Universidad de San Andrés

Departamento de Derecho

Abogacía

El derecho fundamental a la protección de datos personales en Argentina y en el mundo: Los conflictos extraterritoriales por los delitos informáticos

Autor: Estanislao Fuentes Benítez

Legajo: 29063

Mentor: Pablo A. Palazzi

Victoria, Buenos Aires

28 de julio de 2022

Abstract

Las delimitaciones jurisdiccionales se crearon cuando no existía una globalización ni tecnologías como las actuales. El presente trabajo estudia cómo la característica global del internet, en específico los delitos de robo de datos, han incidido en la jurisdicción de los países.

Este impacto ha generado un cambio de paradigma, en el que buscaremos entender como Estados Unidos, la Unión Europea y Argentina han intentado responder y resolver a los conflictos de robo de datos con jurisdicción incierta. Para ello, estudiamos normativas internas, tratados internacionales, jurisprudencia y doctrina de cada uno de los enfoques.

Entendemos que la mejor forma de resolver los conflictos jurisdiccionales es mediante mayor integración y colaboración internacional, para así poder hacer frente a la velocidad y transnacionalidad del internet.

Jurisdictional delimitations were created when there was no globalization or technologies like the current ones. This paper studies how the global characteristics of the Internet, specifically the crimes of data theft, have affected the jurisdiction of the countries.

This impact has generated a paradigm shift, in which we will seek to understand how the United States, the European Union and Argentina have tried to respond and resolve data theft conflicts with uncertain jurisdiction. To do this, we study internal regulations, international treaties, jurisprudence and doctrine of each of the approaches.

We understand that the best way to resolve jurisdictional conflicts is through greater integration and international collaboration, in order to deal with the speed and transnational nature of the Internet.

Contenido

Introducción

El servicio de internet abarca y comprende a todo el planeta. Por este motivo, las leyes, los tratados y las sentencias judiciales suelen tener efectos extraterritoriales. (ISOC, 2018)

Debido al amplio espectro de los delitos informáticos, estos pueden afectar prácticamente a todos los usuarios de tecnología, ya sean a individuos, corporaciones o entidades gubernamentales. Por este motivo, cuando sufren este perjuicio, las personas no saben qué agencia contactar para resolver su problema. (Holt et al., 2017)

La sociedad en general y los individuos en particular estamos tan inmersos en la tecnología que tenemos todos nuestros datos, realizamos todas nuestras transacciones y todos nuestros intereses por plataformas tecnológicas como celulares, computadoras o televisores. Por este motivo, nuestra información personal puede ser vulnerable y que tengan acceso a dichos datos de forma rápida y sencilla.

La protección de los datos es fundamental ya que puede poner en peligro infinidad de derechos, tales como: el consentimiento, datos personales, derecho a la intimidad, derecho a la privacidad, derecho a la imagen, derecho al honor, entre otros.

Uno de los principales problemas de los delitos informáticos es la extraterritorialidad. Puede, y generalmente sucede, que el crimen se produzca en su totalidad en un país, donde tanto el autor del delito como la víctima se encuentran dentro de la misma jurisdicción. Empero, los casos más difíciles de resolver en la actualidad son los delitos informáticos en los que el autor del delito y la víctima se encuentran en distintos países y diferentes jurisdicciones.

El internet ha generado una crisis de identidad que amenaza con el principio de territorialidad. El concepto de soberanía nacional de los Estados fue ideado para un mundo de fronteras físicas, que difícilmente se aplicaba a la realidad que hoy en día se presenta con las nuevas conexiones que no pueden ser eliminadas por los límites físicos.

Con el acceso a Internet, mientras que el tipo penal se consuma en un país sus efectos ocurren en otros a miles de kilómetros a distancia. se realizan los delitos penales, El conflicto que se genera es que no queda claro bajo cuál jurisdicción se debe resolver la disputa. No hay certeza sobre bajo qué país, qué leyes y qué juzgado debe conducirse el proceso penal por el delito

realizado: el país en el que el autor cometió el crimen, el lugar donde se encontraba la víctima o donde estaban ubicados los bienes en los delitos a la propiedad.

Un gran problema es que las víctimas no denuncian los ciberdelitos que afectan muchas jurisdicciones simultáneamente, por lo que es muy difícil conocer hasta qué punto tiene alcance este problema. (Parada & Errecaborde, 2018)

Gracias a los avances que han habido con respecto a la tecnología, muchos países han logrado desarrollarse y expandirse comunicacionalmente, permitiendo intercambiar información de forma más eficiente. En las últimas dos décadas, Internet se ha adaptado e implementado en la vida de millones de personas. Esta aplicación trajo aparejada innumerables beneficios socioeconómicos, pero este avance trajo aparejado, naturalmente, el crecimiento de los ciberdelitos. (Chawki et al., 2015)

El avance de las nuevas tecnologías venía dándose en forma progresiva desde su comienzo. El uso de la tecnología en nuestras vidas fue avanzando año a año. Sin embargo, a raíz de la pandemia, millones de personas debieron quedarse en sus hogares y realizar trabajo o actividades ociosas en forma remota haciendo uso de computadoras. De este modo, el uso de las tecnologías para todo tipo de actividad se ha visto incrementado en forma exponencial en los últimos 3 años. Parece ser que la implementación online ha sido una modalidad que se ha instaurado por más que parezca que hemos vuelto a la “normalidad”.

De acuerdo a un informe de Estadística, en 2020 el número de compradores online de todo el mundo era de 1.240.000.000, mientras que en 2021 aumentó a 2.140.000.000. Esto significa que en 2020 las compras online han pasado de ser el 16.06% al 27.64% en 2021 de la población mundial. Este mismo informe expone que se espera que hasta el 95% de las ventas se realicen a través del comercio electrónico para 2040. (Carter, 2022)

En EE. UU., las ventas de comercio electrónico aumentaron un 44% entre 2019 y 2020. (Carter, 2022). Mientras que en el mismo país, entre 2006 y 2007 las ventas en el comercio electrónico aumentaron un 18,4%. (Wang, 2010)

En la UE, el número de usuarios de Internet aumentó un 218,1 % entre 2000 y culminó en un total que representa el 61,4 % de la población total de la UE y el 18,8 % del uso mundial. El porcentaje de personas que habían comprado bienes o servicios a través de Internet para uso

privado aumentó significativamente: del 22 % al 34 % entre 2004 y 2008. (Banco Mundial, 2021)

De acuerdo con un informe que realizó la Cámara Argentina de Comercio Electrónico (CACE) junto a la consultora Kantar, en 2020 hubo casi 1,3 millones de personas que empezaron a comprar a través de internet, un 6% en comparación a 2019. De esa forma, las ventas por canales online crecieron un 124% respecto al año anterior. (Cámara Argentina de Comercio Electrónico & Kantar, 2021)

Por otra parte, la Cámara Argentina de Comercio Electrónico entiende que el crecimiento del comercio electrónico en el país aumentó en un 68% del 2020 al 2021. (Estadísticas De Comercio Electrónico, 2022)

Esto nos demuestra que es imprescindible tener en consideración que cada vez más nuestras vidas dependen de las tecnologías digitales y cada vez más tendremos más información que podrá ser vulnerada por terceros. Por eso, es menester analizar y estudiar cual es la mejor forma de entender y tratar los robos de datos informáticos.

De acuerdo a Matilde S. Martínez, 2018 se pueden clasificar las conductas antijurídicas o los delitos informáticos de acuerdo al bien jurídico protegido en los siguientes grupos:

a) Por redes sociales que atentan a la intimidad, el honor, integridad moral y otras formas; b) delitos de stalking como persecución, acecho o acoso contra una persona que pueden llevarse a cabo a través de internet u otros medios; c) Delitos sexuales contra menores (online grooming), ataques por medios tecnológicos; d) ciberpornografía infantil, sitios web para tráfico de material pornográfico; e) ciberodio que comprende la xenofobia, el racismo, el odio y la discriminación; f) delitos contra la propiedad intelectual; g) estafas y fraudes como aquellas conductas que atentan contra el patrimonio de terceras personas.

A los fines de este trabajo, nos enfocaremos en este último punto: las estafas y los fraudes como aquellas conductas que atentan contra el patrimonio de terceras personas. De acuerdo a un estudio realizado por la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC), la escala de los delitos cibernéticos más importantes (los más reportados) han sido: el fraude con 24%, luego el phishing con 17% y en tercer lugar el cyberbullying con 16%. El resto de la tabla

la ocupan calumnias (14), extorsión online (12), amenazas (6), publicación ilegítima de imágenes (2), material sexual infantil (1), entre otros. (AALCC, 2021)

De acuerdo a datos recopilados por la AALCC, en el país, el total de delitos cibernéticos aumentó de 400 en 2016 a casi 1600 en 2020, es decir que aumentó un 400% en 4 años. De esta forma, el robo de datos específicamente, pasó de haber 25 casos reportados en 2016 a 264 en 2020.

El robo de datos es uno de los delitos más destacados debido a que son los realizados para obtener beneficios económicos. Estos se deben obtener por medio de phishing que puede ser utilizado para el fraude, la extorsión o su venta en el mercado negro opera otras actividades. Por esta misma razón, el robo de datos será uno de los delitos que más crecerá en el futuro por la múltiple utilidad en el espectro criminal. (AALCC, 2021)

El FBI estima que hasta enero de 2022 el grupo más importante de robo de datos -un grupo ruso llamado Conti- ha extorsionado a más de 1.000 víctimas que han pagado más de US$150 millones en rescates, lo que convierte a este grupo en el más dañino jamás documentado. De este modo se evidencia la incapacidad por parte de los Estados a nivel internacional para solucionar las extorsiones y el robo de datos, debido que como no se puede contar con ningún país para solucionar el conflicto, resulta más conveniente pagar por los rescates. (Chaves, 2022)

Entre febrero y marzo de 2020, un socio del sector privado detectó y comunicó a INTERPOL que los registros maliciosos ─malware y phishing incluidos─ habían aumentado un 569 %, mientras que los registros de alto riesgo habían subido un 788 %. (INTERPOL, 2020)

Es importante remarcar, que los diferentes “países” que estudiamos tienen diferentes formas de encarar esta problemática. Por un lado, Estados Unidos es el único de los principales países que no tiene un conjunto unificado de leyes sobre privacidad de datos. Por otro lado, La Unión Europea tiene, a grandes rasgos, una legislación muy fuerte y avanzada en esta materia y le da principal importancia a la forma en que las empresas almacenan y trasladan los datos. Argentina, sin embargo, tiene una legislación menos avanzada que la europea, pero más fuerte que la de Estados Unidos ya que cuenta con una ley de protección de datos personales.

Como mostramos, es crucial entender en profundidad el inmenso rol que está teniendo el internet en nuestras vidas. El crecimiento del uso de plataformas digitales para compra, ocio y trabajo está en tendencia alcista y lo más probable es que siga siendo parte de nuestras vidas cada vez más. Naturalmente, el mismo fenómeno ocurre con el robo de datos y con el phishing. Dado que cada vez existen más delitos en estas plataformas, es imprescindible entender cómo es la mejor forma de tratar esta problemática para que menos personas se vean perjudicadas.

Pregunta

¿Cómo se resuelven los conflictos de jurisdicción respecto a los delitos informáticos de robo de datos y phishing cuando intervienen agencias en más de un país, tomando los casos de USA, EU y Argentina?

Objetivo

Este trabajo se enfocará en una de las cuestiones más debatidas en el derecho de la tecnología y la privacidad de datos personales: la extraterritorialidad. Se pondrá de manifiesto la necesidad de esclarecer los conflictos de privacidad de datos personales, en especial, la vulneración de información personal utilizada sin consentimiento y con fines maliciosos.

En esta tesis, nos enfocaremos en estudiar, analizar y determinar cuál es la jurisdicción de los delitos informáticos internacionales como robo de datos, fraude y phishing. En los casos en que las partes y el objeto del conflicto radican en diferentes países.

Se argumentará la dificultad o facilidad de las normas del derecho en casos internacionales para adecuarse a los delitos. Se intentará determinar cómo, bajo qué jurisdicción y normativa deben resolverse los casos en los que se comienza a realizar un crimen en un país y se consuma en tiempo real en otro por medio de herramientas como internet.

Metodología

En este trabajo se estudiará cómo está legislado, regulado y cómo se han resuelto conflictos judiciales relacionados a la privacidad de datos personales y protección de datos en la República Argentina, en particular los conflictos emanados de la extraterritorialidad. Se

realizará una comparación con otros países que han abordado esta temática con mayor profundidad y se analizará cuál es la mejor forma de solucionar estos conflictos.

A los fines de cumplir con el objetivo señalado, la metodología que emplearé será la siguiente:

-Descripción y explicación de la problemática por la utilización de datos personales en extraterritorialidad.

