Robo de Identidad y su Incidencia en el Cibercrimen

Abog. Pedro Zarate[1,2], Mg. Abog. Maria del Carmen Becerra[2]

[1] Instituto de Informática – FCEFN-UNSJ.
[2]Departamento de Informática FCEFN-UNSJ.

Abstract- En este trabajo se abordan los delitos cibernéticos, con énfasis en el robo de identidad, se analizan las implicancias de la falta de tipificación de este tipo de conducta disvaliosa en nuestro país y el aumento de los delitos cibernéticos ocurridos en el ciberespacio. Se afirma hoy más que nunca, que es urgente que nuestro país tenga participación activa en la lucha contra la ciberdelincuencia mundial adecuando su legislación penal en materia de robo de identidad para combatir las amenazas y crímenes en el ciberespacio. Después de la firma de adhesión al Tratado de Budapest, Argentina se comprometió con una cooperación internacional mediante la implementación de una legislación relevante y la adopción de métodos estratégicos que respalden la efectividad del trabajo realizado para la obtención de justicia penal a nivel nacional y la cooperación internacional entre los Estados.

Keywords: **Delitos Cibernéticos. Identidad Digital. Robo de Identidad. Cibercrimen**

1 Introducción

El aumento del número de incidentes de delitos cibernéticos, facilitados por el robo de identidad se ha generalizado en muchas partes del mundo. En nuestro país conforme las estadísticas publicadas por la Asociación Argentina de Lucha contra el Ciber Crimen(AALCC), el robo de datos ha crecido en forma exponencial [1].
Esta investigación se centra en las acciones delictivas en el ciberespacio destacados en el "Informe de Riesgos Globales 2021" como uno de los principales problemas a afrontar en la próxima década [2]. Durante estos periodos de pandemia, los llamados ciberdelincuentes avanzaron a pasos agigantados desarrollando técnicas y métodos que vulneran los sistemas de seguridad organizacionales, aún inmaduros, lo que les permite tomar ventaja sobre las autoridades y su escasa preparación para abordar este nuevo problema.

El desarrollo en las sociedades modernas, la evolución tecnológica, la globalización y con ello la especialización en las TIC's, ofrecen a los ciberdelincuentes un espacio intangible donde pueden violar absolutamente todos los derechos de una persona en forma casi invisible. En ese contexto se encuentran comprometidos una triada importante de derechos fundamentales en peligro. Se trata de la dignidad, la identidad y la intimidad. La dignidad se posiciona en el sistema jurídico argentino actual como la fuente, el fundamento y el sustrato, en el que se asientan y de la que derivan todos los derechos humanos.

Se parte, como idea clave, del concepto de identidad digital y se analizan, entre otras, las definiciones de Ciberdelitos y Robo de Identidad. Posteriormente, se trata de

adfa, p. 1, 2011.

conocer la reacción y líneas de acción de naciones y organizaciones, con especial referencia a nuestro país. Para ello se trabaja con estadísticas, para determinar el crecimiento de los ciberdelitos y se emplea un método del pensamiento lógico con un fin cognitivo desarrollando conceptos e intelecciones asociados a los mismos. Su propósito esencial fue la reconstrucción del núcleo teórico sobre el tema investigado, recurriendo a fuentes primarias como la legislación aplicable y la jurisprudencia, secundarias como ser la doctrina elaborada sobre el fenómeno y sobre los derechos fundamentales vulnerados, y terciarias como ser manuales de derecho penal y constitucional.

Como tentativa de hipótesis se puede sostener que la cooperación internacional en materia de ciberseguridad se ve expuesta en nuestro país, ante el alto riesgo que significa el aumento de los ciberdelitos y la falta de tipificación del robo o uso indebido de la identidad digital, que no se encuentra regulado en el derecho penal argentino, provocando un vacío legal al respecto que deja al descubierto la garantía de defensa de derechos fundamentales como son: la dignidad, la identidad y la privacidad.

2 Delitos Cibernéticos

Como lo afirma Temperini, cuando referimos al cibercrimen, estamos hablando de una serie de delitos informáticos que ocurren de una forma más profesional, organizada, sin motivaciones personales más que las económicas, donde los sujetos pasivos de los delitos son elementos fungibles y sin interés para el ciberdelincuente, que busca optimizar sus ganancias a través del perfeccionamiento de distintas técnicas delictivas que utilizan a la tecnología como eje. Si bien es posible encontrar ciberdelincuentes especializados que trabajan de forma independiente, es mucho más común encontrarlos organizados en bandas, con una clara distribución de tareas [3].

En cuanto al alcance de la definición de "delito cibernético" a efectos de cooperación internacional, los países deberían tipificar como delito los actos de ciberdelincuencia en grado suficiente, de modo que quedaran comprendidos no solo los delitos basados en la cibernética, sino también otros delitos que con frecuencia se cometen utilizando internet y medios electrónicos, como el fraude cibernético, el robo cibernético, la extorsión, el blanqueo de dinero, el tráfico de drogas y armas, la pornografía infantil y actividades terroristas[4]. Más aún, que dichos delitos resulten en juicio es todavía un reto mayor. Parte del problema se inicia muchas veces en la propia ley: en un tercio de los países no existe un marco legal sobre los delitos informáticos y pocos países de la región se han adherido a la Convención de Budapest, que promueve la cooperación internacional en la lucha contra el crimen informático. Para un delito que no conoce fronteras, trabajar de la mano con otros países es un factor indispensable para el éxito. La Convención obliga a los Estados firmantes a que incluyan en sus legislaciones penales la figura del robo de identidad o como lo denomina la misma Convención "falsificación informática" determinando que será a criterio de los legisladores la exigencia del dolo fraudulento o delictivo similar. La profesionalización y proliferación de la ciberdelincuencia supone un coste anual enorme en daños que sufren personas, empresas e incluso gobiernos. Los expertos estiman que los daños por culpa de la ciberdelincuencia alcanzarán los 6 billones de USD anuales para 2021, lo que la convierte en una de las actividades ilegales más lucrativas[5].

