ESPECIALIZACIÓN EN CIBERCRIMEN

"LAS CONDUCTAS PREVIAS AL CIBERFRAUDE: LA SUPLANTACIÓN DE IDENTIDAD. EL DEBATE SOBRE SU REGULACION Y SU IMPORTANCIA EN LAS INVESTIGACIONES PENALES"

Carrera: Especialización en Cibercrimen

Alumno: Moisés Naim Carram

D.N.I.: 23.456.743

Dedicatoria y Agradecimiento

A todo el cuerpo docente que forma parte de la “Especialización en Cibercrimen” de la Universidad Siglo XXI, por todo el acompañamiento recibido, la dedicación y la generosidad brindada en cada de una de las materias que tuvieron a su cargo, y especialmente mi agradecimiento va dirigido para los siguientes docentes: Luciano Monchiero, Gustavo Sain, Javier Chilo, Rafael García Borda, Carlos Villanueva, Pablo Croci y Emiliano Piscitelli.

A mi familia que supo acompañarme y “bancarme” en todo este proceso, al cual le dediqué muchas horas de mi vida para lograr mi tan ansiado objetivo; a mis compañeros de especialización, con los cuales puede forjar con muchos de ellos, duraderos lazos de amistad que supieron trascender la “virtualidad” propia del cursado de la especialización.

Por último, vaya mi eterno agradecimiento a la Universidad Siglo 21 por haberme permitido “regresar” a sus aulas y rememorar hermosos recuerdos de mi época de alumno de una carrera de grado, en esta oportunidad haciéndolo como profesional egresado para especializarme en una carrera de posgrado.

Resumen

La exposición y vulnerabilidad en la que se encuentran los datos e identidad digital de las potenciales víctimas que utilizan dispositivos digitales a diario, está quizás en este momento de la historia de la humanidad en su punto más alto y sigue en constante ascenso, por cuanto a cada segundo, minuto, hora, día, mes y año que trascurren, se genera un volumen incalculable de información digital, considerado a nivel mundial como el activo económico más importante, lo cual requiere de mecanismos cada vez más sofisticados y de la intervención de la inteligencia artificial tanto para su procesamiento (recolección, clasificación, análisis, etc.) como así también para su aseguramiento o protección (generalmente a cargo del sector privado) a los fines de evitar que caiga en manos no deseadas. En este último aspecto, y a la luz de un aumento considerable de los ciberdelitos, la doctrina y la sociedad en su conjunto debaten sobre la necesidad de que el estado intervenga regulando aquellas conductas (actualmente no punibles), que son cometidas previas a la comisión de un ciber-fraude y que trascienden en el ciber-espacio por el uso de internet, por cuanto se ha producido una suplantación de identidad digital de las victimas (personas físicas o jurídicas), cuyas consecuencias son casi imposibles de cuantificar debido al efecto global y multiplicador propio del uso de este tipo de red, que a su vez le posibilitó al ciber-atacante quebrantar los limites típicos y propios que definen a los delitos tradicionales (tiempo, modo y espacio) y bajo el paraguas protector de un "eventual" anonimato, configurándose de este modo un complejo escenario que le impide a los órganos judiciales y/o policiales llevar a cabo una eficaz investigación penal no tan solo con el delito consumado sino también con los que pudieran llegar a cometerse a futuro.

Palabras claves: Datos, identidad digital, información digital, inteligencia artificial, ciberdelitos, regulación penal, ciber-fraude, suplantación de identidad, anonimato.

Abstract

The exposure and vulnerability of the data and digital identity of potential victims who use digital devices on a daily basis is perhaps at this moment in the history of humanity at its highest point and continues to constantly rise, in terms of Every second, minute, hour, day, month and year that passes, an incalculable volume of digital information is generated, considered worldwide as the most important economic asset, which requires increasingly sophisticated

mechanisms and the intervention of the artificial intelligence both for its processing (collection, classification, analysis, etc.) as well as for its insurance or protection (generally carried out by the private sector) in order to prevent it from falling into unwanted hands. In this last aspect, and in light of a considerable increase in cybercrimes, doctrine and society as a whole debate the need for the state to intervene by regulating those behaviors (currently not punishable) that are committed prior to the commission of crimes. a cyber-fraud and that transcends into cyber-space due to the use of the Internet, since there has been a digital identity theft of the victims (natural or legal persons), the consequences of which are almost impossible to quantify due to the global and multiplier effect itself. of the use of this type of network, which in turn made it possible for the cyber attacker to break the typical and specific limits that define traditional crimes (time, mode and space) and under the protective umbrella of an "eventual" anonymity, configuring This creates a complex scenario that prevents judicial and/or police bodies from carrying out an effective criminal investigation not only with the completed crime but also with those that could be committed in the future.