-Análisis normativo y doctrinal en materia de protección de datos personales. Cómo cada país protege la información de sus habitantes y qué jurisdicción asignan a los delitos cometidos fuera de su territorio y, del mismo modo, los crímenes cometidos dentro de su territorio con daños en otros países. Se tomará Argentina, como eje central, y se estudiarán Estados Unidos, y la Unión Europea por su desarrollo e importancia social, económica y tecnológica en el ámbito internacional.

Conceptos

Nos referiremos al término “Jurisdicción”, limitándola al área geográfica en el que los tribunales de un determinado país aplican las leyes, teniendo en consecuencia facultad legal para entender y juzgar diversas situaciones que se someten a su resolución. En este trabajo existirán conflictos de jurisdicción cuando dos o más Estados entiendan que pueden intervenir en la cuestión planteada con exclusividad.

Como al poder del Estado de juzgar o de ejercer la función judicial, la competencia es la medida en que ese poder del Estado le es dado a un tribunal determinado. La competencia delimita la zona del conocimiento, intervención, decisión y ejecución del juez o tribunal, determinando el espacio, materia y grado de los asuntos que le incumben. La competencia es improrrogable por simple voluntad de los sujetos de un procedimiento. Además, es inalterable, ya que el único parámetro para atribuir competencia a un tribunal es la ley y, por tanto, deviene en absoluta. (Darahuge & González, 2018)

Así, diremos que existe un “conflicto de jurisdicción internacional” cuando las partes intervinientes en el proceso son de diferentes nacionalidades o residen en distintos países, o bien cuando el objeto o la lesión a un derecho motivo de disputa se encuentra o se produce en diferentes países. En estas situaciones, puede ocurrir que más de un tribunal pretenda tener

jurisdicción sobre el mismo caso. Por lo tanto, se deben aplicar ciertas reglas de jurisdicción internacional y del derecho internacional para determinar el tribunal de qué país es el competente para fallar en la disputa determinada.

La ley de Protección de Datos Personales Argentina define en su artículo 2 a los “datos personales” como la información de cualquier tipo referida a personas físicas o de existencia ideal, determinadas o determinable, a los archivos o bases o bancos de datos que posean el conjunto organizado de datos personales pudiendo ser objeto de tratamiento o procesamiento electrónico o no, sin importar la modalidad de su formación, almacenamiento, organización o acceso. También se entiende como” Titular de los Datos” a toda persona física o persona de existencia ideal con domicilio real o legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.

De acuerdo a las definiciones aportadas por el convenio de Budapest, se entiende por “Sistema Informático” a todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, o bien de algunos de sus elementos, que posea el tratamiento automatizado de datos en función de un programa.

De la misma manera, se entiende como “Dato Informático” toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. Por el contrario, se entiende por “Datos de Tráfico” a los relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Por último, por “Proveedor de Servicios” se entiende a toda entidad pública o privada que ofrece a los usuarios la posibilidad de comunicarse a través de un sistema informático, así como a cualquier otro ente que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo. (Consejo de Europa, 2001)

De acuerdo a Fernández Delpech, 2014, explica que el “Derecho Informático” es el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. Entiende que la informática es una ciencia que estudia métodos,

procesos y técnicas, con el fin de almacenar, procesar y transmitir informaciones y datos en formato digital.

Por “Delito Informático” existen distintas definiciones, ya que se trata de una etapa primitiva en la que la doctrina no ha acordado definirlos de forma unánime. Por un lado, el Profesor mexicano Julio Téllez Valdés desde un ángulo de vista atípico dice que son "actitudes ilícitas en que se tiene al computador como instrumento o fin", y desde un ángulo típico son "conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como medio o fin". Del mismo modo, Nina Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas". (Roca de Estrada, 2001)

Por otro lado, Microsoft sostiene que el phishing es de los delitos cibernéticos más populares y lo entiende como el ataque que intenta robar dinero o identidad, haciendo que el usuario divulgue información personal (como números de tarjeta de crédito, información bancaria o contraseñas) en sitios web que fingen ser sitios legítimos. Los ciberdelincuentes suelen fingir ser empresas prestigiosas, amigos o conocidos en un mensaje falso, que contiene un vínculo a un sitio web de phishing. (Microsoft, 2022)

Se considera “ciberdelito o delito informático” a cualquier actividad ilícita, que involucra a una computadora como la máquina o instrumento que puede ser programada- y que posibilita realizar delitos dentro del ámbito propio de la tecnología. Una definición generalizada del ciberdelito podría ser que trata de aquellos actos ilícitos en los que una computadora es la herramienta, el objetivo o ambas de los mismos.-.

El “delito informático” abarca un sinnúmero de conductas que conforman un amplio abanico de tipos penales. Así puede versar sobre delitos realizados para obtener los datos y/o sistemas informáticos de terceros (hurto de información), o de falsificación y fraude relacionados o por medio de la informática (phishing), puede tratarse también de delitos que lesionen la intimidad, por ejemplo, de corte sexual l (difusión de fotos íntimas o pornografía) o bien afectar l derechos de autor (piratería) entre otros. En la medida que aparecen nuevas tecnologías o nuevos usos de las mismas, aparecen nuevas acciones tendientes a vulnerarlas y/o lesionar derechos que resguardan o datos que contienen, consecuentemente los tipos penales deben estar en constante aumento.

Para algunos el término Phishing proviene del acrónimo de password harvesting fishing (cosecha y pesca de contraseñas). El fenómeno phishing consiste, en general, en el envío de un correo electrónico de aparente similitud con aquellos emitidos por instituciones realmente existente e induciendo así a completar en un sitio web no auténtico datos personales, credenciales de autenticación, números de tarjetas y toda otra información de utilidad para operar en internet. Con esos datos, el agresor accede a servicios en línea y realiza transacciones bancarias y comerciales de variada índole realizando un perjuicio patrimonial. (Petrone et al., 2021)

Brecha internacional digital

Sabemos, que al igual que como sucede con los desarrollos económicos, científicos, educativos, etc, el desarrollo de la tecnología informática y digital tampoco se da ni se ha dado de forma uniforme y simultánea.

Algunos países han comenzado antes con este desarrollo, otros han tenido y tienen políticas que fomentan y alientan este tipo de desarrollo que producen cambios muy rápidamente. Todo esto ha ocasionado que se produzca una brecha digital internacional.

Por este crecimiento desigual, muchos países pobres consideran a la regulación de la tecnología como una forma de desarrollarse y equiparar a los que le llevan ventaja.

Los países más poderosos y desarrollados imponen su voluntad y regulación a otros menos desarrollados, lo que a su vez genera resentimiento y tensión. Cuando un Estado impone su hegemonía mediante legislación nacional en forma agresiva a nivel global es natural que otros países actúen en consecuencia. Pueden negarse a actuar en conjunto o firmar tratados comunes, establecer normativas contrarias a esos países, o también querer imponer su soberanía y no aceptar otras jurisdicciones.

La extraterritorialidad disminuye la colaboración internacional, lo cual resulta contraproducente para marcos y normativas internacionales. La extraterritorialidad crea un rompecabezas de distintas normativas incongruentes entre sí, dado que cada país tiene su propia legislación que puede ser contraria a otros países. Esto, en definitiva, se ve reflejado en una mayor dificultad a la hora de resolver conflictos donde se ven involucrados más de un Estado. (ISOC, 2018)

Diferencia con los delitos tradicionales

Los delitos informáticos, especialmente los delitos que nos enfocamos: fraude, robo de datos o phishing, presentan ciertas diferencias con los delitos del tipo tradicionales. Existen distintas corrientes. Una mayoritaria sostiene que los nuevos delitos se deben adaptar al derecho fundamental y a los delitos tipificados tradicionalmente ya que son los mismos establecidos en todos los países y que únicamente se modifica el medio de comisión del mismo.

Otra corriente sostiene que es necesario un tratamiento procesal y legislativo que lo caracterice y lo diferencie de los demás tipos de delitos. De no ser así, la situación puede producir una verdadera impunidad por no articular con los remedios adecuados. (Díaz Gómez, 2010)

Estas características que lo diferencian son: que los delitos se comenten a distancia, y sin posibilidad de recibir una reacción por parte de la víctima; puede que se cometan de forma instantánea o en un lapso de tiempo –diferencia del tiempo; puede que los delitos afectan a muchas víctimas a la vez e incluso, como habitualmente sucede, que sean desconocidas para el perpetrador. (Díaz Gómez, 2010)

La teoría general del delito se suele aplicar para los casos del ciberdelito, ya que fue ideada para que se pueda aplicar a cualquier tipología en general. Una parte importante de la doctrina sostiene que la naturaleza de la ciberdelincuencia es similar a los delitos tradicionales, ya que son de naturaleza simple: se pueden realizar con poca habilidad y tienen consecuencias a largo plazo. Por eso, para muchos, las personas que cometen delitos cibernéticos deben ser juzgados igual que las personas que hurtan, estafan, roban, golpean, venden drogas y demás. Porque se trata de niveles inadecuados de autocontrol. (Holt et al., 2017)

Además, suelen ser delitos cometidos internacionalmente que afectan a personas ubicadas en zonas geográficas apartadas. Estos atacan a múltiples bienes jurídicos protegidos en un único delito, como la seguridad, la intimidad, la dignidad o el patrimonio. (Arocha Vinagre & Alicia, 2017)

Algunos doctrinarios en argentina entienden que los delitos informáticos no deben ser una nueva categoría, sino que simplemente son los mismos delitos de siempre pero que se realizan a través de nuevos medios. Este sector entiende que los bienes jurídicos protegidos son los

mismos de siempre, nada más se actualizaron los tipos penales, que incluyen, como mencionamos anteriormente, nuevos medios para cometerlos. Un ejemplo de esta actualización podría ser el caso de las modificaciones de los artículos 153 y 153 bis del Código Penal, explicados posteriormente.

Por otro lado, se ubica la postura que entiende que debe haber un nuevo bien jurídico que proteger, que es la información. Esta tiene un valor que debe ser puesto en el plano penal independiente a los otros bienes jurídicos. De acuerdo a Acurio del Pino, 2016, podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona por su fluidez y tráfico jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Finalmente, creemos que de no existir normas penales que logren evitar los delitos informáticos, estos delitos pueden quedar impunes. Puede suceder que los jueces no sepan cómo resolver los casos, como determinar jurisdicción o no tengan claro de qué modo afecta a la víctima. Por este motivo, los Estados buscan la forma para poder determinar su jurisdicción con carácter extensivo, de forma tal que pueda involucrar a más de un ordenamiento.

Comisión del delito

La evolución de la tecnología ha afectado a toda la práctica y ejercicio del derecho. Por este motivo es que existen diversas formas de determinar la competencia territorial:

Una de las formas es la que ha establecido el Tribunal Supremo Español el 23 de noviembre de 2004 (Arocha Vinagre & Alicia, 2017), en el que explica cuándo y en qué casos tiene jurisdicción un país con la teoría de la actividad, la teoría del resultado y la teoría de la ubicuidad.

Por otro lado, Darahuge y González explican en “Empleo de las direcciones Virtuales como elemento fundante en las declaraciones de incompetencia por territorialidad” pp 183 de cibercrimen del de 2018 (Darahuge & González, 2018) que existen tres nuevas versiones de lugar del hecho: El lugar del hecho real (LHR), el lugar del hecho virtual impropio (LHVI) y el

lugar del hecho virtual propio (LHVP). Es necesario explicar qué significa cada una de las categorías.

Teoría de la actividad

Se entiende que habla de la jurisdicción en la teoría de actividad cuando el delito es cometido en el lugar desde donde se realiza la conducta. Lugar en el que el presunto autor concreta los hechos que se denuncian.

Sin embargo, esta teoría no es del todo satisfactoria ya que puede suceder que el servidor en el cual se realiza el acto delictivo se encuentre en otro lugar. Por ello, muchos creen que es más viable atribuir la jurisdicción al órgano donde se encuentra el sistema informático desde el cual fue elaborado el material motivo del delito.

Esta teoría es útil porque resulta más sencillo atribuir competencia a un tribunal cuando se presentan víctimas en distintas jurisdicciones. Resulta más eficiente atribuir competencia al tribunal del lugar donde se encontraba el equipo utilizado para cometer el delito, ubicado por medio de su dirección IP, o la localización del autor de los hechos cuando cometió el delito.

Teoría del resultado

Esta teoría - propuesta por el Tribunal Supremo español a través de Auto del 28 de octubre de 2010 (Arocha Vinagre & Alicia, 2017) - propone que en los delitos contra el patrimonio y con víctimas en numerosos países, se aplique la jurisdicción donde se ha producido el perjuicio económico o la lesión en el sujeto pasivo a través del desplazamiento patrimonial que corresponde con el lugar en el que se encuentra la cuenta dónde se sustrajo el dinero.