Durante los últimos años se han tomado numerosas medidas para implementar políticas y realizar cambios administrativos y regulatorios para los sectores de telecomunicaciones, internet y tecnología en Argentina. En 2017, el Decreto 577/2017 creó el "Comité de Ciberseguridad" en la órbita del entonces Ministerio de Modernización y con representantes del Ministerio de Defensa y el Ministerio de Seguridad con el objetivo de desarrollar una estrategia nacional de seguridad cibernética.

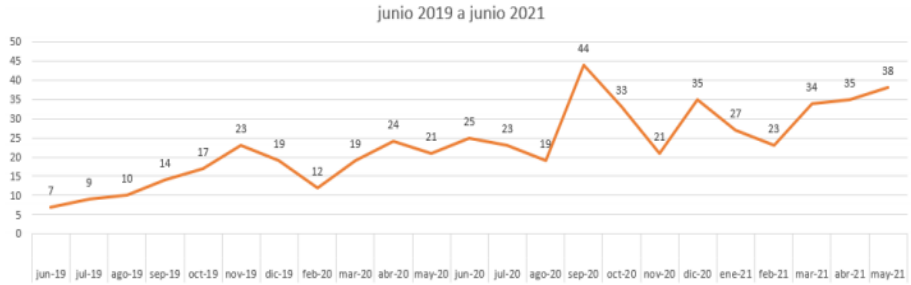
La Estrategia Nacional de Ciberseguridad se aprobó mediante la resolución publicada en el Boletín Oficial (829/2019) y se creó la Unidad Ejecutora, en el marco del Comité de Ciberseguridad y bajo la autoridad de la Secretaría de Modernización de la Nación e invitó a las Provincias y Ciudad Autónoma de Buenos Aires para adherirse a la Estrategia. A través de un préstamo basado en políticas (policy-based loan o PBL, por sus siglas en inglés) aprobado en 2019, el BID brinda su apoyo al gobierno argentino en la implementación de políticas relacionadas con infraestructura crítica, seguridad de los datos personales y buenas prácticas en el uso de las TIC, con acciones puntuales hacia el fortalecimiento de las capacidades nacionales en ciberseguridad. Además, para fortalecer los lazos internacionales y sus políticas de seguridad cibernética, Argentina se asoció con Estados Unidos para establecer un grupo de trabajo que mejorará la cooperación en materia de seguridad cibernética.

Asimismo, se han firmado acuerdos con España y Chile, y se encuentran bajo análisis memorandos de entendimiento con China, República de Corea y Rusia. Argentina también ha establecido un Programa Nacional de Infraestructura de Información Crítica y Ciberseguridad (ICIC), bajo la Resolución JGM N° 580/2011, para crear y adoptar un marco regulatorio orientado a definir y proteger la infraestructura estratégica y crítica de los sectores público y privado, así como organizaciones interjurisdiccionales. Aunque ICIC colabora con el sector privado, un informe de la empresa PwC encontró que el 53% de las empresas encuestadas en Argentina no tiene una estrategia general de seguridad de la información, el 61% no tiene un plan de contingencia sobre cómo responder frente a un incidente y solo el 46% cuenta con un programa de seguridad para los empleados[6].

En cuanto a la legislación, Argentina promulgó la Ley Nº 26.388 en 2008, que modificó el código penal para incluir el delito cibernético. Además, la Ley Nº 26.904 incorpora la figura del grooming en el Código Penal. Por otra parte, la adhesión de Argentina al Convenio de Budapest sobre Ciberdelincuencia del Consejo de Europa fue ratificada en junio de 2018. En mayo del corriente año, se aprobó el proyecto del 2do Protocolo Adicional del citado Convenio, que tiene por objeto afianzar los lazos en materia de cooperación internacional y facilitar la obtención de evidencia electrónica para poder brindar una respuesta eficaz en la investigación criminal para trabajar contra el ciberdelito. El proyecto del texto fue aprobado por consenso de los Estados partes y comienza así el proceso hasta su plena vigencia. Entre otros puntos, la Delegación Argentina expresó en su intervención que "Para prevenir y perseguir el delito cibernético es fundamental contar con mecanismos e instrumentos adecuados que permitan y faciliten la cooperación y asistencia internacional" [7].