KEY WORDS: Data, digital identity, digital information, artificial intelligence, cybercrimes, criminal regulation, cyber-fraud, identity theft, anonymity.

INDICE

Introducción

Para una mejor comprensión del presente trabajo, debemos partir de la idea que la humanidad vive un momento muy especial y único en su historia, invadida por doquier de las nuevas tecnologías de la información y la comunicación, que se encuentran inmersas en un derrotero incesante marcadas por constante y sostenido desarrollo cuyos límites son totalmente impredecibles para la mente humana, creando una interconexión e interdependencia tal, que sería inconcebible para cualquier mortal prescindir de su uso en cualquiera de sus formas.

La aparición de la pandemia por Covid-19, como hecho histórico relevante de enorme trascendencia en el ámbito tecnológico marcó sin lugar a dudas un antes y un después, que si bien se trató de una cuestión de extrema gravedad de tipo sanitaria o de salud pública, obligó a los estados a adoptar una serie de medidas de distinta índole entre las cuales se destaca el confinamiento o aislamiento social obligatorio que se impuso no solo en Argentina sino en todo el mundo, y su principal efecto o impacto en función de lo que aquí nos interesa (es decir lo tecnológico), fue el haber "empujado" forzosamente a miles de millones de personas a un mundo digital conocido a medias hasta ese momento, hasta llegar a un nivel de hiperconectividad inédito hasta ese momento y de una magnitud tal que supo trascender cualquier limite de indole social, económico, etario, racial, religioso, cultural, político, etc.

Estas consecuencias y variaciones sustanciales (mayormente positivas) producidas en todas las actividades humanas por aquel "movimiento tecnológico", lógicamente se trasladó a la actividad delictiva, causando que algunas de las modalidades delictivas conocidas y reguladas por la ley penal, tuvieran una suerte de "aggiornamiento" a estos cambios tecnológicos con algunas particularidades; mientras que en otros casos directamente se evidenció la aparición de nuevas modalidades delictivas, siendo algunas de ellas alcanzadas por la ley penal, mientras que otras no, dando lugar en este último caso a la aparición de una laguna jurídica o vacío legal[1], que a criterio del autor de esta obra deberá ser subsanado con premura y urgencia por el legislador local según los argumentos y/o razones que aquí se indicarán.

Es dable destacar en este contexto, el fuerte impacto que produce en el conjunto de la sociedad ante la presencia de las mencionadas "lagunas legales", que exterioriza su descontento cuando

[1] *Laguna jurídica o vacío legal*: Se refiere a la ausencia de legislación a una materia o caso concreto.

manifiesta percibir una total desprotección ante la real (mal llamada virtual) y concreta peligrosidad que generan este tipo de conductas delictivas aún no reguladas penalmente, y que en consecuencia le permiten al ciber delincuente actuar a "gusto y piacere" bajo ese halo de impunidad, escenario potenciado aún más dado el carácter transfronterizo y atemporal propio de cualquier ciberdelito, cuyos efectos son totalmente diferentes a los delitos tradicionales.

El crecimiento exponencial de la ciberdelincuencia no se debe solamente a la mencionada falta de un marco normativo adecuado, sino también a otras causas, entre las que se mencionan a modo ejemplificativo: la facilidad de acceso a las nuevas tecnologías de la información y la comunicación, en función de los bajos costos económicos para su adquisición, por la amplísima variedad y calidad de equipos disponibles en el mercado, por no requerir de abundantes conocimientos técnicos o de informática para su operatividad, etc.; otra de las causas está referida a un importante nivel de anonimato que los medios tecnológicos le aseguran al ciber atacante, augurándole asimismo grandes chances de "éxito" en su accionar delictivo, y por ende obstaculizando (pero no impidiendo totalmente) la tarea investigativa a los órganos judiciales o policiales encargados a tal fin.