Este es un criterio muy útil ya que resulta fácil determinar la jurisdicción dado que el sujeto afectado habrá obtenido un perjuicio en su cuenta corriente. El será quien interpondrá una denuncia o querella ante el Juzgado competente más cercano a él. Esta teoría resulta muy eficaz en los casos que los ilícitos tengan repercusión en múltiples países. Sin embargo, si no existen convenios o tratados internacionales, puede que sea muy dificultoso obtener poder de policía frente al presunto criminal y de esa forma sancionarlo.

Teoría de la ubicuidad

La teoría de la ubicuidad es un término medio entre la teoría de actividad y del resultado. El lugar de comisión del delito se entiende desde quien realizó la acción hasta donde la misma que se produjo.

Entonces, se entiende competente aquel órgano judicial en el que se hubieran iniciado acciones por hechos considerados delitos. Se entiende que el Juez que primero haya realizado las actuaciones procesales, será el primero para tener instrucción en la causa.

Lugar del Hecho Real

Se entiende por Lugar del Hecho Real al área definida y determinada en espacio y tiempo donde ocurre un evento o una serie de ellos. Esta categoría es la más estudiada, múltiples teóricos entienden la competencia a partir de la ubicación geográfica, entendiendo la resolución de problemas basado en el territorio.

Lugar del hecho virtual impropio

Todos los dispositivos informáticos están asociados a una placa de comunicaciones con una dirección física única que se la identifica a dicha placa. Este conjunto de números se denomina como dirección Media Access Control (MAC), propio de cada dispositivo y cada uno se asocia con una dirección IP.

Esa información siempre se encuentra en un dispositivo determinado. De esta forma, si se logra determinar la dirección IP de origen o de destino de una transacción digital, dependiendo de que sea necesario, se puede lograr establecer el lugar de ocurrencia de un evento virtual, que puede resolver el problema de competencia judicial.

Con la dirección IP se asocia un determinado dispositivo móvil y permite determinar el dispositivo y el lugar de ubicación. El problema surge cuando no se puede establecer con precisión dónde se encontraba el dispositivo cuando ocurrió el ilícito. Este conflicto se debe solventar con otras pruebas complementarias para establecer el lugar, como pueden ser la geolocalización, testimonios, pruebas de informes, inspecciones judiciales o cualquier medio que ayude a dilucidar la ubicación del dispositivo en ese momento.

Este método explicado, no soluciona la problemática general de competencia, ya que depende de las jurisdicciones posibles determinar por qué una tiene competencia sobre la otra. Puede ser por lugar de ocurrencia, por el lugar donde se lo ejecutó, por la nacionalidad del delincuente o de la víctima.

Una vez que podemos dilucidar y determinar mediante los medios descritos anteriormente el lugar hecho virtual impropio, es cuando el lugar del hecho real es revelado. Así que finalmente, no existen problemas de competencia debido que la misma está determinada específicamente por el lugar del hecho real, en el cual solo se realiza una reconstrucción en el lugar del hecho virtual impropio.

Lugar del hecho virtual propio

El Lugar del Hecho Virtual propio es en el que se intenta enfocar esta tesis. Se refiere a los casos en los que las acciones ocurren completamente en entornos virtuales con muchas jurisdicciones diferentes. Un ejemplo sería un falsario argentino que, por medio remotos, dispone de una granja de servidores en Estados Unidos para descubrir una clave de acceso a una cuenta bancaria en Europa y así transferir esos fondos de nuevo hacia algún país de Sudamérica con el objetivo de obtener un beneficio económico.

La figura que se puede utilizar para reconocer al delincuente y realizar una inspección judicial virtual, local o remota, no se encuentra específicamente descrita, ni detallada en la codificación procesal vigente en Argentina. De esta forma, es que los delitos informáticos propios resultan muy difíciles de probar porque no se pueden encuadrar en las figuras procesales vigentes.

Puede ocurrir que, debido al conflicto de competencia, existan diferentes elementos probatorios del delito en distintos países y la comisión del delito no esté perfectamente definida o no coincidan en la definición. De esta forma, pueden surgir distintas situaciones suponiendo que ya está establecida la competencia del tribunal nacional. Si no está clara la competencia del tribunal porque se excusan o son recusados, el problema es de difícil solución.

Las formas habituales de solucionarlos son por dos medios:

1) a) Existen convenios bilaterales de asistencia judicial o policial recíproca como es el caso de Argentina-Uruguay. b) Países en los cuales existen tratados

multilaterales de similar índole como es el caso de Argentina-Paraguay y su relación con el Mercosur. Estos convenios son más restrictivos y limitados que el del punto (a). c) elementos probatorios obrantes en un país donde no existe ningún vínculo de asistencia judicial/ policial de ningún tipo, como es el caso de Argentina con Irak. El peor caso implica que no pueda ser posible obtener dato alguno de medios judiciales lícitos.

2) También existen acuerdos de extradición como es el caso del Acuerdo de Extradición entre la Unión Europea y los Estados Unidos de América, 2003. que fue firmado con el fin de establecer mecanismos ante las solicitudes de extradición. Otro ejemplo que comprende la misma categoría es el de la Decisión Marco 2009/948/JAI.

Derecho Federal

Existen muchos problemas de jurisdicción causados por la víctima y el victimario que viven en diferente municipalidad o provincia. La policía local en todos los países parece haber sido desafiada y superada por el ciberdelito. Muchos académicos argumentan que la policía local puede y debe desempeñar un papel más importante en la investigación de los delitos cibernéticos. (Holt et al., 2017)

En los Estados Unidos, muchos departamentos de policía están estableciendo unidades de delitos informáticos investigados por las divisiones. Los delitos cibernéticos constituyen una gran proporción de los delitos investigados por estas divisiones. (Chawki et al., 2015)

Por otro lado, la Unión Europea ha creado un organismo llamado Foro sobre la Ciberdelincuencia, y varios estados europeos han firmado el Tratado del Convenio sobre Ciberdelincuencia del Consejo de Europa, que busca estandarizar las leyes europeas relativas a la ciberdelincuencia. (Consejo de Europa, 2001)

Si una persona es víctima de algún delito cibernético como robo de datos de tarjetas y realiza compras en línea, la jurisdicción es tan limitada para la policía local que implicaría que no pueden actuar cuando son llamados para ejercer su servicio. (Walker & Katz, 2012). En cambio, probablemente sea más efectivo realizar la denuncia en una agencia de policía federal o nacional, e incluso allí, es posible que no encuentren jurisdicción ni puedan resolver

satisfactoriamente a favor de la víctima debido a las dificultades en las investigaciones transnacionales. (Holt et al., 2017)

Poder de policía nacional

No existe problema jurisdiccional únicamente a nivel internacional. También se presenta una importante superposición jurisdiccional a nivel federal, considerando que varios entes estatales son responsables de investigar las mismas categorías de delitos cibernéticos.

En Estados Unidos, por ejemplo, el Servicio Secreto de los Estados Unidos también investiga intrusiones informáticas que afectan a instituciones financieras y delitos económicos. La Oficina de Aduanas y Protección Fronteriza de EE. UU puede desempeñar un papel en las investigaciones de robo intelectual y delitos económicos, mientras que el Servicio de Inmigración y Control de Aduanas también puede involucrarse en el robo intelectual, delitos económicos.

Por este motivo, es que se suscitan superposición de organismos dentro de Estados Unidos y se presentan problemas de competencia cuando llegan a los Tribunales y Cortes. Esto demuestra que incluso los países más desarrollados tienen inconvenientes en aplicar jurisdicción incluso dentro de su propio país.

Los niveles más altos de aplicación de la ley en países como Canadá, Corea del Sur y el Reino Unido son las fuerzas policiales nacionales, que cumplen la misma función que las fuerzas del orden federales en los EE.UU. Sin embargo, al tratarse de un único organismo es más sencillo eliminar las problemáticas de potestad dentro del mismo Estado.

Jurisdicciones internacionales

Las legislaciones nacionales son necesarias para combatir y acabar con los delitos cibernéticos de robo de datos. A pesar de esto, la regulación nacional por sí sola es inviable debido a la expansión transnacional de los ciberdelitos. Por este motivo debe regirse, necesariamente, por el derecho internacional (Smyth, 2007)

Algunos actos en Internet pueden ser legales en un país e ilegales en otros. Por ejemplo, puede ser que un acto en internet sea legal en el país de origen, pero ilegal donde se consuma

aunque la acción no esté dirigida específicamente a ese país. Los conflictos de jurisdicción en ciberdelitos abundan, tanto en los casos en el que ningún país reclama potestad como cuando varios países la reclaman al mismo tiempo.

El problema principal surge ya que no queda claro qué constituye jurisdicción: Si el lugar del acto, el país de residencia del perpetrador, la ubicación del efecto, la nacionalidad autor, o todas juntas. Lo cual significa que el internet ha otorgado a criminales la facultad de actuar sin las delimitaciones de las fronteras. (Chawki et al., 2015)

El actual e inminente aumento en los números del ciberdelito, indican que es necesario una urgente convergencia de la comunidad internacional frente a un conjunto de normas jurídicas sustantivas y procesales. Para de esta forma, expandir la jurisdicción para que los países puedan trabajar en conjunto. (Chawki et al., 2015)

Dado que se trata de un tema reciente, una gran número de países no han enmarcado ni establecido como quieren tratar este tema. Muchos se resisten a unirse a cualquier convención internacional que no hayan negociado desde su creación. Una doctrina mayoritaria cree que se debe facilitar y flexibilizar la adhesión de nuevos integrantes a la comunidad internacional para unir fuerzas contra el delito cibernético y así lograr mejores resultados. (Chawki et al., 2015)

Por otro lado, el Reino Unido y muchos países del Medio Oriente parecen alejarse poco a poco del enfoque de detección y eliminación de contenido ilegal o no deseado para imponer a las plataformas de tecnología una obligación positiva de controlar el contenido existente o incluso evitar que se suba a internet. Y, de esa forma, evitar que se ocasionen delitos antes de que ocurran.(Bischoff, 2022)

Sin embargo, de acuerdo a un artículo de Internet Society, 2018, no hay que perder de vista que la globalización es una ventaja de internet, no una desventaja o un perjuicio. Los países deberían intentar adaptarse a él en lugar de intentar corregir su internacionalidad. Las decisiones del alcance extraterritorial y sus legislaciones deberían estar ideadas para permitir que internet continúe siendo una tecnología abierta, segura, fiable y globalmente conectada con todo el mundo.

Muchos conflictos comienzan cuando se elaboran políticas o se emiten sentencias judiciales con efectos fuera de su jurisdicción que dañan las características únicas y el alcance global del

internet. Creemos que los Estados no deberían impedir la circulación de ideas e información que trae aparejada esta tecnología, especialmente a sus propios ciudadanos. (ISOC, 2018)

Por lo tanto, el cibercrimen, al tratarse de un fenómeno global, no se puede limitar a perseguirse únicamente por medio de los estados nacionales, su lucha requiere estrategias legales y globales conjuntas. La única forma de solucionar este problema es mediante la armonización de leyes nacionales, la cooperación mutua de los países y de los organismos encargados de cumplir la ley para que respondan adecuadamente a métodos sofisticados y ágiles utilizados por ciberdelincuentes (Chawki et al., 2015)

En definitiva, a raíz de los crecientes casos de ciberdelitos a nivel global, es necesario un trabajo en conjunto de la comunidad mundial para establecer una clara legislación internacional. Debido a que es ésta, a nuestro entender, la mejor forma de solucionar la problemática internacional que se genera a raíz de los ciberdelitos.

Derecho Internacional Privado

El derecho internacional privado trata los conflictos entre las leyes nacionales de los países, es la rama del derecho que busca encontrar soluciones a controversias jurídicas internacionales entre personas o entidades de diferentes países o estados. Se ocupa de la resolución de disputas con elementos extranjeros. (Wang, 2010)

Dado el carácter internacional del internet y la tecnología, la normativa global sostiene el principio de que todas las disposiciones deben ser interpretadas conforme al carácter internacional de esta tecnología y no en forma restrictiva implicando solo a un país. (Torello, 2015)

Es necesario que se modernicen leyes del derecho internacional privado para aumentar de esta forma la seguridad jurídica en cada país y la ley aplicable frente a los contratos y a los delitos por internet. El mundo actual requiere que el derecho internacional privado se ocupe de problemas contemporáneos. (Wang, 2010)

En el derecho internacional privado, las normas jurídicas aplicables a situaciones vinculadas con varios ordenamientos jurídicos nacionales se determinan eventualmente por tratados y convenciones internacionales vigentes de aplicación en el caso. En defecto de normas de

fuente internacional, se aplican el derecho internacional privado (El de Argentina en este caso se encuentra regulado en el CCyC) de fuente interna. El análisis de la jurisdicción y competencia en materia de delitos informáticos de robo de datos, deberá ser apreciado por los jueces a la luz de la mencionada normativa. (Torello, 2015)

La jurisdicción extraterritorial puede ser un problema porque las normas y resoluciones judiciales nacionales tienen aplicación fuera del país. Esto puede tener consecuencias negativas y a menudo imprevistas, debido a que países podrían involucrarse en el derecho interno de otros. De este modo, se puede generar incertidumbre jurídica sumamente perjudicial para la seguridad de los usuarios en línea.