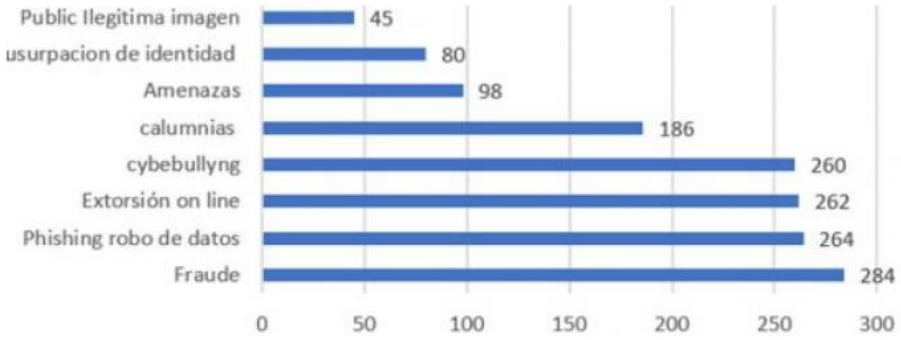
Argentina también tiene la Ley Nº 25.326 del año 2000 que cubre la protección de datos personales. De hecho, ha sido uno de los primeros países de las Américas en tener un marco regulatorio para la protección de datos personales, y lo ha fortalecido y actualizado desde entonces. Y es uno de los pocos países de las Américas que participa

en el "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" del Consejo de Europa (CdE).
En 2018 se remitió un proyecto de Ley modificatorio de la Ley Nº 25.326 del año 2000 enfocado en actualizar el marco normativo vigente. Argentina tiene dos decretos sobre gobierno electrónico. El Decreto Nº 378/2005 describe la estrategia de gobierno electrónico para aumentar las TIC a fin de mejorar la entrega y prestación de servicios gubernamentales. El segundo y más reciente es el Decreto Nº 87/2017 para la creación de una plataforma digital orientada a facilitar la interacción entre las personas y el Estado. El Decreto Nº 996/2018 ha creado la "Agenda Digital Argentina", la cual tiene entre sus objetivos "desarrollar capacidades en ciberseguridad para generar confianza en los entornos digitales".
Según la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC) los delitos informáticos extorsiones, sextorsiones, estafas y ransomware se dispararon en el país a partir del año 2020 y aumentaron un 60%. El 51,62% de los delitos consultados a la AALCC corresponden a finalidades económicas. Las consultas en el transcurso del 2021 (periodo en análisis 1/1/2021 al 5/6/2021) se incrementaron un 65% en comparación al mismo periodo de año 2020 , dejando constancia que la tendencia creciente de estafas on line – principalmente instrumentos financieros – comenzó a finales de 2019 y continuo su marcha ascendente hasta estos días, tal cual lo muestra el Gráf.1 [8].



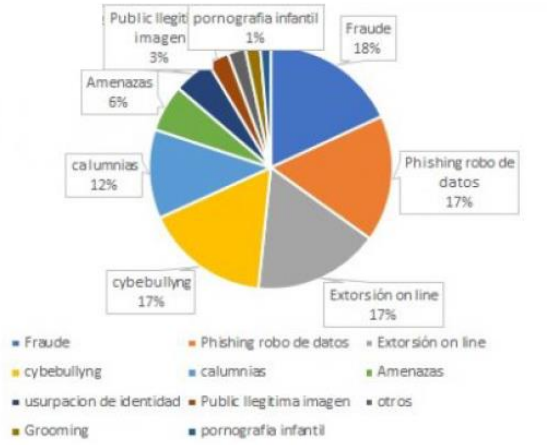
Graf. 1. Medición según Tipologías penales (Fuente AALCC)

En el Gráf. 2, el periodo en análisis desde el 1 de enero de 2020 al 21 de diciembre de 2020, se observa un considerable incremento en reglas generales de los delitos respecto al 2019, especialmente delitos configurables a través de internet con objetivos económicos : Robo de datos, extorsión, estafas .



Graf. 2. Medición según Tipologías penales (Fuente AALCC)

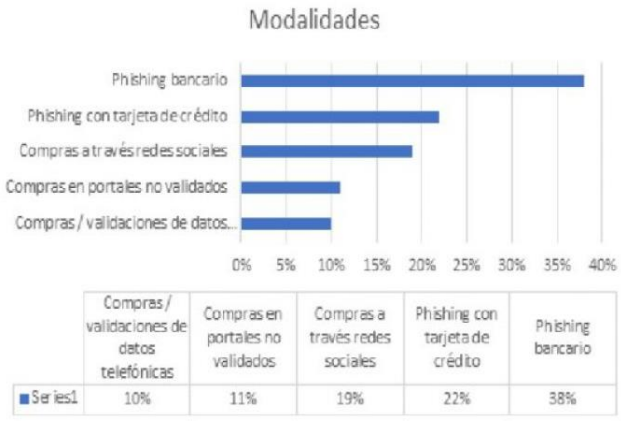
En el Graf. 3 se observa la distribución porcentual de los ciberdelitos en 2020, de los cuales podemos indicar que el fraude informático (65,7%) es el principal delito cometido en la actualidad, seguido de las amenazas y coacciones (19,1%) y la falsificación informática (3,8%). Existe un considerable incremento en estos tipos de delito.



Graf. 3. Estadísticas año 2020 completo (Fuente AALCC)

Como se muestra en el Graf. 4, el robo de datos ha aumentado en forma inimaginable en las últimas décadas. El ciberespacio esquematiza la zona donde tiene lugar esta interconexión entre computadores y personas sin límites fronterizos ni temporales, y donde se ejecutan una serie de fenómenos de la comunicación que se asientan cada día más en nuestra vida diaria. Una de las prácticas informáticas deshonestas más comunes es el robo o suplantación de identidad, conocida como phishing [9]. Si bien el fraude bancario a través de la modalidad phishing – robo de datos –, también se reportaron robo de información a través de falsos perfiles de WhatsApp – utilizado logos de entidades- y llamadas telefónicas cuyo objetivo era obtener información de la víctima

para acceder al home banking y perpetrar el delito autopréstamos y transferencia a terceros también han estado entre las modalidades principales [10].



