-RELATED CRIME

SOBRE CRIMES CIBERNÉTICOS OU CRIMES INFORMÁTICOS

Luis González Laguna (*)

RESUMEN. El presente trabajo tiene como objetivo poder internalizar respecto del proyecto de ley sobre ciberdelitos o delitos informáticos, al mismo tiempo poder analizar la importancia, los desafíos que presenta y sobre todo visualizar tanto las cuestiones positivas para su aprobación, como negativas, contrarias, o simplemente que pueden llegar a ser cuestionables, para el derecho siempre las regulaciones presentan – aparte de la discusión- una serie de debates necesarios que tienden a mejorar la ley o norma que se pretenda integrar al ordenamiento jurídico, mediante la técnica legislativa y por supuesto la participación de especialistas de distintas áreas. Este artículo intenta mostrar la regulación que se pretende incorporar al ordenamiento jurídico uruguayo, inspirado en un instrumento internacional de referencia en el Mundo, y lo que implica de ser aprobada esta nueva tipificación de actualidad, que hoy en día es un desafío y preocupación de magnitud internacional.

PALABRAS CLAVES. Delitos informáticos. Cibercrimen. Convenio Budapest. Crimen organizado. Ciberdelincuentes.

ABSTRACT. This paper aims to delve into the draft law on cybercrime or computer-related crime, as well as to analyze the importance, the challenges, and above all to review the positive, negative and contrary issues or even issues that may be questionable for its enactment. For the law, regulations always present – apart from the discussion – a series of necessary debates that tend to improve the law or regulation intended to be incorporated into our legal system, through legislative technique and of course the participation of specialists on different areas. This paper seeks to disclose the regulation that is intended to be embedded into the Uruguayan legal system, based on a

(*) Abogado. Docente colaborador en el consultorio jurídico de asistencia a las víctimas del delito, convenio (Udelar, Asfavide, Ministerio del interior. Correo electrónico: dr.luisgonzalez101@gmail.com

world benchmark international instrument, and the implications of this new, current regulation, which is a worldwide challenge and concern.

KEY WORDS. Computer-related crime. Cybercrime. Budapest convention. Organized crime. Cybercriminals.

RESUMO. O presente trabalho tem como objetivo permitir a internalização em relação ao projeto de lei sobre cibercrimes ou crimes informáticos, ao mesmo tempo poder analisar a importância, os desafios que apresenta e sobretudo visualizar tanto as questões positivas para sua aprovação, como negativas, contrárias, ou simplesmente que podem chegar a ser questionáveis. Para o direito sempre os regulamentos apresentam - além da discussão- uma série de debates necessários que tendem a melhorar a lei ou norma que se pretenda integrar na ordem jurídica, através da técnica legislativa e, evidentemente, da participação de especialistas de diferentes áreas. Este artigo tenta mostrar a regulamentação que se pretende incorporar ao ordenamento jurídico uruguaio, inspirado em um instrumento internacional de referência no mundo, e o que implica de ser aprovada esta nova tipificação de atualidade, que hoje é um desafio e uma preocupação de magnitude internacional.

PALABRAS - CHAVES. Crimes informáticos. Cibercrime. Convênio Budapest. Crime organizado. Cibercriminosos.

Introducción

Nos encontramos hoy en el mundo con un avance exponencial de la tecnología, dispositivos electrónicos, software y equipos técnicos; estas herramientas no solamente ayudan al ser humano a ser más eficiente en los soportes o plataformas digitales y al desempeño de las empresas, sino también son utilizados para violentar información, manipular datos, concretar hechos ilícitos y lesionar bienes jurídicos. En 2020 la crisis sanitaria a nivel global produjo una aceleración de los medios tecnológicos, los cuales tuvimos que poner en funcionamiento a nivel mundial para poder derribar los obstáculos de la cuarentena y aislamiento social, dar continuidad al funcionamiento de la comunidad tanto desde los centros educativos como de las grandes corporaciones. Las potencias más grandes impulsaron plataformas y mecanismos para continuar de una u otra manera con la vida social y una nueva normalidad. Por definición podemos hablar de Ciberdelitos en forma genérica haciendo mención de una actividad delictiva, la cual es menester se realice con equipos informáticos o a través de redes en Internet. Esta nueva modalidad delictual -ya regulada en otros países de la región y el mundo-, o calificada como tal, es cometida por sujetos llamados ciberdelincuentes a través de medios tecnológicos, equipos informáticos o internet. Los ciberdelincuentes atacan a personas físicas, jurídicas, entidades u organismos y/o agencias del gobierno con diferentes objetivos, la nómina puede ser bastante amplia: desde dañar, destruir, violentar información confidencial para realizar es-

tafa económica o simplemente con el fin de llevar adelante una acción que no ingrese dentro de la calificación (ciberdelito).