Desafíos a la aplicación del derecho internacional

Una vez que se comete un delito cibernético transnacional, puede que uno de los países en los que se cometió tenga jurisdicción para entender con plenitud el caso. Sin embargo, muchas agencias y/o naciones de todo el mundo están limitadas a la normativa existente y a acuerdos de cooperación internacional. Es cierto que muchas naciones desarrolladas han tipificado muchos delitos informáticos y está comenzando a existir cierta paridad en la forma de tratar estos conflictos en los diversos países (Brenner, 2011)

Una de las dificultades que tiene el derecho informático y sus respectivos delitos es su complejidad y su carácter pluriofensivo. Estos delitos se caracterizan porque simultáneamente abarcan muchos intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo. Por ejemplo, un fraude electrónico puede afectar numerosos delitos, como la confidencialidad de la información, la integridad, el patrimonio, y hasta delitos que ataquen el orden económico y financiero (Magliona Markovicth, 1999). Lo cual genera que sea realmente desafiante la tipificación de los delitos informáticos en el plano internacional.

Estados Unidos sigue siendo el país en el que se originan mayor cantidad de delitos cibernéticos, pero de acuerdo a los estudios más recientes de la Internet Crime Complaint Center, las naciones que le siguen son Canadá, India y Filipinas. (Chawki et al., 2015) Sin embargo, puede que existan muchos delitos originados en otros países que no sean reportados como los que tienen sede en Rusia.

Algunos conflictos de jurisdicción de delitos informáticos se ven agravados por las tensiones internacionales entre Estados Unidos, China, Rusia y Ucrania, entre otros. Los ciberdelincuentes aprovechan y ven atractiva esta poca colaboración bilateral para cometer delitos desde un país para con el otro (Brenner, 2008). Siguiendo con este orden de ideas, los fiscales pueden no tomar el caso si los sospechosos residen en alguna de las naciones mencionadas anteriormente, ya que haría prácticamente imposible el arresto (Holt & Bossler, 2017). Por este motivo, el sistema de resolución de estos conflictos se ha vuelto dependiente de las relaciones internacionales entre naciones amigas y enemigas, y la opción de poder detener a ciberdelincuentes depende de las relaciones entre países. (Holt & Bossler, 2017)

Los diversos países se comportan de forma diferente a la hora de resolver delitos informáticos, lo cual ha generado una fragmentación internacional. De modo que la resolución de los conflictos internacionales de este tipo, se está tornando compleja.

Por tanto, debido a la incertidumbre jurídica, muchas empresas deciden no invertir ni desarrollarse en esos países. De este modo, antes de que incluso se cometa el delito, los usuarios se pueden ver afectados por tener poca variedad de contenido o que el mismo no se encuentre disponible en su país o región. Como resultado, esto ha generado una gran brecha digital y concentración de beneficios de la innovación de algunos países y no de otros que prohíben o disuaden el ingreso de productos, servicios o contenido del extranjero a su mercado.

La tensión entre la seguridad y la privacidad

Para regular los delitos cibernéticos se requiere un equilibrio justo entre la privacidad y la seguridad. Como no pueden llegar a este acuerdo entre los diferentes países, no logran establecer normas conjuntas para resolver conflictos.

Ya que es un tema de novedad, un gran número de países todavía no regularon los delitos cibernéticos. Por este motivo, son reacios a formar parte de tratados internacionales en los que no participaron desde el comienzo y actualmente pueden no estar de acuerdo en algunas partes.

Debido al creciente aumento del peligro que significa internet, muchas naciones han aumentado los mecanismos para obtener acceso a información en línea y a comunicaciones.

De esta manera, se intenta anticipar y frustrar los planes antes de que se produzca el delito. La razón detrás de ello es que si se persigue posteriormente a que se haya producido el crimen transnacional es muy difícil resolverlos jurisdiccionalmente ya que como comprenden a más de un país el proceso se vuelve más delicado para ser resuelto acertadamente. (Holt et al., 2017)

Esto, naturalmente, genera un conflicto con las sociedades occidentales u otras que también respetan la libertad de los individuos, porque interfiere con el derecho a la libertad y a la privacidad personal, incluso con el de mantener en secreto aspectos de las vidas de las personas. Si el Estado intenta violar la privacidad de un individuo, esa información debería hacerse pública para evitar que fuera ilegal. Por esta razón, se genera una tensión entre el derecho a la privacidad de la población y la necesidad del gobierno de proteger la seguridad del público en general y evitar que se produzcan delitos.

Este tema tiene importante controversia a nivel de política internacional ya que muchos supuestos en los que un Estado accede a evidencia alojada en extraña jurisdicción puede ser entendido por algunos países u organismos internacionales como violaciones a la soberanía nacional del Estado en el que los datos informáticos están alojados. (Salt, 2021)

Esta tensión entre la privacidad y la seguridad se ve afectada entre Estados que ponderan más la seguridad que la privacidad. Dada esta diferente concepción en prioridad de derechos, resulta más dificultoso para los países llegar a un acuerdo sobre cómo responder a los delitos cibernéticos transnacionales. De esta forma, consolidar tratados internacionales y las legislaciones en común se vuelve impracticable.

Debido a la falta de cooperación entre países y a la escasa normativa se ha generado incertidumbre jurídica que puede derivar en violación de garantías individuales y abuso de algunos países que deriven en conflictos geopolíticos innecesarios. Resulta evidente la afectación a libertades individuales cuando un Estado accede a datos alojados en otras jurisdicciones de otro marco normativo que no se ve amparado por sus derechos y garantías.

La computación en nube

La computación en la nube es un servicio de internet que sirve para migrar información y actividades informáticas de una persona u empresa a computadoras y sitios de hosting con un tercero con quien se celebra un contrato con ese fin. (Fernández Delpech, 2014)

Se plantean muchos problemas de jurisdicción y ley aplicable frente a la computación de nube. No es sencillo saber cómo resolver el problema de legislación aplicable de computación de nube. (Fernández Delpech, 2014)

Esta controversia puede llevar a conflictos entre Estados por acceder a elementos alojados en distintas jurisdicciones y algunos países lo pueden entender como violacion a su soberanía nacional. Se puede profundizar la controversia por el uso masivo de almacenamiento de datos informáticos en dispositivos externos y de los servicios de computación en la nube. Esto lleva a la consecuente pérdida de la localización física de la información. Los usuarios desconocen y le asignan poca importancia al lugar físico, que implica la jurisdicción. (Sponele, 2010)

El mismo problema respecto de la ley aplicable a los contratos de computación de la nube es que la ley aplicable para la mayor parte de los contratos es Estados Unidos, ya que los principales proveedores de estos servicios se encuentran en el país americano (Kaspersen, 2009). Por lo tanto, se puede volver muy dificultoso para los usuarios obtener jurisdicción en algunos países ya que contractualmente se puede interpretar que deben promover acciones en la Justicia Estadounidense.

Los servicios de cloud extranjeros, establecen jurisdicciones extranjeras fuera del Estado Argentino por contrato. Estas cláusulas en principio son válidas, pero de acuerdo al artículo 37 de la Ley de Defensa del Consumidor, se tendrá por cláusula ineficaz o abusiva en los contratos de consumo cláusula no convenidas que importen renuncia o restricción de los derechos del consumidor o amplíen los derechos de la otra parte. De esta forma, el artículo 36 de la misma ley establece que será nulo cualquier pacto en contrario, el tribunal que corresponde es el del domicilio real del consumidor.

También se pueden aplicar a los contratos de consumo la resolución 2612003 de la Secretaría de Coordinación Técnica, que fue dictada en el marco de la normativa de Defensa del Consumidor, que establece que son abusivas las cláusulas en los contratos de consumo en los que la jurisdicción sea distinta del lugar de domicilio del consumidor al tiempo de la celebración del contrato, a menos que se trate de su domicilio real. (Fernández Delpech, 2014)

El artículo 14 del Código Civil establece que el derecho extranjero no debe ser incompatible con principios de orden público del orden jurídico argentino. Del mismo modo, el artículo 1004 describe que las convenciones particulares no pueden dejar sin efecto leyes que estén interesadas en el orden público y las buenas costumbres. (Fernández Delpech, 2014)

Finalmente, muchos opinan que la deslocalización de la información genera que sea necesario preparar y contemplar en el contrato de cloud procedimientos adecuados para lograr validez jurídica de las evidencias electrónicas almacenadas en la nube.

Finalmente, podemos interpretar que no se han encontrado, todavía, soluciones consensuadas en el ámbito de la política internacional ni líneas normativas y jurisprudenciales afianzadas en el proceso civil o penal de los diferentes países. A pesar de que se han logrado avances legislativos, tratados, fallos y concesiones, es un conflicto que todavía no tiene una solución consolidada y que tiene gran trascendencia práctica para el futuro de las investigaciones en entornos digitales.

En Argentina, entendemos que el cuidado de datos no ha recibido un adecuado tratamiento normativo ni jurisprudencial y los tribunales aumentan los casos en que utilizan evidencia transfronteriza sin una normativa clara.

Convenciones y tratados

Como ya mencionamos antes, el carácter global del internet provoca que los delitos por este medio generen problemas políticos y jurisdiccionales producidos por la incompatibilidad de tratar estos ilícitos que pueden estar tipificados distinto en las regulaciones y códigos penales y procesales penal de cada país. Por lo tanto, es sumamente importante que los países ratifiquen documentos, tratados y convenciones internacionales sobre ciberdelincuencia para unificar la solución de estos conflictos.

Si esto no sucede, puede que se generen refugios para los criminales. Es decir, países en los cuales los criminales encuentren protección y puedan cometer ilícitos amparados por la legislación de determinados Estados perjudicando a otros. (Chawki et al., 2015)

Las ventajas de los tratados es que fomentan la cooperación internacional. Estas normativas exploran cómo las naciones abordan la problemática de la globalización del internet y los

delitos informáticos sin fronteras y permiten su persecución más allá de las jurisdicciones de las naciones. (Chawki et al., 2015)

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional ha contribuido modernizando y armonizando reglas en los negocios internacionales. La Convención de las Naciones Unidas se refirió la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales y esta complementa la Convención sobre los Contratos de Compraventa Internacional de Mercaderías que incrementa la seguridad jurídica de los contratos electrónicos internacionales y ayuda a predecir la ubicación de las partes para establecer la jurisdicción en caso de delitos. Este avance será de gran utilidad para la determinación de la jurisdicción y la elección de la ley para contratos celebrados en línea.

Muchas leyes nacionales tienen como objetivo producir efectos a nivel extraterritorial. Estas normativas se aplican a individuos o empresas fuera de las fronteras del Estado que las creó. (ISOC, 2018)

Prosiguiendo con este análisis, la normativa de la Unión Europea sobre protección de datos está regulada en el Reglamento General de Protección de Datos (GDPR), que se aplica respecto a empresas fuera de la Unión Europea pero que pueden tener o utilizar datos de ciudadanos europeos.

Muchas leyes y tratados internacionales que regulan internet solo lo hacían cuando era estrictamente necesario, y de esa forma brindar cierta seguridad en el comercio. Así como fomentar la apertura e innovación en el desarrollo de las redes. Por ejemplo, antes se entendía que casi todas las plataformas de internet eran un mero intermediario, en el que los operadores de redes no eran responsables por el contenido que compartían. Sin embargo, la Directiva de la Unión Europea sobre el Comercio Electrónico del 2.000 o La Ley del Derecho de Autor en el Digital Millennium Copyright Act ha cambiado este paradigma.

La corriente global se está enfocando en tratar los ciberdelitos en conjunto mediante convenios y tratados internacionales. Con los años, han ido surgiendo nuevos tratados y normativas en todos los planos, pero parecen ser todavía insuficientes al momento de resolver los conflictos y los delitos de robo de datos.

El enfoque estadounidense

Antes de las legislaciones en los años ochenta, los tribunales americanos se basaban en principios consuetudinarios para perseguir los delitos informáticos, y en gran parte de los casos, sirve para diferenciar delitos comunes y las nuevas situaciones creadas por las nuevas tecnologías.