Graf. 4. Estadísticas año 2020 completo (Fuente AALCC)

3 Identidad Digital

La identidad configura un conjunto de características que son propias de una persona y que la distingue del resto. Abarca diversas aristas: datos estáticos y dinámicos de la vida de una persona. Es una cantidad de información que hacen a una persona ser lo que es y no otra. Hace a su esencia. Proteger a la identidad se vincula con la dignidad misma de las personas humanas y con su ámbito de privacidad. Esos derechos personalísimos fundamentales se ven afectados y lesionados cuando se utiliza la información de una persona a través de sistemas digitales con fines contrarios a la ley. Sin embargo, la problemática del derecho penal argentino es que se encuentra limitado para dar respuestas a la gravedad del asunto brindando soluciones eficaces en el ámbito civil y no así a través del derecho penal. El Código Penal de La Nación Argentina no contempla la figura del robo de identidad digital por ello es importante aclarar los conceptos y diferenciar el robo de la apropiación indebida

En principio se debe aclarar que la identidad es un derecho personalísimo y como tal es un bien jurídico tutelado por las Convenciones Internacionales de Derechos Humanos de las cuales la Argentina es parte y le otorga jerarquía constitucional. La identidad digital es una manifestación de la identidad en la "vida virtual", en el ciberespacio. De allí la relevancia de poner de manifiesto que el bien jurídico tutelado en este tipo delictivo es la identidad y por lo tanto la dignidad e intimidad. El mundo maneja la información a través de la informática y las bases de datos informáticas. El espacio físico que contenía información fue absorbido totalmente por los softwares. La globalización y la circulación y el flujo comercial lograron que necesariamente tengamos que utilizar la informática e insertar en sitios virtuales nuestra información de identidad [11].

Sessarego, sostiene que: La identidad de la persona, en tanto inescindible unidad psicosomática, presupone un complejo de elementos, una multiplicidad de aspectos esencialmente vinculados entre sí de los cuales unos son de carácter

predominantemente físico o somático, mientras que otros son de diversa índole, ya sea ésta psicológica, espiritual, cultural, ideológica, religiosa o política. Estos múltiples elementos son los que, en conjunto, perfilan el ser 'uno mismo', diferente a los demás, no obstante que todos los seres humanos son iguales [12].

La identidad comprende un conjunto de elementos estáticos y dinámicos. Digitalmente ese conjunto conforma una masa de datos. Datos denominados en la Ley de Protección de Datos Personales (en adelante LPDP) en sus dos variantes [13]:

a) Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

b) Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

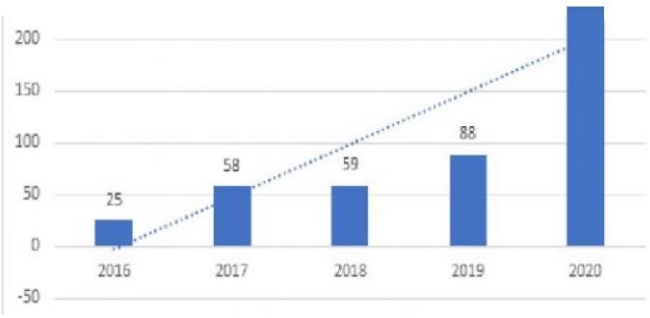
Ni la doctrina penal ni el Proyecto de Ley de Robo de Identidad Digital, como así tampoco sus fundamentos aclaran que se debe entender y cuál es el contenido del término identidad [14]. La jurisprudencia le da la relevancia que merece al decir que "Pocos derechos humanos pueden ser más dignos de protección que el de (...) conocer la identidad, reconocer sus raíces..." y tal derecho "debe prevalecer sobre otros bienes jurídicos de menor jerarquía". Y afirma que: En el marco de la teoría de la integralidad de los derechos humanos, un principio orientador es el de la norma más favorable a la persona, más conocido como el principio "pro hominis". Es en este contexto donde el derecho a la identidad ha adquirido y desarrollado su autonomía, cabiéndole una construcción propia. Si se asume que cada ser humano es único e irrepetible, la identidad es la condición de nuestra particularidad, de nuestro ser concreto en el mundo. Así por medio del derecho a la identidad, se protege la vida humana en su realidad radical que es la propia persona en sí, indivisible, individual y digna.

La identidad que se manifiesta en el mundo virtual, a través de datos en sus diversas formas, como informativos o sensibles, debe ser protegida como bien jurídico. La legislación argentina si bien protege a la misma, lo hace vinculándola a otros bienes jurídicos como la seguridad jurídica o la integridad personal con tipos penales propios de cada una de ellas, pero no como bien jurídico autónomo. En el ámbito civil, la LPDP delinea de modo minucioso el tratamiento que deben tener los datos personales en el ciberespacio, pero de la legislación penal no surge un tipo específico que sancione al autor que usurpe, robe o utilice de cualquier modo o con cualquier fin la identidad ajena. La sola acción de utilizar la identidad ajena debería configurar un delito en sí.

La identidad digital debe ser definida desde el lenguaje informático. Ella se va construyendo a partir de la propia actividad e interactividad con los demás en internet. Los especialistas en análisis de sistemas dicen que la identidad digital "somos nosotros en Internet", en el ámbito de las nuevas tecnologías comprende toda información que compartimos y todo lo relacionado a nosotros que existe en Internet. Por ejemplo, la interacción con blogs y redes sociales, publicaciones, fotos, videos, comentarios, etiquetas por parte de otras personas, información en formularios on line, son las que establecen un conjunto de información que nos define en la red [15].