En consecuencia, el problema de investigación que aquí se analiza gira en torno precisamente, en la identificación y caracterización de todas aquellas acciones o actividades que necesariamente se llevan a cabo previo a la comisión de cualquier ciberfraude típico, y muy especialmente con respecto a la suplantación de identidad, que según el régimen legal actual no serían punibles por tratarse de "simples actos preparatorios", que generalmente son impunes salvo que una norma expresa determine lo contrario. En este aspecto, se pone de manifiesto que en función de la trascendencia jurídica que dichas conductas poseen, tanto en el entramado constitutivo del iter criminis[2] de un ciberfraude "típico" (por ej: requiere "suplantar" o "robar" la identidad de la víctima) como así también para la comisión de otros tipos de ciberdelitos, se debate en la doctrina sobre la necesidad de su tipificación penal y por ende su inclusión dentro de la categoría de "delitos informáticos", que a su vez le facilite a los operadores judiciales y/o policiales un eficaz accionar preventivo, como así también la obtención de investigaciones penales con un alto porcentual de productividad positivo.

[2] *Iter criminis*: termino de origen latino que significa "camino del delito" y que es utilizada en derecho penal para referirse al proceso de desarrollo del delito en sus distintas fases o etapas, cuyo inicio nace con el surgimiento de la idea criminal, la planificación, la preparación y por ultimo su consumación o ejecución.

El objetivo general o principal del presente trabajo pretende: "Analizar el fenómeno de la suplantación de identidad como conducta previa al ciberfraude y el debate que se ha generado en la doctrina y a nivel general en torno a la necesidad de su regulación como una figura penal autónoma que posibilite lograr investigaciones judiciales eficaces". Mientras que los objetivos específicos o secundarios consisten en: a) Identificar las fases de producción de un ciberfraude, y dentro de cada uno de ellas las conductas requeridas a los fines de su detección temprana; b) Demostrar que la obtención ilegal o no de datos y el posterior uso o no de los mismos (suplantación de identidad), además de ser conductas previas configurativas de un ciberfraude típico, se tratan de verdaderos delitos autónomos, potencialmente capaces de producir perjuicios patrimoniales o extra patrimoniales; c) Destacar la necesidad de regular como delito y con carácter excepcional este tipo conductas, consideradas en el contexto de un "iter criminis" como actos preparatorios para la comisión de un ciberfraude típico u otras figuras delictivas; d) Describir y analizar la legislación actual vigente a nivel nacional en materia de ciberfraudes y específicamente respecto a la suplantación de identidad digital, a fin de establecer las "lagunas" existentes; e) Analizar la legislación comparada a nivel internacional que regularon la suplantación de identidad digital, especialmente la cometida a través de una obtención ilegal o legal de datos; f) Destacar la necesidad de proteger la identidad digital, que comprende un conjunto de rasgos y características que toda persona posee en la red de redes (internet), cuya vulneración (suplantación de identidad) lo afecta en su faz psicológica, moral y social; g) Resaltar la importancia de contar con una legislación penal capaz de adecuarse a las nuevas variantes delictivas que vayan sucediéndose, en función a los constantes avances tecnológicos y h) Demostrar que la regulación penal de la obtención ilegal de datos con suplantación de identidad digital contribuirá a una significativa disminución (función preventiva) de futuros ciberfraudes y de otros ciberdelitos.

Desde lo metodológico, la finalidad del presente trabajo es esencialmente de investigación, con un sentido de tipo dogmático propositivo, a partir de la utilización de una técnica de tipo documental que gira en torno a la recolección, selección y análisis de información que pueda ser obtenida en libros, publicaciones y artículos científicos, relacionados con las conductas que integran un ciberfraude y con especial énfasis en lo relacionado con la suplantación de identidad, a partir del debate que surge sobre las distintas maneras que fue regulada en la legislación comparada y el problema actual por la falta de regulación en el derecho local, cuyas consecuencias repercuten notablemente en las investigaciones penales.