Se tornó muy difícil comparar los delitos tradicionales con los nuevos delitos tecnológicos. El aumento en el uso de la tecnología condujo a más casos y la comprensión generalizada de que se requería regulación para mejorar la situación y fue una mejora notable en claridad y facilidad de uso. (Chawki et al., 2015)

Estados Unidos, desde hace muchos años viene implementando leyes y jurisprudencia para ampliar el alcance de su jurisdicción. Es decir, se intenta implementar que más personas que cometen delitos en los que pueda afectar de alguna forma a este país o a sus ciudadanos, sean juzgados en territorio americano. Tal es el caso del convenio de extradición con la Unión Europea. Otro ejemplo, es la reciente decisión de extraditar a Julian Assange desde Gran Bretaña a Estados Unidos por robar y compartir datos. Esta decisión se tomó por medio de la Ley de Extradición Británica artículo 73 y categoría 2 del año 2003 (British Parliament, 2003), en la que se permite la extradición a Estados Unidos y demás países, así como con la Unión Europea cuando los delitos fueron cometidos en esos países.

Para Estados Unidos es más difícil aceptar las normativas de la Unión Europea debido a su mayor rigurosidad. Esto puede desencadenar en menor aplicación de los tratados internacionales que por carecer de apoyo de naciones, puede faltarle fuerza de aplicación. (Chawki et al., 2015)

En los Estados Unidos, no existe una Codificación Nacional del Derecho Internacional Privado. Es un tema que trata cada Estado en particular. Por ejemplo, el Código Penal de California establece qué actos constituyen los crímenes cibernéticos, los cuales incluyen: La alteración, daño, eliminación o uso de datos informáticos para realizar defraudaciones, el engaño, la extorsión o la obtención o control del dinero, la propiedad o los datos usando servicios informáticos sin permiso. Sin embargo, existe un sinnúmero de sentencias y casos judiciales sobre disputas internacionales respecto a jurisdicción electrónica de carácter federal.

Debido a la ausencia de leyes uniformes respecto a las relaciones contractuales en los Estados Unidos, el Uniform Commercial Code y el Second Restatement son importantes para determinar las leyes aplicables a los contratos concluidos y perfeccionados electrónicamente, y sus correspondientes delitos dentro del país.

Si bien en Estados Unidos, cada Estado regula los delitos cibernéticos, existen leyes de alcance federal y estatal. Todas intentan proteger los datos de los usuarios y así evitar robos o usos indebidos. Algunas de ellas son la Stored Communication Act, Clarifying Lawful Overseas Use of Data Act y la California Consumer Privacy Act. Y también jurisprudencia como United States V. Ivanov y Microsoft V. United States.

Ley de Comunicaciones Almacenadas (Stored Communication Act)

La Ley de Comunicaciones Almacenadas proporciona protección de la privacidad para aquellos usuarios de proveedores de servicios de red.

El artículo 2.701 de la ley Stored Communication Act (SCA) dispone penas para personas que accedan intencionalmente, sin autorización, a algún servicio en el cual se acceda a comunicaciones o que se viole autorización para acceder a esos datos. Puede que tenga, altere o impida el acceso autorizado a una comunicación por cable o electrónica que esté almacenada en el sistema. (Congress of the United States of America, 1985)

La Ley de Comunicaciones Almacenadas tiene como objetivo alcanzar dos tipos de servicios en línea: los servicios de comunicación electrónica y los servicios de computación remota. (Chawki et al., 2015)

Ley de Uso Legal de Datos en el Extranjero (Clarifying Lawful Overseas Use of Data Act)

La Ley Estadounidense Clarifying Lawful Overseas Use of Data Act (CLOUD) se creó con el objetivo de coordinar los intereses de las fuerzas de seguridad y empresas de tecnología para acceder a datos a nivel internacional. (Congress of the United States of America, 2018)

Esta ley obliga a las empresas tecnológicas que tienen sede en Estados Unidos a proporcionar datos que tengan almacenados al Estado. En la sección 3 (1) se establece que tiene efectos

extraterritoriales porque se aplica a cualquier dato en poder de un proveedor estadounidense de servicios de comunicación electrónica o servicios informáticos remotos, independientemente si están dentro o fuera de los Estados Unidos.

Ley de Privacidad del Consumidor de California (California Consumer Privacy Act)

La presente ley sancionada en California en el año 2018, codifica la privacidad y la protección del usuario. Introduce penalidades por el uso erróneo de datos personales. (Congress of the State of California, 2018)

El California Consumer Privacy Act puede tener posibles efectos extraterritoriales. Se aplica a todas las empresas, sin importar en qué lugar del mundo se ubican, el único requisito es que recoja o posea información de residentes californianos.

United States v. Ivanov

Para muchos doctrinarios, este caso es el primer precedente a nivel internacional en el que se realiza el registro y el secuestro transfronterizo de datos utilizando medios tecnológicos. Por este motivo, se desencadenó un gran interés y fue el puntapié de muchas discusiones en el plano internacional. En 1999, dos ciudadanos rusos accedieron ilegalmente a sistemas informáticos en EE. UU, donde lograron obtener datos personales y comerciales que disponían empresas de servicios de internet como Yahoo! o Ebay y con estos datos lograron cometer fraudes.

El caso lo investigó el FBI, que posteriormente descubrió que el fraude se realizó en computadoras ubicadas en Rusia. Con esta información, el buró ideó una operación para traer engañosamente a los sospechosos rusos al territorio americano. Una vez en su territorio, logró detenerlos.

El FBI, consiguió obtener evidencia ingresando a los presuntos servidores sospechosos y encontrar las pruebas necesarias para condenar a los imputados (que incluían más de 56.000 tarjetas de crédito) sin requerir colaboración de autoridades rusas por medio de convenios de cooperación. Los imputados fueron condenados por esa evidencia obtenida de forma

transfronteriza sin cooperación internacional y sin ninguna ayuda ni conocimiento de las autoridades rusas, que no prestaban voluntad cooperativa. (Salt, 2021)

Entendemos que esta no es la forma ideal de resolver los conflictos de extraterritorialidad realizados desde servidores en distintos países. La mejor solución es lograrlo mediante convenios internacionales y cooperación internacional. Los países deben fomentar y desarrollar sus lazos en materia de ciberseguridad con el fin de tener un mundo más seguro.

United States v. Microsoft

La gran mayoría de las empresas que proveen servicios multinacionales relacionados a la tecnología, se rehúsan a colaborar con pedidos de autoridades de justicia penal de diferentes países a la sede central o ubicación de los servidores que se refieren generalmente a empresas norteamericanas. (Salt, 2021)

En este caso, Microsoft rechaza entregar datos solicitados por autoridades alegando que los datos están alojados en Irlanda, obligando a la empresa a cumplir con la legislación de datos personales de ese país y de Europa. Asimismo, las autoridades estadounidenses deben utilizar los convenios internacionales de cooperación internacional, aunque se trate de una empresa estadounidense. (United States v. Microsoft Corp, 2015)

Microsoft sostiene que el cumplimiento implica un caso de acceso transfronterizo a datos almacenados en Irlanda a pesar de que puedan ser accedidos desde Estados Unidos. Según la empresa, esto violaría la cuarta enmienda de Estados Unidos y generaría una intromisión en la soberanía de otro Estado violando convenciones internacionales. El juez no hizo lugar al reclamo de Microsoft y actualmente existe una apelación pendiente de resolución. (Salt, 2021)

El enfoque europeo

Europa es un pionero en la regulación de los conflictos informáticos. En muchos países se ha comenzado a regular desde 1970. La mayor parte se han enfocado en la protección de objetos tangibles. La revolución de las nuevas tecnologías ha generado el desarrollo de nueva legislación incorporando estos nuevos avances. (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020)

Las primeras legislaciones en esta materia abordaron la protección de la privacidad, la regulación respecto a recopilar, almacenar y transmitir datos de computadora (Siber, 1998). Las legislaciones que protegen los datos han sido constantemente actualizadas para proteger el derecho a la intimidad por medio de normas administrativas, civiles y penales. (Chawki et al., 2015)

La Unión Europea tiene como objetivo conformar un mercado único fuerte y así desarrollar e implementar un enfoque integral para la ciberdiplomacia, no solo a nivel europeo, si no también a nivel mundial. Esto se puede ver en la Estrategia Global para la Política Exterior y de Seguridad de la Unión Europea, de esta forma, construir una mayor resiliencia y autonomía estratégica para aumentar las capacidades en términos de tecnología y habilidades. Esto lo hace enfocándose en el Mercado único Digital, la Estrategia Global, la Comunicación Conjunta al Parlamento Europeo y al Consejo sobre Resiliencia, Disuasión y Defensa en Ciberseguridad y la Agenda Europea de seguridad. (Comisión Europea, 2017)

La UE ha avanzado sustancialmente en la criminalización de los ciberataques a un nivel comparable en todos los Estados Miembros, lo cual facilita la cooperación transfronteriza de todas las autoridades que se encargan de investigar y juzgar los casos. Debido a la naturaleza sin fronteras de Internet, el marco de cooperación internacional está provisto esencialmente por el Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa.

La Asociación Europea le da prioridad al establecimiento de un marco legal y estratégico para la prevención de conflictos y la estabilidad en el ciberespacio en sus compromisos bilaterales, regionales, de múltiples partes interesadas y multilaterales, dado que la UE promueve el derecho internacional para resolver los ciberdelitos a nivel global. (Consejo de la Unión Europea, 2017)

El Consejo de la Unión Europea, en el año 2000 promulgó el Reglamento N° 44/2001 respecto a la competencia judicial, reconocimiento y ejecución de sentencias en materia civil y mercantil. El Reglamento de Bruselas tiene como objetivo armonizar la normativa y así evitar conflictos jurisdiccionales en materias civiles y asuntos comerciales. De esta forma, ejecutar rápidamente sentencias de los Estados Miembros. Este reglamento fue revisado en 2009 para modernizar las reglas de jurisdicción.

En España, por ejemplo, el fallo Google Spain SL, Google Inc. V Agencia Española de Protección de Datos, Mario Costeja González (2014) en el que su tribunal creó un derecho al olvido en los resultados del buscador de Google para toda Europa. Este fallo amplió enormemente la aplicación territorial de las normas europeas como el Reglamento General de Protección de Datos a entidades para países fuera de la Unión Europea al momento de dictar sentencias y resoluciones de las normas de protección de datos frente a entidades no europeas. (López-Lapuente, 2019)

Por lo tanto, podemos mencionar como destacados las siguientes normativas y fallos que tienen aplicación en la Unión Europea respecto a conflictos originados por ciberdelincuencia y robo de datos.

El Convenio de Budapest sobre la Ciberdelincuencia

El Consejo de Europa firmó el convenio de Budapest en 2001 y es considerado el tratado internacional más completo hasta la fecha, ya que proporciona una seguridad jurídica frente al cibercrimen esencial para su utilización. Este tratado proporciona un marco integral y coherente frente al ciberdelito. El convenio de Budapest es hasta ahora la respuesta más eficaz que existe legislativamente para combatir los crímenes informáticos hasta la fecha (Koops, 2011).

Este acuerdo se ha transformado en un modelo preferido por muchos países, en los términos de la promoción de su propia legislación nacional y en la construcción de una cooperación internacional. El Convenio criminaliza conductas desde el acceso al ilícito, ataques a la integridad del sistema, datos de fraude informático, delitos de pornografía infantil, entre otras. También brinda herramientas procesales para que la investigación y la obtención de evidencia sea más efectiva. Por último, proporciona cooperación internacional más ágil y eficiente. La GDPR se diseñó para proteger datos personales de usuarios europeos sin importar la jurisdicción donde se procesen. (Consejo de la Unión Europea, 2016)

El tratado no se ha limitado a la adhesión únicamente a miembros de la Unión Europea, también, se ha permitido por medio del artículo 37 invitar a adherir a Estados que no sean miembros del Consejo de Europa, por ello el convenio cuenta con miembros de otros continentes, conformado por 66 en total como los casos de: América (Argentina, Chile, Canadá, Estados Unidos, Panamá, Colombia), Europa fuera de la Unión Europea (Reino Unido, Albania,

Andorra, Suiza, Serbia, Ucrania), África (Mauricio, Cabo Verde, Ghana, Senegal, Marruecos), Asia (Armenia, Israel, Japón, Filipinas), Oceanía (Australia, Tonga), y muchos países más dentro de cada continente.

El mismo consta de cuatro capítulos: Sistema informático, dato informático, proveedor de servicio y datos de tráfico. El capítulo dos establece la necesidad de criminalizar ciertas conductas realizadas por medio de dispositivos tecnológicos. Como es el caso del acceso ilícito a un sistema informático, la interceptación ilícita de datos, el abuso de dispositivos, el fraude informático y demás. Del mismo modo, se establecen medidas sobre la forma en la que deben llevarse a cabo los procedimientos de investigación. De esta forma, encontramos disposiciones de conservación rápida de datos y así evitar que sean eliminados, así como respecto a registros y secuestros de dispositivos y la obtención en tiempo real de datos de tráfico o interceptación de contenido. El capítulo tres refiere a la cooperación internacional y describe disposiciones sobre asistencia mutua en temas como extradición, acceso, conservación, obtención e intercepción de datos. Por último, el capítulo final se refiere a cuestiones de entrada en vigor, forma de adhesión de los estados y las reservas que pueden hacerse al momento de incorporarse. (Asociación por los derechos civiles, 2018)

La aplicación territorial, como se prescribe en el artículo 38, dice así: “Los Estados podrán, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, designar el territorio al que resultará aplicable el presente Convenio. (...) Los Estados podrán, en cualquier momento, a través de una declaración dirigida al Secretario General del Consejo de Europa, extender la aplicación del presente Convenio a otros territorios diversos a los designados en la declaración.”