Por lo tanto, la utilización de uno solo de nuestros datos, sea cual fuere, es parte de nuestra identidad digital, con ello se quiere especificar que no solamente con la utilización del nombre y apellido o el número de documento nacional de identidad nos estarían usurpando o robando la identidad. El uso para cualquier fin de cualquier dato

referido a nuestra persona es ilícito. La utilización de los datos incorporados a los bancos de datos, las informaciones financieras y bancarias, las claves de las distintas cuentas abiertas en distintas páginas web, sin autorización previa de su titular configura el delito de robo de identidad. En el Graf. 5 se observa un incremento masivo de "correos trampa" con el objetivo de engañar al usuario y que este voluntariamente remita información sensible . El criminal o las organizaciones criminales utilizaran esta información con tres objetivos principales : Extorsión , fraude o venta de información en el mercado negro [16].



Graf. 5. Robo de Datos (Fuente AALCC)

Capurro nos habla de una identidad propia a partir de la interrelacionen con el mundo [17]. Por ello el contenido de la identidad digital es amplísimo e incluye hasta el dato más insignificante referido a nuestra persona, y el alcance de la misma se circunscribe al ciberespacio, al mundo virtual o sociedad de la información. La mayoría de las veces, la utilización de la identidad de otra persona, ajena, es una herramienta para cometer otros delitos como fraudes, estafas, calumnias, injurias, robo, grooming, phishing, etc.

4 Robo de Identidad como riesgo global

El robo es un tema muy relevante, a través de él los delincuentes utilizan datos personales para hacerse pasar por el individuo al que le han robado su identidad. Estos robos, en combinación con el anonimato de las transacciones en línea y otras actividades, se utilizan para cometer una serie de delitos que comprenden desde el fraude hasta las actividades terroristas. Dentro de esta modalidad se encuentra el fraude bancario, la extorsión en línea, el blanqueo de dinero y el contrabando con ayuda de computadoras y los delitos contra sistemas de computación y sus usuarios, con utilización de virus y otros programas hostiles, así como ataques de denegación de servicios.

El robo de la identidad digital, tanto en Internet como en redes sociales, se produce o bien suplantando la identidad digital de un usuario de Internet y redes sociales, o robando sus claves y contraseñas para acceso a las mismas, con fines generalmente, delictivos, siendo delito en sí mismo el robo o la suplantación de la identidad en Internet. Al respecto, puede afirmarse que no existe un único y homogéneo concepto de Robo de Identidad, sin embargo, de todas las conceptualizaciones existentes, pueden observarse determinados elementos comunes. En términos generales el robo de

identidad tiene lugar cuando una persona utiliza la información personal de otro individuo para realizar compras, solicitar préstamos, obtener un trabajo; en definitiva: hacerse pasar por alguien que realmente no es [18].

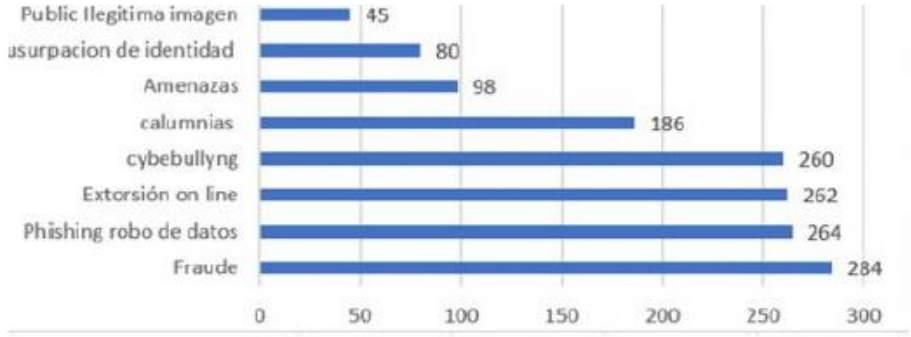
Como mencionábamos anteriormente, la identidad digital es una manifestación de la identidad en la vida virtual en el ciberespacio. De allí la relevancia de poner de manifiesto que el bien jurídico tutelado en este tipo delictivo es la identidad y por lo tanto la dignidad e intimidad. El robo de identidad puede ocurrir de diversas maneras, aunque los elementos básicos y la finalidad son los mismos: la obtención de información personal para realizar algún tipo de perjuicio. Para analizar estas actividades es importante destacar la diferencia entre el robo de identidad y la impersonalizarían, que sucede simplemente cuando alguien se hace pasar por otra persona u organización [19].

La distinción en la mayoría de las legislaciones que ya tipifican el robo de identidad digital es solo a los fines de la cuantificación de la pena, ya que la sola impersonalizarían es considerada en si un delito. Para poder determinar la existencia del delito se deben analizar los elementos posibles del tipo penal. En el derecho comparado algunas legislaciones como EE. UU., Canadá o México ya se legisló el robo de identidad se ofrecen varias propuestas de denominación: usurpación de la identidad, suplantación de identidad, falsificación de identidad y su uso indebido, el robo o apropiación indebida de identidad. Se ha tipificado a la figura como: “la obtención y posesión de información de la identidad de una persona con la intención de engañarla o realizar actos deshonestos o fraudulentos en su nombre”. El tráfico de identidades, según este país, es un delito en el cual se “transfiere o vende información a otra persona con conocimiento o por imprudencia y cuyo fin es la posible utilización criminal de dicha información. EE. UU., a nivel federal lo define como el que “a sabiendas, posea, transfiera o use, sin autoridad legal, un medio de identificación de otra persona con la intención de cometer, ayudar o instigar, cualquier tipo de actividad ilegal”.