Desde el punto vista del enfoque es de tipo cualitativo, ya que, a partir de la producción de datos descriptivos y subjetivos, se pretende descubrir lo más profundo posible a todo lo que rodea a una suplantación de identidad como fenómeno de análisis, por medio de la comprensión analítica y/o la interpretación del sentido y alcance que tanto la doctrina, la legislación comparada y otras fuentes, le han asignado a aquella en función del contexto social en que se desarrolla.

Sintéticamente, el trabajo comienza en el capítulo 1 aportándole al lector algunas aproximaciones conceptuales sobre la figura del ciberfraude, a partir de sus aspectos principales y en función de la identificación de sus elementos constitutivos, para luego ramificarse en otros aspectos muy importantes relacionados con la descripción de las fases o secuencias y la importancia de ciertas actividades delictivas constitutivas que puede derivarse en otras figuras delictivas; seguidamente se deslizan algunas definiciones de identidad digital destacando su importancia, su relación con los datos personales y los dilemas y desafíos que surgen por la intervención de la Inteligencia Artificial como herramienta de Big data. Posteriormente, previo a comprender en que consiste un ataque a la identidad, se abordará la figura central del trabajo relacionada con el robo o suplantación de identidad digital, a partir de sus aspectos distintivos y particulares, las técnicas o modalidades que utilizan los ciberdelincuentes para llevarlo a cabo y sus diferencias con el intrusismo informático o hacking ético.

En el capítulo 2, se analizará el marco normativo general regulatorio de las tecnologías de la información y la comunicación (TICs) según el proceso evolutivo acaecido producto del avance tecnológico y de algunas circunstancias trascendentales, que fueron impulsando la agenda nacional e internacional en esta temática, analizando específicamente la figura de la suplantación de identidad, a partir de la regulación prevista por la legislación comparada como así también por los numerosos proyectos legislativos locales que intentaron incorporarla como delito en nuestro sistema penal y la incipiente legislación de carácter contravencional que supo regularla.

Dando por culminada la introducción, aprovecho la oportunidad para despedirme del lector no sin antes agradecer su valioso tiempo dispensado y lo invito a que continúe su recorrido en la presente obra, con la certeza de que este humilde aporte a la ciencia jurídica será de mucha utilidad en su formación profesional.

Capítulo 1. Aproximaciones conceptuales.

Introducción

En este primer capítulo, abordaremos algunos conceptos claves que conforman la estructura medular del presente trabajo, con la finalidad de que el lector, al continuar con su recorrido por el resto del mismo, pueda llegar a comprender la problemática aquí tratada, por haber adquirido previamente conocimientos básicos propios de esta "nueva" especialidad dentro del derecho penal.

En primera instancia, iniciaremos nuestro recorrido con el abordaje de la figura del "ciberfraude", "estafa electrónica" o "ciber estafa", distintas denominaciones que ha acuñado la doctrina especializada pero que confluyen en torno a una misma figura penal; comenzando por sus aspectos principales, es decir aquellas notas características que la distinguen notablemente de la estafa común o tradicional por todos conocida, y continuando luego con sus elementos constitutivos. En segunda instancia, se analizará lo relacionado con la identidad digital, haciendo la salvedad que será de una manera resumida en función de lo extensa y profunda que resulta esta importante temática por estos días, para lo cual analizaremos algunas definiciones, sus características, alcance e importancia. En último término, estudiaremos una figura penal que al igual que el ciberfraude, la doctrina ha denominado de diferentes maneras en todo el mundo, pero que todas esas definiciones refieren al mismo delito, nos referimos concretamente a la "suplantación", "robo" y/o "usurpación" de identidad, refiriéndonos como se dan generalmente este tipo de ataques a la identidad de una persona por parte del ciberdelincuente, cuáles son sus notas distintivas, bajo que modalidades o técnicas o modalidades se producen, que entiende la doctrina por esta figura aún no legislada en nuestro país y su relación con el intrusismo informático.

Para una adecuada lectura del presente capitulo, le sugerimos al lector, que los temas tratados sean analizados en forma conjunta e integral, ya que tal como se desprende de la lectura de los mismos, todos están interrelacionados y conforman un todo, que se puede verificar en la faz práctica, cuando el ciberdelincuente en ocasión de realizar conductas ilícitas, comete uno o más delitos (por ej: el que obtuvo datos sensibles de la víctima luego de cometer un ciberfraude también suplanta la identidad de la víctima afectando otros bienes jurídicos protegidos por el código penal).