Del mismo modo, en el anexo de recomendaciones, punto 17, se prevé la necesidad de extender registros de datos a sistemas ubicados en extrañas jurisdicciones para casos de urgencia. También se exhorta a los países a establecer por medio de acuerdos internacionales una base legal clara para precisar casos y condiciones en los cuales las extrañas jurisdicciones serían permitidas.

A pesar de esto, en el artículo 4 se permite a cada miembro adoptar todas las medidas necesarias para perseguir las ofensas criminales bajo el derecho doméstico.

La idea del tratado es criminalizar la producción, la venta, el uso, la importación, distribución o cualquier forma de utilizar los dispositivos, incluyendo los programas de computadora. (Chawki et al., 2015) Desde la Convención, se criminaliza la creación y la distribución de virus informáticos.

El creciente éxito de la Convención se puede ver tanto en escala micro como en macro. Muchos países están en el proceso de armonizar sus leyes domésticas con las del Convenio y compartir estándares, sea que tengan la intención de unirse o no.

El comité ha decidido desde el comienzo no realizar cambios normativos domésticos. Entendieron que en un futuro debería ser tratado, pero en el momento en que se creó, no lo consideraron oportuno por la arraigada idea de soberanía nacional relacionada con la jurisdicción nacional. (Salt, 2021)

El Comité del Convenio de Budapest generó grupos de trabajo para estudiar y generar alternativas relacionadas al acceso transfronterizo de datos y jurisdicción (2012) y luego un grupo para el trabajo de justicia penal y acceso a evidencias almacenadas en la nube (2014). De todas formas, hasta la actualidad, no se logró un consenso en el que se pueda reformar el texto de la convención o promover un protocolo adicional.

Como mencionamos anteriormente, países de todos los continentes han firmado el tratado e intentan resolver estos conflictos cada vez más frecuentes. Los países árabes del Medio Oriente parecen ser los más reticentes a firmar el convenio, y prefieren utilizar sus propios mecanismos. Igualmente, en muchos casos son muy similares a los de la Convención. Estos países no quieren firmar y ser parte porque algunos lo entienden como un tratado muy occidental.

Por este motivo, el Convenio de Budapest es un instrumento internacional muy útil para la armonización de leyes, estrategias y estatutos para la prevención de los cibercriminales (Ibid). Incluso, es eficaz para los países que no se unieron, ya que muchos lo han utilizado como modelo. (Chawki et al., 2015)

Reglamento General de Protección de Datos

Como explica López Lapuente en La aplicación extraterritorial del Reglamento General de Protección de Datos (2019), el Reglamento UE 2016/679, fue una ampliación del ámbito de aplicación territorial de las normas europeas de protección de datos respecto al ámbito natural que se establecía. Introdujo reglas de aplicación extraterritorial por lo que se permite a países fuera de la Unión Europea quedar sujetas a su aplicación en todo sentido, incluso respecto al régimen sancionador.

Se describe en el apartado 2 del artículo 3 del RGPD y establecen los supuestos en los que se pueden sumar ajenos de la unión para quedar sujetos a reglas establecidas por el presente reglamento. Datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) La oferta de bienes o servicios a interesados en la unión y b) el control de su comportamiento en la medida que tenga lugar en la unión.

“El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. 3.El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público”. (López-Lapuente, 2019)

Esta amplitud de extraterritorialidad en el Reglamento de Protección General de Datos confirma la tendencia de consolidación por parte de la Unión Europea que implica la exigibilidad de cumplimiento de normas de protección de datos para entidades que no estén ubicadas ni sean europeas pero que lleven a cabo actividades empresariales en la Unión Europea.

La única exigencia es un establecimiento en algún país de la unión, pero no se exige ninguna forma de entidad jurídica concreta. La guía de la UE dice que con un solo empleado o agente

dentro de la Unión Europea es suficiente. El reglamento tiene por objetivo ser lo más laxo posible para obtener jurisdicción.

Cualquier recolección de datos online no genera que se pueda aplicar el reglamento automáticamente. Es necesario analizar la finalidad prevista por el responsable, incluso posibles tratamientos ulteriores como el perfilado de datos personales.

El mero hecho de que una página web esté disponible en castellano, por ejemplo, no significa que pueda aplicarse el RGPD. No tiene importancia que se vendan productos a España desde el extranjero, si no cuenta con los requisitos mencionados anteriormente, no es relevante para determinar la aplicabilidad que se esté ofreciendo a ciudadanos extranjeros.

La Convención de Roma

La convención de Roma es de gran utilidad cuando las partes establecen qué derecho aplicar. Este tratado es útil porque asegura la protección de las interpretaciones o ejecuciones de los artistas intérpretes o ejecutantes, los fonogramas de los productores de fonogramas y las emisiones de los organismos de radiodifusión.

El Convenio entró en vigor en 2009. Su principal objetivo fue consolidar la autonomía de las partes, y permitir que las partes involucradas en los contratos puedan determinar las leyes de qué país pueden ser aplicables. Asimismo, establece reglas más específicas y adaptadas a las tecnologías de la información. El Convenio en cuestión, fue redactado con coherencia al reglamento de Bruselas y establece reglas provisorias para la elección de los contratos. (Wang, 2010)

La Convención de Roma no se aplica específicamente para transacciones comerciales electrónicas. El objetivo es reforzar dos principios fundamentales: La libertad de elección y la ley aplicable frente a la ausencia de elección.

El artículo 1 del Convenio describe que las normas del Convenio se aplican a las obligaciones contractuales en cualquier situación que implique una elección entre las leyes de diferentes países. Respecto al ámbito territorial, el artículo 2 del Convenio establece: “Cualquier ley especificada por el presente Convenio se aplicará, sea o no la ley de un Estado contratante” Esto es de aplicación universal. (Wang, 2010)

En caso que en el contrato no haya una cláusula de elección de ley, la determinación de la ley aplicable puede ser muy complicada. La convención dispone en el artículo 4.1 que en caso que no exista la mencionada cláusula, el contrato se regirá por la ley del país con el que el contrato tenga lazos más estrechos.

Directiva sobre Ataques Contra los Sistemas de Información (Directive on Attacks Against Information Systems)

La presente directiva criminaliza los ataques contra los sistemas de información e introduce nuevas ofensas criminales en el caso de obtener acceso ilegal a información o interferir en sistemas de datos. (Consejo de la Unión Europea, 2013)

La directiva establece que si un acto delictivo contra la información toma lugar en su territorio, no importa si el infractor se encuentra físicamente en el territorio o que sea nacional de un estado miembro, igualmente poseen jurisdicción para tratar el delito.

En cambio, cuando el delincuente tiene nacionalidad de un estado miembro de la Unión Europea pero comete el delito fuera del territorio, la directiva posee jurisdicción extraterritorial basada en el principio restrictivo de nacionalidad activa. (ISOC, 2018)

El caso de Portugal

Portugal ha admitido buenas soluciones para el conflicto de extraterritorialidad que se produce por delitos ocasionados por medio de internet.

El país ha avanzado partiendo desde la Convención de Budapest. Posteriormente, con la ley 109/09 habilita el acceso transfronterizo de datos en determinados supuestos. El artículo 15.5 de la ley admite que se puedan secuestrar datos de un dispositivo transfronterizo cuando en el transcurso de la investigación surgieran razones para creer que puede encontrarse evidencia en otros sistemas judiciales mediante autorización u orden de autoridad competente. Asimismo, el artículo 25 de la misma ley prevé la posibilidad que un Estado extranjero pueda acceder a datos alojados en servidores o dispositivos ubicados físicamente en Portugal en casos de datos abiertos o con consentimiento de la persona autorizada a revelarlos. (Salt, 2021)

El caso de Bélgica

El artículo 88 del Código Procesal Penal de Bélgica autoriza al juez de investigación cuando ordena registro de un sistema informático a extender investigación en el lugar que estuviese con el fin de descubrir la verdad, que sea proporcional y con el peligro de que desaparezca la prueba. (Salt, 2021)

La norma autoriza a copiar los datos, pero no removerlos. El legislador del país entiende que la copia de datos no afecta el principio de territorialidad ya que la copia no es lo mismo que el secuestro de datos.

El enfoque argentino

En un principio, en nuestro país no existían normas jurídicas que tipifican todos los delitos informáticos. Poco a poco, se han comenzado a regular los delitos informáticos en todos los aspectos y ámbitos, y se ha comenzado a tipificar ampliamente tanto por tratados internacionales, como por códigos y leyes de alcance nacional y provincial.

La regulación en el Código Penal Argentino y las leyes que lo complementan han contribuido en un avance respecto a este tema y sirven para proteger a los consumidores y a las víctimas de un delito que, como expusimos anteriormente con datos, cada vez afecta más a los usuarios argentinos.

No obstante ello, es necesario que se continúe realizando trabajo en materia legislativa en delitos cibernéticos y en su tipificación, ya que actualmente resulta de una ardua tarea resolver los ciberdelitos con jurisdicciones extrañas que involucran nuestro país.

Código Civil y Comercial de la Nación

En el nuevo Código Civil y Comercial (Roble, 2014), no se encuentra regulado específicamente el derecho informático ni su alcance territorial. Sin embargo, en el Código sí se regula el derecho internacional privado, el cual tendría alcance para entender los fraudes y las estafas en el derecho nacional. El art. 2.595 expresa que se determina el derecho aplicable por las reglas en vigor dentro del Estado al que ese derecho pertenece y, en defecto de tales reglas,

por el sistema jurídico en disputa que presente los vínculos más estrechos con la relación jurídica de que se trate.

También explica que, si diversos derechos son aplicables a diferentes aspectos de una misma situación jurídica o a diversas relaciones jurídicas comprendidas en un mismo caso, esos derechos deben ser armonizados, procurando realizar las adaptaciones necesarias para respetar las finalidades perseguidas por cada uno de ellos.

Es interesante entender que de acuerdo al artículo 2.598, para determinar el derecho aplicable en materias que involucran derechos no disponibles para las partes, no se tienen en cuenta los hechos o actos realizados con el solo fin de eludir la aplicación del derecho designado por las normas de conflicto. Este artículo es esencial, ya que muchas veces los delitos los realizan desde otro país para así tener las ventajas de la ley de dicha jurisdicción. Por este motivo, el derecho argentino entiende que, si es con este fin, rige nuestro derecho.

De acuerdo al artículo 1.109 del Código Civil y Comercial, en los contratos por medios electrónicos o similares, se entiende la jurisdicción en el lugar donde el consumidor recibió o debió recibir la prestación. Allí se fija la jurisdicción aplicable para los conflictos derivados del contrato. En otras palabras, el lugar de cumplimiento del contrato es aquel en que el consumidor hubiera recibido la prestación y fija la jurisdicción. (Torello, 2015)

Código Penal de la Nación Argentina

Recientemente se regularon por medio del Código Penal los delitos informáticos contra la integridad sexual, contra la libertad, la propiedad, la seguridad pública y contra la administración pública.

La Ley de Delitos Informáticos 26.388 tipifica delitos e incorpora al código penal algunos tipos de delitos relacionados con la nueva tecnología. La reforma del código introducida por esta ley modifica determinadas figuras penales ya previstas en el código penal para introducir elementos y modalidades de carácter informáticos para su comisión.

En esta ley se incorpora el daño informático al artículo 183 del Código Penal: “Sera reprimido con prisión de quince días a un año (…) el que alterare, destruyere o inutilizar datos,

documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujera en un sistema informático, cualquier programa destinado a causar daños".

En el fallo de la Corte Suprema de Justicia de la Nación "Russo, Christian Carlos", un argentino adquirió un software para manipular computadoras remotamente y desplegó maniobras para utilizar el sitio web de la Embajada de los Estados Unidos. La embajada de Estados Unidos lo denunció frente a la Justicia Argentina. Podría haber tenido jurisdicción las cortes de Estados Unidos dado que fue un hecho dentro de la embajada, pero de todas formas decidieron iniciar el proceso en Argentina. La Corte se basó en el artículo 183, segundo párrafo del código penal mencionado anteriormente para entender el caso. (Russo, Christian Carlos y otro s/ infracción art. 183 del Código Penal - incidente de competencia, 2015)

En un principio se entendía al artículo 172 que refiere a estafas y otras defraudaciones como que englobaba los delitos de phishing, ya que el artículo dice asi: "Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño".