En un informe de la O.E.A. legisladores e investigadores en las Américas son quienes han tenido que centrarse en la persecución y sanción de los delitos cibernéticos, como la pornografía infantil, acoso, entre otros. Según estimaciones de LACNIC, el organismo que maneja el registro de direcciones de Internet para América Latina y el Caribe, el cibercrimen le cuesta a nuestra región alrededor de 90.000 millones de dólares al año.

En nuestro derecho no tenemos regulación aprobada pero recientemente ha ingresado un proyecto de ley al Parlamento para su tratamiento (carpeta N°1734 de 2021).

Convenio Budapest

El proyecto tiene como antecesor el Convenio de Budapest sobre ciberdelitos del 23 de noviembre del año 2001; se trata del primer tratado internacional creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en Internet mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y de la cooperación internacional. Dentro de cada uno de los tipos penales, la redacción de Budapest sobre cibercrimen otorga un margen a cada país, de forma tal que la norma se vuelve más o menos punitiva en los diferentes ordenamientos jurídicos. El convenio no solo incluye y menciona delitos sino también normas procesales, que son las más controvertidas dentro del ámbito.

Existe una inequidad a favor de la seguridad por sobre las garantías de los ciudadanos; en estos puntos muchos países han puesto reservas a la hora de ratificar el Convenio, surgiendo las siguientes interrogantes: ¿los Estados pueden grabar todas las actividades en línea?, ¿cuándo lo pueden hacer?,¿por cuánto tiempo? Existe un límite muy sagaz entre la privacidad de datos y el acceso a la información. Cabe mencionar que este instrumento internacional tomado por la mayoría de los Estados no contemplaba situaciones como la de Edward Snowden y la compra por parte de varios gobiernos de herramientas de espionaje, así como para el mundo del tráfico de datos personales.

Proyecto uruguayo

En primer lugar es importante mencionar que en Uruguay ya se han presentado 4 proyectos con influencia en el instrumento europeo sobre cibercrimen (Budapest), que no tuvieron éxito, es decir que estamos hoy en la discusión sobre el 5to proyecto referido al tema, el mismo propone la creación de 9 ciberdelitos y medidas educativas, que tienen como objetivo

advertir y prevenir respecto del uso de herramientas informáticas, instruir a la ciudadanía en el manejo de sus finanzas personales a través de medios digitales y ciberseguridad. Asimismo, la propuesta legislativa menciona medidas educativas dirigidas a estudiantes de secundaria y escuelas técnicas. Finalmente, el proyecto deja abierta la posibilidad de definir ciertos conceptos que se consideran como relevantes dentro de este capítulo, definiciones tales como: medios de pagos, todo lo que concierne al pago electrónico, código QR, operaciones online y otra serie de enumeraciones.

Los nuevos tipos penales creados por el proyecto, en realidad no tienen autonomía como bien jurídico diferenciado, sino que se integran a los títulos existentes en el Código Penal. En otras palabras, los ciberdelitos no crean un nuevo título donde queden consagrados en esta modalidad delictual, sino que se integran en forma precisa y acertada a los bienes jurídicos con los que se los relaciona, o de acuerdo con el bien jurídico que se pretende tutelar.

A nivel de **derecho comparado**, Argentina ratifico Budapest en 2017 y además tiene una ley referida que es la 26.388, por otra parte, Brasil, no ratifico Budapest, pero el instrumento inspiro la aprobación de la ley 12.737 de 2012 y la tipificación de delitos informáticos, a su vez Paraguay ratifico Budapest, pero anteriormente ya había regulado la tipificación sobre sabotaje.