El robo de identidad digital ha sido definido de varias maneras en la legislación comparada: apropiación indebida de identidad digital, aprehensión ilegitima de identidad digital, usurpación de identidad digital y la más aceptada es la suplantación de identidad digital. Sin embargo, existe una diferencia entre usurpación o suplantación de identidad y robo de identidad. La suplantación de identidad digital podría definirse también como un delito informático que, puede realizarse con múltiples fines, con mayor o menor gravedad y trascendencia. La suplantación de identidad suele ser realizada por la creación de un perfil falso, pero con la identidad de otra persona a la que se pretende suplantar. El robo de identidad se produce cuando el que suplanta la identidad lo realiza por haber sustraído los datos de acceso a Internet y redes sociales. En ambos casos la gravedad del hecho es el mismo, la suplantación de identidad de otra persona, con fines presumiblemente delictivos [20].

Al robo de identidad, se le da el carácter jurídico como una forma de fraude, destinado a acceder a recursos u obtener crédito u otros beneficios, mediante lo cual una persona asume la identidad de otra persona. El término robo de identidad, en realidad, no es del todo correcto; de hecho, no es posible robar literalmente una identidad como tal, sino que sólo se puede usar. La víctima del robo de identidad puede sufrir consecuencias muy negativas si se le considera responsable de las acciones cometidas por el usurpador. Las organizaciones e individuos que han sido engañados o defraudados por

ladrones de identidad pueden sufrir consecuencias y pérdidas considerables en el sentido material y psicológico [21].
No se puede ocultar, con cierta perplejidad, acerca de la hipótesis de "uso" la identidad humana de otras personas, en paralelo con la oportunidad de "robar". Después de todo, lo que aparece es de forma única el intento legislativo a una "materialización" de la identidad personal en la red y, por lo tanto, la necesidad de que el intérprete para traducir la identidad de alguna entidad definida, tales como datos personales, destinados como formas preferidas con las cuales los sujetos se proyectan de manera voluntaria al mundo digital [22].
El adoptar, crear o apropiarse de una identidad en internet si bien consideramos que debería ser de un delito autónomo también consideramos a esta acción dolosa como "el puente a decenas de delitos" en donde el autor busca impunidad desde el anonimato supuesto. Una de las problemáticas asociadas a la protección de datos que más recibió el Centro de Ciberseguridad del Gobierno de la Ciudad de Buenos Aires es la de la suplantación de identidad. Durante 2020, se reportaron 102 incidentes de este tipo.



Graf. 6. Estadísticas de Casos año 2020 completo (Fuente AALCC)

Dentro de los casos más reportados en CABA en relación a la suplantación de identidad se destacan estas modalidades: 1. Publicación de imágenes íntimas y datos personales - como el número de celular- sin el consentimiento de la víctima, tanto en sitios web pornográficos como en perfiles falsos creados. 2. Creación de identidades falsas utilizando datos personales de la víctima para solicitar productos financieros en su nombre.
A su vez, durante 2020, el Centro recibió 190 consultas por casos de phishing, lo cual implica un aumento del 143% respecto al año anterior. Se destacan las campañas en las que se engaña a los usuarios mediante una comunicación de "carácter urgente", es decir, donde que requieren una acción inmediata para evitar una supuesta consecuencia negativa. Se les dice que deben renovar la contraseña, aceptar algunas condiciones o actualizar datos, por ejemplo, y de esa manera logran obtener las credenciales de acceso a cuentas bancarias, en redes sociales o correos. El año pasado se reportaron 19 casos de fraudes, lo cual implica un incremento del 35% respecto del año anterior. Dentro de los incidentes recibidos se destacan las estafas bancarias en los que se crearon cuentas falsas de redes sociales de entidades bancarias, por ejemplo y los accesos indebidos a datos o cuentas personales. En relación a esta problemática, los casos que sí tuvieron

un crecimiento exponencial son los relativos a publicidad engañosa y estafas digitales. En ese sentido, se pasó de 7 casos en 2019 a 138 en 2020. El uso de las tecnologías informáticas, las páginas web, las redes sociales, los medios de comunicación electrónicos, los bancos de datos informáticos crean un espacio virtual en el cual se acumula información personal y financiera que las personas mismas proporcionan, sin tener la debida consciencia de la relevancia de brindar cierto tipo de información, y de la mala utilización de los medios informáticos. En ese contexto las personas constantemente son víctimas de formas de delinquir muy avanzadas para el derecho penal. El ordenamiento jurídico argentino regula la protección de los datos personales, pero no lo hace a través de una sanción penal. La ley especial N° 25.326 denominada "Protección de los datos personales" garantiza la protección a través del ejercicio de la acción expedita de habeas data contemplada en el art. 43 de la Constitución Nacional (en adelante CN), pero de ningún modo la acción dañina de robar o usar indebidamente la identidad (usurpar) de otra persona, configura un delito propiamente dicho que este tipificado y penado en la legislación nacional. El uso de las TIC's (tecnologías de la comunicación y de la información) es inevitable en nuestro siglo, pero de ello deriva la utilización responsable de las mismas. En nuestro derecho nacional no hay regulación de las mismas, siendo algunas leyes especiales las que de manera obsoleta regulan algunas cuestiones como las analizadas. El Código Penal de la Nación Argentina (en adelante CPN) contempla varias figuras de delitos informáticos, pero no contiene un tipo penal de robo o uso indebido de identidad. El robo de identidad digital ha sido definido de varias maneras en la legislación comparada: apropiación indebida de identidad digital, aprehensión ilegitima de identidad digital, usurpación de identidad digital y la más aceptada es la suplantación de identidad digital. El número de casos en los que se reportó robo de identidad en los Estados Unidos se duplicó en 2020 en comparación con el año previo, dijo la Comisión Federal de Comercio (FTC, por sus siglas en inglés). En una publicación que marca el inicio de la Semana de Concientización sobre el Robo de Identidad en Estados Unidos, la FTC dijo que recibió aproximadamente 1.4 millones de reportes de casos de robo de identidad el año pasado[23]. Este aumento en los casos se debe principalmente a que los ciberdelincuentes que apuntan a personas que se han visto afectadas financieramente por la pandemia de COVID-19-.