Sin embargo, doctrinarios como Aboso y Zapata (2006) entienden que la figura del 172 no se puede emplear con algunos delitos de fraude informático ya que el encuadre requiere ardid en el autor del delito, error de la víctima y perjuicio patrimonial. En este sentido, como se produce daño en el software y se afecta la lógica del sistema, no se generan las premisas explicadas anteriormente, debido que los actuales sistemas están completamente informatizados y su funcionamiento se encuentra automatizado, de modo que no se podría entender como error de la víctima el hackeo sobre el sistema informático.

Por otro lado, posteriormente se han adicionado al artículo 173, los incisos 15 y 16 para tratar específicamente los delitos de phishing: "al que defraudare a otro mediante uso de tarjetas de compra, crédito o débito, cuando hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos (...) o también el que defraudare mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos". Se puede observar que, por elección legislativa, importa una necesidad de remitir a la

figura básica tradicional contenida en el art. 173 para determinar los elementos constitutivos de su tipicidad. (Petrone et al., 2021)

La jurisprudencia se expresó en relación al artículo 173 en “Juz. Fed. San Isidro N° 1 Sec. N°2, Sec. Penal N°1- Sala I “Inc. de apelación del procesamiento de B”- San Martin- 7/6/2013” que: La disposición patrimonial debe ser consecuencia de cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos que produce el hecho lesivo. En esta dirección, se entiende como manipulación a cualquier modificación del resultado de un proceso automatizado de datos a través de la alteración de los existentes o la introducción de nuevos, en cualquiera de las fases del proceso.” De igual forma, se entiende el artículo 173 inc. 16 en el fallo ““C., P. A. s/ recurso de casación”- CFed. Casación Penal - Sala III- 16/6/2015- Cita digital IUSJU001828E“. (Parada & Errecaborde, 2018)

Otro fallo, referente a Phising, (G.R. y otro s/procesamientos, 2010) imputa a dos personas por realizar estas técnicas informáticas para obtener datos necesarios de tarjetas de crédito y así efectuar transferencias de dinero dentro de sus cuentas bancarias. La jurisprudencia entendió que en Argentina se puede entender y regular el robo de datos y casos de phishing. Del mismo modo, aquí se pena entendiendo phishing con el delito de defraudación por el art. 173, inc. 16.

La mencionada ley 26.388 incorpora en el año 2008 el artículo 153 bis y 153 que dice: Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica (…) en la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

Tomando en cuenta el artículo precedente (153), la Corte Suprema de Justicia de la Nación, ha entendido en “Díaz, Sergio Darío” donde la ex pareja del denunciante ingresó a sus cuentas de Facebook y correos electrónicos sin autorización para disponer y utilizar datos de la víctima abusando de su confianza. La Corte entendió que se debía aplicar el artículo 153, pero decidió que era la justicia federal la que debía entender el proceso y no la justicia local. (Diaz, Sergio Dario s/ violación correspondencia medios electo art. 153 2° p., 2014)

Artículos similares que atañen a esta tesis son el 157, que reprime con un mes a dos años e inhabilitación especial de uno a cuatro años al funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos, y el 157 bis que reprime de 1 mes a dos años a aquél que, violando seguridad de datos, 1. accediera a bancos de datos personales y 2. proporcionare o revelare esa información o 3. ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Del mismo modo, está legislada la protección de datos por la ley de datos personales número 25.326, especialmente el art. 12 y el art. 12 del decreto 1.558/2001 de Protección de Datos Personales. Está ley, incorporada en el año 2.000, brinda ciertas definiciones y regulación útil que en su momento fue esencial para comenzar a entender y regular los delitos cibernéticos en Argentina.

También, complementan para brindar seguridad jurídica, la ley 24.766, denominada como sustracción de secretos comerciales contenidos en soportes informáticos. Así mismo, por la alteración dolosa de registros, establecido como delito en los arts. 12 y 12 bis. de la ley 24.769. (Banco Interamericano de Desarrollo & Organización de los Estados Americanos, 2020)

Es importante que nuestro país continue firmando tratados y convenios internacionales de ciberdelitos y extradición, ya que como explica el perito informático de la causa (P. y otros s/defraudación, 2015): “por lo general, y acorde a su experiencia en el tópico, estas maniobras defraudatorias son realizadas por personas con vastos conocimientos técnicos informáticos que encuentran en países extranjeros. A su vez, los verdaderos titulares de las I.P. son herramientas de los autores, quienes infectan los softwares de estas personas a través de virus troyanos y la controlan mediante aplicaciones de la más variada índole allí instaladas, que no suelen dar a conocer su origen, o si lo hacen remiten a servidores en el exterior. Estos virus a los que se hace referencia permiten el acceso a un sistema remoto en el que se pueden realizar distintas acciones sin contar con permiso alguno de su titular, quien en la mayoría de estos casos siquiera tiene conocimiento de la invasión de sus datos personales”.

La mencionada normativa, permite y brinda a la Argentina tener competencia y jurisdicción para resolver los casos en los cuales se vean involucrados los delitos cibernéticos de phishing. Por lo tanto, las leyes y los fallos referidos han demostrado haber resuelto delitos de estas categorías, Argentina no es totalmente ajena a los delitos de robo de datos. Dicha regulación

permite que Argentina posea una normativa uniforme y, por ende, pueda tener jurisdicción y resolver los casos que acontezcan total o parcialmente en el país.

Como reflexión final, podemos concluir que la argentina en relación a la ciberdelincuencia necesita un gran desarrollo y una legislación más clara de forma que tiene muchos desafíos por delante. La ley de delitos informáticos 26.388 así como el código penal son un gran avance y pueden ser considerados como un puntapié inicial en este desarrollo y no como la conclusión en este tema.

Consideraciones adicionales sobre jurisdicción

Todos los Estados Miembros de la OEA adoptaron legislación penal nacional para contar con disposiciones para delitos relacionados con la informática. Además de las disposiciones legales, muchos estados, como el Argentino, se adhirieron al Convenio de Budapest sobre ciberdelincuencia, que ofrece un marco legal internacional integral y confiable para combatir el delito cibernético desde hace veinte años.

Como explican Darahuge y Arellano González (Parada & Errecaborde, 2018) la regla fundamental es que el juez competente es el del lugar de comisión del delito. Su fundamento se encuentra en el artículo 118 de la Constitución Nacional:

> *"Todos los juicios criminales ordinarios, que no se deriven del derecho de acusación concedido a la Cámara de Diputados se terminarán por jurados, luego que se establezca en la República esta institución. La actuación de estos juicios se hará en la misma provincia donde se hubiere cometido el delito; pero cuando éste se cometa fuera de los límites de la Nación, contra el Derecho de Gentes, el Congreso determinará por una ley especial el lugar en que haya de seguirse el juicio."*

Para poder llevar a la práctica esta regla, las provincias, al dictar leyes orgánicas del poder judicial, decidieron dividir los territorios dentro de los límites que se le atribuye la competencia un juez o grupo de jueces.

El objetivo de la legislación argentina se funda en la proximidad del tribunal al lugar del hecho para, de esta forma, favorecer la garantía de defensa en juicio y el principio de economía procesal, ya que se favorece a la rápida, sencilla y más económica investigación.

En derecho penal, se considera que el delito se comete en el lugar de su consumación definitiva. Nuestro ordenamiento lo entiende cuando ya se hayan cometido todos los actos constitutivos de delito. (Parada & Errecaborde, 2018)

Pueden suceder distintos supuestos. Uno es el caso de la tentativa del delito que, en este caso, será competente el juez del lugar donde se cumplió el último acto de ejecución. En el caso que se trate de un delito continuado, será competente el juez del lugar donde cesó de cometerse el delito. En este caso, el lugar donde se encontraba la víctima.

Si no se sabe el lugar donde se cometió el delito, será competente el juez que primero previno del caso. En el supuesto que un tribunal se reconoce como incompetente territorial, debe remitir su causa al tribunal competente, poniendo a disposición a los detenidos, si los hubiere. (Código Procesal Penal Federal, 2019)

Pueden existir problemas de competencia cuando dos o más órganos jurisdiccionales se declaran simultáneamente competentes para la investigación o juzgamiento del mismo hecho. El conflicto surge cuando el juez decide oficiosamente sobre su competencia o cuando ello es planteado por las partes. Si ambos o ninguno de los jueces aceptan el caso, corresponde la decisión a quien resulte superior jerárquico común de los enfrentados.

Observaciones de los enfoques comparados

Hemos analizado cómo regulan y entienden los conflictos jurisdiccionales los Estados Unidos, la Unión Europea y Argentina. Todos los países presentan sus propias características que la diferencian del resto. Luego de estudiar los distintos enfoques podemos llegar a distintas conclusiones.

La Unión Europea se ha enfocado en redactar tratados internacionales, como el Convenio de Budapest, que comprenden, no solo a toda la Unión, si no que además a los que no forman parte pero que desean adherirse. Esta es una gran herramienta, ya que se facilita la solución de los conflictos extraterritoriales trabajandolos en conjunto. Esta forma puede resultar útil en tanto muchos países se adhieran a los tratados y convenciones, y hagan un esfuerzo por aplicarlos.

Estados Unidos, por su lado, ha intentado extender su jurisdicción lo más internacionalmente posible para poder entender la mayor cantidad de casos. Esto lo lleva a cabo por medio de, por ejemplo, la ley federal CLOUD o el Código Penal de California. Este método no es el más conveniente porque si el delincuente se encuentra en territorios donde no existen buenas relaciones bilaterales se deviene muy difícil de juzgar.

Finalmente, en Argentina se definen delitos informáticos y se encuadran los delitos cibernéticos, especialmente por el Código Penal. De esta forma, se logra establecer jurisdicción en el plano nacional. En el plano internacional, Argentina se ha adherido a algunos tratados internacionales para así poder resolver los casos que involucran a muchos países.

Creemos que una tipificación en el plano nacional como la de Argentina es conveniente, porque es relativamente sencilla y fácil de aplicar. Se puede encontrar en los Códigos Nacionales la normativa referente a los delitos informaticos de fraude sin la necesidad de hacer una busqueda minuciosa de leyes como es el caso de los Estados Unidos.

Por otra parte, en el plano internacional, es esencial el rol que ha tomado la Unión Europea para unir los intereses de ciberseguridad de las naciones y encontrar soluciones en conjunto. Sostenemos que en el plano transnacional, las naciones deberían acercarse al accionar de la Unión Europea con relación al trabajo en conjunto para de esta forma priorizar la solución de los conflictos por sobre las delimitaciones transfronterizas.

Conclusiones

A lo largo de este trabajo se ha demostrado que es preciso tratar los delitos de ciberdelincuencia, robo de datos o phishing entre los Estados a través de la implementación de un enfoque internacional centrado en la armonización de las normativas referentes a la ciberseguridad.

Debido al alto nivel de conexión entre los Estados que genera internet, puede que los usuarios en todo el mundo se vean afectados en algún momento por disponer de este servicio. Por esta razón, brindarle un enfoque regional o internacional podría favorecer y motivar a muchos Estados para que participen en el desarrollo de capacidades de seguridad, prevención y solución de seguridad cibernética, tal como lo hace el Convenio de Budapest.

La habitual falta de disposiciones y soluciones legales en las normativas internas y externas de los países dificulta la cooperación internacional para prevenir, disminuir y solucionar los delitos de fraude. Esta falta de cooperación disminuye la eficacia del trabajo, la obtención de pruebas y el trabajo transfronterizo eficiente. Actualmente, los Estados se ponen trabas y dificultan la resolución de los casos. Lo cual debería ser lo opuesto.

Debido a la falta de acuerdos y convenios internacionales, la mayor parte de los países han legislado en su derecho interno soluciones propias al conflicto de extraterritorialidad. Esto se puede plasmar en posteriores deficiencias en relaciones bilaterales y protección de derechos y garantías de los individuos. Del mismo modo, dificulta la solución veloz y eficaz de casos transfronterizos con jurisdicciones extrañas.

Podría ser una contribución positiva proteger las garantías individuales por medio de la jurisdicción al enfocarse en el lugar de comisión del delito desde el plano territorial y juzgando el hecho con referencia territorial. Si bien sin tratados o relaciones bilaterales puede ser difícil juzgar al actor, esto es beneficioso para la víctima ya que así no se aplican las normas del lugar de alojamiento del sospechoso, donde suele tener beneficios por la laxa normativa. Y, del mismo modo, más sencillo para el perjudicado que suele preferir la justicia más próxima.

Es esencial que se creen mecanismos para acelerar los trámites, desformalizar y eliminar trabas y eficientizar la cooperación internacional. Se deben eliminar fronteras y trámites burocráticos para así alcanzar la transnacionalidad que provee internet. Las autoridades relativas deben trabajar delimitaciones geográfico-políticas para que así exista una comunicación directa entre sistemas de justicia en la que dadas situaciones previstas, con regulación simple y transparente pueda facilitar la obtención de datos y la resolución de procesos.