Ciberdelitos enfoque crítico

El crecimiento de casos y de nuevas modalidades de ciberdelito ponen en tela de juicio la eficacia de los operadores del sistema de justicia y la capacidad del código penal vigente para imputar las nuevas conductas delictivas. A su vez, también se plantean cuestionamientos sobre la responsabilidad del sistema bancario, sus límites, y las obligaciones de los usuarios sobre sus datos, desafiando por completo a los Estados modernos, donde casi la totalidad de las operaciones económicas o transacciones son de realización digital. La era tecnológica actual obliga a mantener nuestra vida reflejada en el ámbito electrónico, he ahí la importancia que tiene regular los aspectos concernientes a la ciberseguridad.

La Fiscalía y el Ministerio del Interior enfrentan una gama bastante amplia de delitos realizadas a través de equipos informáticos o redes de internet; una de las estafas más comunes es la simulación de venta de un producto que no se entrega por medio de perfiles falsos en redes sociales. En los últimos meses se han complejizado y sofisticado las maniobras de estafa por intermedio de dispositivos tecnológicos, ejemplo de ello es una modalidad reciente que afectó a decenas de usuarios de bancos cuyas cuentas fueron hackeadas para comprar criptomonedas.

En opinión del Dr. MARTIN PECOY TAQUE la criminología deberá ser la gran aliada del Derecho Penal al enfrentar la posibilidad de legislar al respecto, pues, para conocer cuál es la realidad estadística de estos delitos previo a legislar, ya que resulta evidente que necesitamos información precisa sobre la ciber victimización, lo cual resultara clave a la hora de tipificar, para que no elaboremos meramente un derecho penal simbólico, pero teniendo en cuenta que la ausencia de nueva normativa específica no necesariamente implica un vacío legal.

Precisamente, tal como afirmara antes, *"No existen muchos estudios criminológicos serios en este sentido, sino datos de agencias que intentan justificar las tendencias del momento, pero cuidándose de no afectar los intereses de las poderosas empresas, las cuales, a su vez, temen denunciar los delitos porque se perjudicaría su buen nombre al conocerse que fueron víctimas* (PECOY, 2021).

Otra modalidad frecuente es la del uso de perfiles falsos de redes sociales simulando ser un conocido de la víctima que se encuentra en el exterior y donde el mismo pide dinero para liberar un supuesto paquete retenido en aduanas. Esa maniobra implica también la falsificación de un perfil de la empresa de encomiendas que pretende liberar el paquete inmovilizado -y desde donde se reclama el pago a la víctima- y un comprobante de transferencia bancaria falso con la supuesta devolución del dinero girado por la víctima. También se ha detectado el hackeo de cuentas bancarias para el pago de Sistema Único de Cobro de Ingresos Vehiculares, lo que se concreta en connivencia con el deudor de la patente de rodados.

Las estafas que no superan los 100.000 dólares no son derivadas a las fiscalías especializadas en Delitos Económicos, por lo que recaen en las departamentales o las de Flagrancia, que deberían contar con condiciones adecuadas para perseguir y detener las maniobras más intrincadas.

Respecto a la persecución, es compleja, muchas veces no se logra determinar quién está detrás de la maniobra ni hay tiempo para dedicarle a esa investigación, la cual también requiere de equipos de personas preparadas en redes, software y equipamientos tecnológicos.

Uno de los puntos que puede cuestionarse es la pena prevista en el delito de estafa informática (que va de seis meses de prisión a cuatro años de penitenciaría) cuando a través de los sistemas informáticos pueden concretarse estafas muy dañosas para la víctima que alcanzan los miles de dólares o cientos de miles de pesos (con la penas previstas para el hurto simple, que van de tres meses a seis años, o una rapiña, que tiene un mínimo de cuatro años) siendo todos delitos contra la propiedad (tal vez es más un tema de dosimetría penal que del delito mismo).

Sin dudas existe la necesidad de especializarse para poder avanzar en la persecución penal de este tipo de delitos. En esta modalidad la fiscalía debería instrumentar una persecución sofisticada para que la misma sea efectiva y puedan brindar garantías en el procedimiento de investigación, poder congelar cuentas en forma inmediata, aplicando una especie de medida cautelar anticipada o preventiva -a los efectos de la investigación- y teniendo en cuenta que es muy difícil poder detectar muchas situaciones donde quien comienza la ejecución mediante actos externos, pueda ser interceptado y localizado con inmediatez; éste es un desafío complejo desde la prevención, persecución y eventual detención.