El Comité del Convenio sobre la Ciberdelincuencia (Cybercrime Convention Committee), denominado oficialmente por la sigla T-CY, es el órgano que sirve de consulta entre las Partes, y que tiene por misión facilitar la utilización y aplicación efectiva del tratado, intercambiar información, y estudiar la posibilidad de enmendar o ampliar el acuerdo, según lo establecido en el Artículo 46° de la Convención. Entre las principales funciones que cumple el T-CY se encuentra evaluar la aplicación del Convenio, adoptar opiniones y recomendaciones respecto de su implementación, revisar el funcionamiento del Punto de Contacto 24/7, y promover la adhesión al tratado (Cybercrimen Convention Committee, 2016). Al respecto, el T-CY ha desarrollado un Plan de Acción desde el año 2012, que a la fecha entre sus mayores logros alcanzados ha adoptado ocho Notas Guías (Guidance Notes) que representan un común entendimiento entre las Partes referido a la actualización y precisión de la terminología utilizada en el Convenio sobre los siguientes temas: sistema informático (computer system), robot informático (botnets), ataques de denegación de servicio (Distributed Denial of Service DDoS attacks), robo de identidad y phishing relativo a fraudes

(identity thefts), ataques a infraestructura de información crítica, nuevas formas de software maligno o malware, acceso trasfronterizo a datos (Artículo 32°), y correo basura o spam (Cybercrime Convention Committee, 2014). De acuerdo a las Guidance Notes, la apropiación indebida de una característica de la identidad personal (nombre, fecha de nacimiento o dirección) sin consentimiento previo, con motivo de obtener bienes o servicios a nombre de esa persona, es un tipo de fraude que se puede realizar mediante actividades de phishing, pharming, spear phising o spoofing, conductas a través de las cuales se intenta acceder a contraseñas u otras credenciales restringidas por medio de correos electrónicos o sitios web falsos[24].

La convergencia de las tecnologías de la información con la tecnología operativa y los sistemas heredados ya plantea grandes desafíos en todo el ecosistema digital. La aparición de nuevas tecnologías y sus aplicaciones, tales como inteligencia artificial, big data, redes de quinta generación, computación en la nube, IoT y computación cuántica, cuestionan drásticamente nuestro pensamiento convencional sobre el futuro de la economía digital. Por un lado, ofrecen inmensas oportunidades de eficiencia e innovación, pero también amplifican la superficie de ataque y pueden crear riesgos de seguridad y privacidad de datos todavía desconocidos. Por esta razón, las empresas y los gobiernos deben trabajar juntos para desarrollar una comprensión sólida de los riesgos emergentes de ciberseguridad relacionados desde una perspectiva de políticas, de los riesgos y de las operaciones. y descentralizada, versus el enfoque en la "cibersoberanía", o el uso del ciberespacio como un entorno para la competencia estratégica.

Los enfoques divergentes de las principales potencias cibernéticas en relación con la forma en que se aplica el derecho internacional en el ciberespacio, la cual se encuentra en discusión en los foros relevantes de Naciones Unidas, reflejan un entorno internacional bastante conflictivo, exacerbado aún más por los llamados a la "autonomía estratégica" digital, lo que incluso sería problemático lograr en un contexto de rápido cambio tecnológico y cadenas de valor globales.

Debido al alto nivel de interconexión de los Estados en el ciberespacio, la estabilidad de uno afecta el bienestar de todos los que lo rodean. Por lo tanto, un enfoque regional podría estimular a mucho s Estados para que participen en el desarrollo de capacidades de seguridad cibernética [25].

Por lo tanto, las iniciativas políticas y legislativas, junto con las medidas de creación de capacidad, son algunos de los elementos clave para combatir las amenazas derivadas del ciberespacio, incluida la conducta de los delincuentes. Por ello, la implementación de legislación relevante y la adopción de métodos estratégicos respaldarán la efectividad del trabajo realizado para la obtención de justicia penal a nivel nacional y la cooperación internacional entre los Estados de la OEA bajo el auspicio de las disposiciones del derecho internacional. La armonización regional de marcos legales para abordar el delito cibernético y las mejores prácticas de aplicación de la ley podrían contribuir a obtener seguridad y estabilidad regional en el ciberespacio [26].