1.1. El Ciberfraude. Aspectos principales.

La figura del ciberfraude o también como conocida "estafa informática", incorporada al código penal argentino por Ley 26.388[3] como una modalidad especial de estafa en el inc. 16° del art. 173°[4], será abordada aquí solamente tomando en consideración algunos aspectos principales en función de la importancia que tiene con respecto a sus conductas constitutivas, cuya trascendencia estriba entre otros aspectos, en su carácter transfronterizo, que como bien se explica en la obra de Aboso y otros (2022), se comprueba por "un mayor poder de expansión del perjuicio patrimonial alcanzado a un número significativo de víctimas impersonales, en especial, porque estos delitos interactúan con procesos de almacenamiento y transmisión de datos, siendo prescindible la conexión entre los individuos" (p. 14)[5].

Esta controvertida modalidad delictiva fruto del adelanto tecnológico propio de estos tiempos, ha generado en la doctrina especializada las más variadas y diferentes discusiones dogmáticas al respecto, algunos lo hicieron desde una mirada normativa criticando la utilización de una deficiente técnica legislativa para la redacción del inc. 16° del art. 173° del C.P., cuando en el mismo se refiere a sistemas informáticos incurre en una falta de conocimiento del funcionamiento tecnológico requerido para que se configure el delito, ya que "no es lo mismo introducir un dato falso que alterar el funcionamiento de un sistema informático" (Neme y Portillo, 2020, p. 8)[6]. En este sentido, la ley 26.388 que tuvo como principal antecedente legislativo el art. 8° del Convenio sobre la Ciberdelincuencia, popularmente conocido como Convenio de Budapest[7], no tuvo en cuenta la diferenciación que si había realizado el citado convenio en dicho art. 8° al sostener que estos delitos "consisten principalmente en manipulaciones respecto de la introducción de datos, cuando se introducen datos incorrectos en un ordenador, o en manipulaciones respecto de los programas y otras interferencias al procesamiento de los datos" (Neme y Portillo, 2020, p. 6), es decir que esa manipulación

[3] Ley N° 26.388, también conocida como "Ley de Delitos Informáticos", incluyó algunos artículos y modificó otros existentes del código penal argentino, tuvo su sanción el 4/6/2008 y su promulgación de hecho el 24/6/2008.
[4] Art. 173° Inc. 16°: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".
[5] Aboso, G. y otros. (2022). *Ciberdelitos. Análisis Doctrinario y jurisprudencial*. Ciudad Autónoma de Bs.As., Argentina. Ed. Albrematica S.A.
[6] Neme, Catalina F. y Portillo, Víctor H. (noviembre de 2020). El Ciberfraude en el Código Penal Argentino. Bs.As., Argentina. Ed. Erreius on line.
[7] Convenio sobre la Ciberdelincuencia. Aprobado por el Comité de Ministros del Consejo de Europa el 8/11/2001 y abierto a la firma en Budapest, el 23/11/2001. Argentina se adhirió por Ley 27.411 de fecha 22/11/2017. Informe explicativo del Convenio recuperado de https://rm.coe.int/16802fa403

indebida se da "en el transcurso del procesamiento de datos con la intención de efectuar una transferencia ilegal de bienes" (Neme y Portillo, 2020, p. 6).

Para graficar la disparidad de criterios al respecto, sostiene el maestro Riquert (2010), que más allá de la inclusión por el legislador de esta figura en el "Capítulo IV Estafas y otras defraudaciones" en nuestro código penal argentino, algunos autores como Alonso Salazar, consideran que la "estafa electrónica" no es ninguna estafa, por ausencia de un sujeto pasivo que realice el acto dispositivo, pero que sin embargo se asemeja a la hipótesis de la estafa triangular (el engañado y el estafado son personas diferentes)" (p. 30)[8].

El ciberfraude o estafa informática, es considerada como una modalidad especial de estafa que se distingue principalmente por que la disposición patrimonial o transferencia de activos se produce por "medios informáticos", es decir que el medio comisivo para producir el perjuicio patrimonial se realiza a través de la manipulación de un sistema informático o transmisión de datos de un sistema informático, no obstante ello se da la misma "secuencia" típica de las estafas tradicionales (figura genérica), por la cual el estafador (sujeto activo) lleva a cabo conductas que, mediante un ardid o engaño, provoca un error en la víctima (sujeto pasivo) y, a raíz de ese error, se produce una disposición patrimonial que causa un perjuicio económico ya se en su propio patrimonio o en la de un tercero (ofendido).