Las nuevas tipificaciones

Está previsto que la nueva ley (de ser aprobada), incorpore 9 figuras penales nuevas, distintas de acuerdo con el concepto que las define y respectivas al bien jurídico que pretendan proteger. La preparación respecto de la persecución de los delitos informáticos será una gran prueba para la nueva era en la que vivimos.

El uso desmedido y constante de medios tecnológicos, permite abrir una nueva brecha y un nuevo desafío para el derecho penal ante el crecimiento exponencial en el uso de medios electrónicos para guardar datos personales, desarrollar la economía y comunicarse, lo que acrecienta los delitos cometidos por quienes tienen mayor conocimiento sobre el funcionamiento de esos sistemas.

La dogmática penal tiende a ser muy crítica con la expansión penal y con la creación de normas penales. Por su parte, el comisionado parlamentario Juan Miguel Petit advierte sobre el crecimiento de la población carcelaria en un 12% este último año, siendo imprescindible poder conectar y analizar que este aumento puede ser un conflicto mucho más intenso con la creación de 9 figuras nuevas, lo que puede agravar el hacinamiento y la población penitenciaria, generando mucha más dificultad en lo que refiere al índice de rehabilitación. Todo esto acentúa el debate en torno a los derechos humanos, los lineamientos de la política criminal que se llevan adelante y el equilibrio que hay que mantener entre los factores más importantes en materia de seguridad pública, como lo es la prevención del delito, la persecución del delito y detención. Además, esto supone la apuesta de muchas instituciones y organizaciones que colaboran en el proceso de rehabilitación para con la PPL (personas privadas de libertad), para que la misma sea satisfactoria debería caer el índice de reincidencia, deberían existir oportunidades reales afuera de los centros penitenciarios para que las personas puedan apostar por el trabajo digno, y valores fundamentales como la familia, la educación, la dignidad humana, entre otros. Pero la cuestión radica

en poder entender la complejidad que existe en materia de seguridad, para poder llegar a obtener resultados positivos tenemos que comprender que hay que mantener armonía y equilibrio, desde las políticas sociales, el ministerio del interior, el poder judicial, y los lineamientos de política criminal por parte del Estado.

Si bien estas nuevas figuras han sido tomadas y reguladas por varios Estados, deberíamos analizar nuestro contexto interno para poder tener una conclusión justa.

Por otra parte -nuevamente referido al tema en cuestión: CIBERDELITOS- tanto para la fiscalía como para el ministerio del interior es muy importante que los operadores del sistema de justicia estén capacitados para afrontar este cambio. Para perseguir los delitos hay que prepararse y conocer cómo funciona, el modus operandi y también para no terminar incriminando a personas inocentes por desconocimiento, o la falta de procedimientos adecuados, es un aspecto relevante tanto para prevención como para la persecución.

Los nuevos tipos penales

El proyecto plantea la creación de los siguientes delitos, a saber:

Acceso ilícito a datos informáticos, Daños informáticos, Abuso de dispositivos, Estafa informática, Grooming, Acoso telemático, Vulneración de datos, Suplantación de identidad, Terrorismo digital (LEY, 2021).

Este proyecto no regula solo tipos penales, también establece medidas educativas o campaña nacional educativa que mencione ut supra, un registro para ciberdelincuentes, e integra un capítulo sobre prevención de transacciones no consentidas, donde faculta a instituciones de intermediación financiera a no ejecutar ciertas operaciones si detectara que dichas acciones puedan ser fruto de una maniobra delictual.

Cabe mencionar que el delito de **GROOMING** ya está tipificado en Uruguay por la ley 19.580 articulo 94 – el cual incorporo el artículo 277 bis del Código Penal y que transcribo a continuación.

El que, mediante la utilización de tecnologías, de internet, de cualquier sistema informático o cualquier medio de comunicación o tecnología de trasmisión de datos, **contactare** a una persona menor de edad o **ejerza influencia** sobre el mismo, con el propósito de cometer cualquier delito contra su integridad sexual, actos con connotaciones sexuales, obtener material pornográfico u obligarlo a hacer o no hacer algo en contra de su voluntad será castigado con de seis meses de prisión a cuatro años de penitenciaría.

Por otra parte, el delito de **STALKING O ACOSO TELEMATICO** también se encuentra tipificado en Uruguay por la Ley 19.580 en su artículo 92, con la siguiente redacción.

(Divulgación de imágenes o grabaciones con contenido íntimo).