5 Conclusiones

Si se considera la naturaleza sin fronteras de los delitos que se perpetran en el ciberespacio, la cooperación regional en el desarrollo de capacidades es vital

para poder reaccionar ante el crimen informático organizado y detener los ataques cibernéticos antes de que lleguen a niveles incontrolables. Los incidentes más recientes de 2020 y 2021 analizados en Argentina han demostrado el riesgo de un mayor daño financiero, en términos de la cantidad de personas y Estados a los que afectan.
Las TIC's abren camino en el sistema jurídico argentino al estudio exhaustivo del mundo virtual, del ciberespacio y los daños y delitos que fueran originados en él. Desde comienzos del milenio es una preocupación las consecuencias dañinas del robo o apropiación indebida de la identidad y actualmente con el uso desmedido de la internet, sitios web, buscadores y redes sociales el problema de la identidad digital se ha vuelto un desafío para la legislación argentina.
Como lo afirma Claus Schwab en su libro La Cuarta Revolución Industrial, "La tecnología no es una fuerza exógena sobre la cual no tengamos control. No estamos limitados por una elección binaria entre 'aceptar y vivir con ella' o 'rechazar y vivir sin ella'. En lugar de ello, debemos tomar el cambio tecnológico como una invitación a reflexionar sobre quiénes somos y cómo vemos el mundo" [27].
El robo de identidad o su apropiación indebida, constituye en este tiempo un tema de discusión no sólo en el ámbito jurídico, sino también en el económico, social y de seguridad financiera. La realidad de las nuevas técnicas sobre recogida y elaboración de datos ha hecho que sea necesaria una revisión no sólo de cómo proteger determinados bienes jurídicos como la identidad, la dignidad y la intimidad, sino incluso de hasta dónde debe llegar esta protección, como ocurrió en su momento con otras actividades propiciadas por las nuevas tecnologías, por lo que el derecho se ha visto desbordado por la nueva situación, incapaz de realizar su función con los instrumentos que tradicionalmente ha tenido a su alcance.

6 Referencias

[1] https://www.cibercrimen.org.ar/
[2] https://www.weforum.org/reports/the-global-risks-report-2021
[3] Temperini, Marcelo. Delitos Informáticos y Cibercrimen: Alcances, conceptos y características. Cibercrimen y Delitos Informáticos. Errepar-Suplemento Especial.2018.
[4] https://www.unodc.org/documents/Cybercrime/IEG_Cyber_website/UNODC_CCPCJ_EG.4_2020_2/UNODC_CCPCJ_EG.4_2020_2_S.pdf
[5] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[6] https://www.cibercrimen.org.ar/tag/delitos-informaticos/
[7] https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest
[8] https://www.cibercrimen.org.ar/wp-content/uploads/2021/06/El-fraude-informatico-en-2021.pdf
[9] https://www.weforum.org/press/2020/01/new-internet-security-principles-developed-with-world-economic-forum-to-help-protect-up-to-1-billion-users
[10] Belcic, I. (2020). ¿Qué es el phishing? | Detecte y evite los correos electrónicos de phishing | Avast. (2020). Recuperado el 15 de septiembre de 2020, de https://www.avast.com/es-es/c-phishing.
[11] Goscilo, A. (1981). Publicaciones. Revistas. Los bienes jurídicos penalmente protegidos. Lecciones y Ensayos, no. 46 (1) Segunda Época. Recuperado el 19/06/2018 de: http://www.derecho.uba.ar/publicaciones/lye/revistas/46-1/los-bienes-juridicos-penalmente-protegidos.pdf.

[12] Fernández Sessarego C. (1990) El derecho a la identidad personal, en 1990-D, p. 1248 de Revista Jurídica La Ley. [10] Monastersky, D - Salimbeni, J. M. (2013) Robo de identidad. Primera parte. Revista de Derecho de las Telecomunicaciones, Internet y Medios Audiovisuales (N°4). Buenos Aires: Editores Argentina.
[13] https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790
[14] Proyecto de Ley Proyecto de Ley Expte 4643-D-2010.
[15] Lugo, A (2016) Precauciones para el cuidado de tu identidad digital. Ideas y recursos para el docente. Buenos Aires. Editorial ACES.
[16] https://www.cibercrimen.org.ar/2020/12/24/estadisticas-ano-2020-completo/
[17] Capurro, R, Eldred M&Nagel,D(2013)Digital Whoness:Identity, Privacy and Freedom in the Cyberworld;Frankfurt;VOntos-velag. http://link.umsl.edu/portal/Digital-whoness--identity-privacy-and-freedom/QdyBjvNEM0w/
[18] Martinez Matilde, Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. Implicancias y consecuencias en materia penal y responsabilidad civil. Cibercrimen y Delitos Informáticos. Errepar-Suplemento Especial. 2018.
[19] Borghello C y Temperini M.G.I, (2012) Suplantación de Identidad Digital como delito informático en Argentina. Simposio Argentino de Informática y Derecho 2012. Argentina.
[20] Zarate, Pedro. Tesis de Grado Universidad del Siglo XXI. Robo y apropiación indebida de la identidad digital. Un Análisis en el marco de los derechos de raigambre constitucional.2018. https://repositorio.uesiglo21.edu.ar/handle/ues21/15688
[21] https://www.welivesecurity.com/la-es/2021/02/04/el-robo-de-identidad-aumento-durante-la-pandemia/
[22] Barba Álvarez, R. (2017) El robo de identidad en México. Revista de investigación en Derecho, Criminología y Consultoría Jurídica /245/ Año 11, No. 22, núm. 22, octubre de 2017-marzo de 2018 / pp. 245-260. México: Benemérita Universidad Autónoma de Puebla.
[23] https://www.consumidor.ftc.gov/
[24] https://www.coe.int/en/web/cybercrime/tcy
[25] https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe.
[26] https://books.google.com.ar/books/about/La_cuarta_revoluci%C3%B3n_industrial.html?id=BRonDQAAQBAJ&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false
[27] http://40.70.207.114/documentosV2/La%20cuarta%20revolucion%20industrial-Klaus%20Schwab%20(1).pdf