En síntesis, los países deben trabajar en conjunto para así facilitar, y en algunos casos habilitar, la posibilidad de acceder a datos e información para poder prevenir afectaciones y encontrar soluciones a problemas como la obtención de pruebas, notificaciones, la extradición o la comunicación. De este modo, creemos que se debe facilitar la recolección de información utilizada por medios delictivos a través de mecanismos internacionales de cooperación como tratados internacionales, sean bilaterales o, convenientemente, multilaterales que regulen situaciones en estos casos.

Referencias

AALCC. (2021, diciembre 28). *Estadísticas archivos*. AALCC. Retrieved June 28, 2022, from https://www.cibercrimen.org.ar/category/estadisticas/

Aboso, G. E., & Zapata, M. F. (2006). *Cibercriminalidad y derecho penal* (Montevideo- Buenos Aires ed.). IB d F.

Acurio del Pino, S. (2016). *Delitos informáticos: Generalidades*.

Arocha Vinagre, S. B., & Alicia, G. N. (2017). Ciberdelincuencia: Problemas en la determinación de la jurisdicción y competencia de los tribunales del orden penal. *Universidad de La Laguna*, 1-40.

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

Banco Mundial. (2021, enero 01). *Personas que usan Internet (% de la población)* | *Data*. Banco Mundial - Datos. Retrieved June 29, 2022, from https://datos.bancomundial.org/indicator/IT.NET.USER.ZS

Bischoff, P. (2022, January 25). *Internet Censorship 2022: A Global Map of Internet Restrictions*. Comparitech. Retrieved June 30, 2022, from https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/

Brenner, S. W. (2009). *Cyberthreats: The Emerging Fault Lines of the Nation State*. Oxford University Press.

Brenner, S. W. (2011). Cybercrime: The Investigation, Prosecution, and Defense of a Computer-related Crime. *Carolina Academic Press*, *3*, 15-104.

British Parliament. (2003). *Extradition Act 2003*. Extradition Act 2003. Retrieved June 30, 2022, from https://www.legislation.gov.uk/ukpga/2003/41/section/73

Britz, M. (2013). *Computer Forensics and Cyber Crime: An Introduction*. Pearson.

CALIFORNIA PENAL CODE 2021: Desktop Edition. (2020). WEST GROUP.

Cámara Argentina de Comercio Electrónico, & Kantar. (2021, February 24). *La facturación por comercio electrónico creció 124% en Argentina durante 2020*. El Economista. Retrieved June 28, 2022, from https://eleconomista.com.ar/negocios/la-facturacion-comercio-electronico-crecio-124-argentina-durante-2020-n41557/amp

Carter, R. (2022, May 29). *24 estadísticas y datos de comercio electrónico imprescindibles para 2022*. Findstack. Retrieved June 28, 2022, from https://findstack.com/es/ecommerce-statistics/

Chaves, R. (2022, May 20). *"Estamos en guerra": 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia*. BBC. Retrieved June 28, 2022, from https://www.bbc.com/mundo/noticias-america-latina-61516874

Chawki, M., Darwish, A., Ayoub, M., & Kahn, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer.

Chen, R., Gaia, J., & Rao, R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 1-14.

Código Procesal Penal Federal. (2019). *Código Procesal Penal Federal Argentino*. Infoleg.

Comisión Europea. (n.d.). *EU Global Strategy | EEAS Website*. EEAS. Retrieved June 29, 2022, from https://eeas.europa.eu/topics/eu-global-strategy

Comisión Europea. (2017). *Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE*.

Congreso de la Nación Argentina. (1984 (actualizado)). *Código Penal de la Nación Argentina*.

Congreso de la Nación Argentina. (1993). *Ley N° 24.240: Ley de defensa del consumidor*.

Congreso de la Nación Argentina. (1994). *Constitución de la Nación Argentina*.

Congreso de la Nación Argentina. (1996). *Ley 24.766: Confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos*.

Congreso de la Nación Argentina. (1997). *Ley 24.769: Delitos tributarios. Delitos relativos a los Recursos de la Seguridad Social.*

Congreso de la Nación Argentina. (2000). *Ley 25.326: Datos Personales*.

Congress of the State of California. (2018). *California Consumer Privacy Act*.

Congress of the United States of America. (1985). *Stored Communications Act (SCA)*.

Congress of the United States of America. (1996). *Digital Millennium Copyright Act*.

Congress of the United States of America. (2018). *Clarifying Lawful Overseas Use of Data*.

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia* [Budapest].

Consejo de la Unión Europea. (2005). *Decisión marco relativa a los ataques contra los sistemas de información* [DM 2005/222/JAI]. Diario Oficial de la Unión Europea.

Consejo de la Unión Europea. (2013). *Directive 2013/40/EU: attacks against information systems*.

Consejo de la Unión Europea. (2016). *General Data Protection Regulation*. EUR-Lex. Retrieved June 29, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

Consejo de la Unión Europea. (2017, June 19). *Cyber attacks: EU ready to respond with a range of measures, including sanctions*. Consilium.europa.eu. Retrieved June 29, 2022,

from http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/

Darahuge, M. E., & González, L. A. (2018). Empleo de las direcciones virtuales como elemento fundante en las declaraciones de incompetencia por territorialidad. In *Cibercrimen y Delitos Informáticos* (pp. 183-190). Erreius.

Diario Oficial de la Unión Europea. (2003). *Acuerdo de Extradición entre la Unión Europea y los Estados Unidos de América*.

Díaz Gómez, A. D. (2010). *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*. REDUR.

Diaz, Sergio Dario s/ violación correspondencia medios electo art. 153 2° p. (2014). *Corte Suprema de Justicia de la Nación*.

Emarketer. (2021). *Data and Research on Digital for Business Professionals*. Data and Research on Digital for Business Professionals | Insider Intelligence. Retrieved June 29, 2022, from https://www.emarketer.com/

Estadísticas de Comercio Electrónico. (2022, Marzo 01). Cámara Argentina de Comercio Electrónico. Retrieved June 28, 2022, from https://www.cace.org.ar/estadisticas

European Commission. (2015). *The European Agenda on Security*.

Fernández Delpech, H. (2014). *Manual de Derecho Informático*. Abeledoperrot.

Ferreyra, E. (2018). *La Convención de Cibercrimen de Budapest y América Latina*.

G.R. y otro s/procesamientos. (2010). *Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, Sala VI* [Cita digital IUSJU184903D].

Gutiérrez Francez, M. (2005). Reflexiones sobre la ciberdelincuencia hoy. *Universidad de Salamanca*, *1*(1), 1-24.

Hanus, B. (2014). The impact of information security awareness on compliance with information security policies: a phishing perspective. *University of North Texas*, 1-24.

Holt, T., Bossler, A., & Kathryn, S.-S. (2017). *Cybercrime and Digital Forensics*. Routledge.

Holt, T. J., & Bossler, A. M. (2017). *Cybercrime in Progress: Theory and Prevention of Technology-enabled Offenses*. Routledge Taylor & Francis Group.

INTERPOL. (2020). *Ciberdelincuencia: Efectos de la COVID-19*.

Int'l Shoe Co. v. Washington. (1945). *U.S Supreme Court*.

ISOC, I. S. (2018). Internet y los efectos extraterritoriales de las leyes. *Internet Society (ISOC)*, *1*(1), 1-26.

Kaspersen, H. (2009, marzo 5). *Cybercrime and internet Jurisdiction*. Consejo de Europa. Retrieved June 28, 2022, from https://rm.coe.int/16803042b7

Kohl, U. (2007). *Jurisdiction and the Internet: Regulatory Competence Over Online Activity*. Cambridge University Press.

Koops, B.-J. (2011). Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice. *SCRIPTed*, *8*(3), 229-256.

López-Lapuente, L. (2019). La aplicación extraterritorial del reglamento general de protección de datos. *Actualidad Jurídica Uría Menéndez*, (52), 136-140.

Lynch, J. (2005). Identity Theft in Cyberspace: Crime Control Methods and their effectiveness in combating phishing attacks. *CyberLaw*.

Magliona Markovicth, C. P. (1999). *Delincuencia y fraude informático: derecho comparado y Ley no. 19.223*. Editorial Jurídica de Chile.

Martinez, M. S. (2018). Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil. In *Cibercrimen y delitos informáticos* (pp. 33-48). Erreius.

Microsoft. (2022, s.f s.f). *Protéjase del phishing*. Microsoft Support. Retrieved June 28, 2022, from https://support.microsoft.com/es-es/windows/prot%C3%A9jase-del-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44

Ministerio de Asuntos Exteriores. (2001). *Convenio sobre la ciberdelincuencia*. Consejo de Europa.

Ministerio de Asuntos Exteriores, España. (2005). *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba*. Consejo de Europa.

Ordoñez, C. (2019). Conflicto de Competencia. Nuevas Tecnologías. Jurisprudencia te. *Instituto Argentino de Derecho Procesal*.

Palazzi, P. (2017). Revista Derecho y Nuevas Tecnologías. *RDYNT*, *1*(1), 1-378.

Palazzi, P. A. (2008). Análisis de la ley 26.388 de reforma del Código Penal en materia de delitos informáticos. *Revista de Derecho Penal y Procesal Penal*, 1212-1224.

Palazzi, P. A. (2016). *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388*.

Parada, R. A., & Errecaborde, J. (2018). *Cibercrimen y delitos informáticos*. Erreius.

Parlamento Europeo y del Consejo. (2000). *DIRECTIVA 2000/31/CE*.

Parlamento Europeo y del Consejo. (2016). *Reglamento (UE) 2016/679*.

Petrone, D., Basso, M., & Emiliozzi, A. (2021). Phishing Attacks: Problemáticas de su recepción en el ordenamiento local y nuevos desafíos. In *CIBERCRIMEN: Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet* (pp. 277-290). Faira J.

Purkait, S. (2015). Examining the effectiveness of phishing filters against DNS based phishing attacks. *Information & Computer Security*, *23*(3), 333-346.

P. y otros s/defraudación. (2015). *Cámara Federal de Casación Penal. Sala III* [Cita digital IUSJU001828E].

Roble, M. R. (2014). *Código Civil y Comercial de la Nación*. D - Ministerio de Justicia y Derechos Humanos de la Nación.

Roca de Estrada, P. (2001, s.f s.f). *Delito informático, virus y legislación*. SAIJ. Retrieved June 28, 2022, from http://www.saij.gob.ar/doctrina/dacf010038-roca_de_estrada-delito_informatico_virus_legislacion.htm?bsrc=ci

Russo, Christian Carlos y otro s/ infracción art. 183 del Código Penal - incidente de competencia. (2015). *Corte Suprema de Justicia de la Nación* [2358].

Salt, M. (2021). Obtención de pruebas informáticas en extraña jurisdicción: Los conflictos del principio de territorialidad en un mundo virtual sin fronteras. In *CIBERCRIMEN: Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de Servicios de Internet* (pp. 517-546). Faira J.

Smyth. (2007). *Mind the gap: a new model for internet child pornography regulation in Canada*.

Sponele, J. (2010, Agosto 31). *Cloud Computing and Cybercrime Investigations: Territoriality vs the ower of disposal?* Il Consiglio d'Europa. Retrieved June 28, 2022, from http://www.coe.int/cybercrime

Supreme Court of Canada. (2017, June 30). *Supreme Court of Canada upholds global search engine de-indexing decision: Five implications for internet intermediaries*. Osler, Hoskin & Harcourt LLP. Retrieved June 28, 2022, from https://www.osler.com/en/resources/regulations/2017/supreme-court-of-canada-upholds-global-search-engi

Torello, V. S. (2015). La incorporación de normas de derecho informático en el nuevo Código Civil y Comercial y sus proyecciones en los procedimientos judiciales. *Sistema Argentino de Información Jurídica*, 1-39.

United Nations. (2007). *Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales*. Naciones Unidas.

United Nations. (2011). *Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías*. Naciones Unidas.

United States of America v. Aleksey Vladimirovich IVANOV, a/k/a Alexey Ivanov, a/k/a "subbsta". (2001). *U.S. District Court for the District of Connecticut*.

United States v. Microsoft Corp. (2015). *United States Court of Appeals*.

Van Der Sar, E. (2017, Noviembre 22). *Sci-Hub Loses Domain Names, But Remains Resilient*. Torrentfreak. Retrieved June 28, 2022, from https://torrentfreak.com/sci-hub-loses-domain-names-but-remains-resilient-171122/.

Villanueva, N. (2019). *Smart Contracts: Desafíos para su adopción*. Universidad de San Andrés.

Wang, F. F. (2010). *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China*. Cambridge University Press.