El que **difunda**, **revele exhiba** o **ceda** a terceros imágenes o grabaciones de una persona con contenido íntimo o sexual, sin su autorización, será castigado con una pena de seis meses de prisión a dos años de penitenciaría.

En ningún caso se considerará válida la autorización otorgada por una persona menor de dieciocho años.

Este delito se configura aun cuando el que difunda las imágenes o grabaciones haya participado en ellas. Los administradores de sitios de internet, portales, buscadores o similares que, notificados de la falta de autorización, no den de baja las imágenes de manera inmediata, serán sancionados con la misma pena prevista en este artículo.

Otro aspecto que se podría platear eventualmente-respecto de los artículos mencionados- seria la derogación al menos tacita, en caso aprobarse el proyecto de ley sobre delitos informáticos, entendiendo que la nueva ley integra en dos de sus tipos penales, los mismos delitos ya consagrados en la ley 19.580.

Por otra parte, existen otras figuras, por ejemplo, el espionaje informático empresarial o la denegación de servicio de nombres de dominio (que no son consideradas en el proyecto como sí lo han sido a nivel de derecho comparado). Las distintas clasificaciones podemos encontrarlas en instrumentos internacionales como el suscrito por la Unión Europea que ha sido ratificada por 65 países y la **Convención de Cibercriminalidad de Budapest instrumento de referencia en la materia**, **Uruguay aun no ratifico este instrumento tan valioso para la protección de delitos informáticos.**

Budapest presenta una clasificación de criminalidad informática ordenada conforme al bien jurídico protegido:

Conductas que afectan datos y sistemas informáticos:

Acceso e Interceptación ilícitos (Hacking)

Daño de datos o sistemas (Sabotaje)

Conductas que afectan la autenticidad:

Falsificación de documento electrónico

Estafa informática

Conductas relativas a pornografía infantil:

Producción, ofrecimiento, difusión, búsqueda y posesión de pornografía infantil.

Conductas relativas a propiedad intelectual:

Reproducción ilícita de obras

Reproducción ilícita de fonogramas y videogramas.

También podemos encontrar clasificaciones en la doctrina comparada, como la siguiente (formulada conforme a la finalidad de la acción):

Informática como objeto del delito:

Sabotaje

Piratería

Hacking

Informática como medio del delito:

Falsificación de documento electrónico, cajeros automáticos y tarjetas de crédito

Robo de identidad

Fraudes electrónicos

Pornografía infantil.

Informática como ocasión del delito:

Venta de software violando propiedad incorporal.

Información como valor económico de la empresa:

Espionaje informático empresarial

Sabotaje informático empresarial. (BUDAPEST, 2001).

Conclusión

En definitiva, en mi opinión es importante contar con una regulación, con una ley que tipifique estas conductas que hoy no pueden ser perseguidas, de acuerdo al principio de legalidad, no hay crimen ni pena sin ley,

"nullum crimen, nulla poena sine lege", específicamente hoy en día en Uruguay contamos con un departamento de delitos informáticos del ministerio del interior, pero que no cuenta con respaldo jurídico suficiente para lo que concierne a la persecución, este departamento tiene como finalidad la investigación, lucha contra el crimen organizado y delitos a través de internet, pero básicamente hoy en día sin el marco jurídico adecuado se dedica a perseguir e investigar algunos tipos de estafa que se dan mediante maniobras a través de información digital. Si bien **"aequitas praefertur rigori"** es decir, es preferible la equidad que el rigor, en nuestro país necesitamos un marco jurídico para proteger a los ciudadanos, empresas, agencias, instituciones, organizaciones, ya al país de los ciberataques.

Sin perjuicio de ello, como mencione ut supra, la dogmática penal tiende a ser contraria a la expansión y creación de leyes penales, pero el Mundo esta cambiando y debemos adecuarnos a las nuevas formas delictuales, tenemos un instrumento internacional (BUDAPEST) que en 2001 fue aprobado, es decir que el mundo estaba pensado ya en esos tiempos en combatir y en prepararse para luchar contra el cibercrimen.

Referencias bibliográficas

BUDAPEST, C. D. (2001). *Convenio sobre cibercrimen.* Budapest: Consejo de Europa.

LEY, P. D. (2021). *Ciberdelitos.* Montevideo: Parlamento.

PECOY, M. (2021). *Proyecto de ley uruguayo.* Montevideo: La Ley.