En esta última hipótesis, es decir cuando no convergen ambas circunstancias en el mismo sujeto pasivo, se da el caso de "quien resulta víctima del ardid o engaño producido por el sujeto activo no sea quien se vea perjudicado en su patrimonio por esta acción" (Neme y Portillo, 2020, p. 2), por lo que se usa el término "ofendido", a la víctima que efectivamente sufrió el perjuicio patrimonial en manos de la víctima del fraude (sujeto pasivo).

Lo que distingue a una estafa típica o genérica de ciberfraude o fraude informático, es que "el error humano es reemplazo por la manipulación informática que influye sobre el proceso de tratamiento y transmisión de datos que culmina con la producción del resultado desvalorado" (Aboso y otros, 2022, p. 34).

Con respecto al sujeto activo, es importante resaltar que el beneficio obtenido producto de la estafa puede ser para el mismo sujeto que comete el ciberdelito como así también para un

[8] Riquert, Marcelo. (2010). *Algo más sobre la legislación contra la delincuencia informática en Mercosur a propósito de la modificación al código penal argentino por ley 26388*. Bs.As., Argentina. Publicación de CIIDPE (Centro de Investigación Interdisciplinaria en Derecho Penal Económico).

tercero, aquí intervienen lo que en la jerga policial se conocen como las "mulas"[9], cuya participación criminal es muy discutida por la doctrina.

1.2.1. Elementos constitutivos

Al respecto nos enseñan Neme y Portillo (2020), sobre la existencia de dos elementos constitutivos en el ciberfraude, a saber: 1) La manipulación informática, que consiste en toda acción que suponga intervenir en el sistema informático alterando, modificando u ocultando los datos que deban ser tratados automáticamente, o modificando las instrucciones del programa, todo ello con el fin de alterar el resultado debido de un tratamiento informático; y 2) La consecuente transferencia indebida de fondos que causa un perjuicio patrimonial de la víctima o de un tercero (p. 4).

La complejidad que acarrea esta figura especial de estafa, que la distingue claramente de la estafa "tradicional", tal como lo expresan en Aboso y otros (2022), se debe a que "junto al objeto de protección mencionado, esto es, el patrimonio, confluyen otros intereses penalmente tutelados que se identifican con la integridad, el correcto funcionamiento y la facultad de disposición de datos" (p. 17), configurándose de esta manera según este autor, en tipo penales diferentes llamados "tipos penales conglomerantes" por la pluralidad de interés protegidos en juego" (p. 17).

Haciendo foco en las conductas o comportamientos comisivos, que forman parte de su estructura interna (iter criminis), las mismas propenden a la obtención de datos, que valiéndose de una previa "manipulación informática que provoca el perjuicio puede entonces darse a través de la introducción, alteración, borrado o supresión de datos informáticos, o por cualquier ataque al funcionamiento mismo del sistema" (Neme y Portillo, 2020, p. 4), los cuales posteriormente de su obtención, son utilizados generalmente para suplantar la identidad digital de la víctima para cometer ese mismo ciberfraude o cualquier otro tipo de delito de contenido extrapatrimonial. La acción típica consiste en "defraudar a un tercero mediante una técnica de manipulación informática que abarque la alteración del normal funcionamiento de un sistema informático o la transmisión de datos" (Aboso y otros, 2020, p. 35), es decir que se requiere de

[9] Se entiende por "mulas digitales": a una persona que transfiere dinero u otros activos que han sido obtenidos ilegalmente, mediante estafas u otros medios, de un punto geográfico a otro (suelen ser transferidos al lugar donde el autor del delito reside).

una manipulación informática con el consecuente beneficio patrimonial ilícito para el autor para que se configure la estafa informática.

Generalmente en este tipo de delito se da la concomitancia que se produce de manera simultánea o sucesiva un daño informático (por ej.: sustracción de claves bancarias digitales, de cuentas de redes sociales, introducción de programa malicioso, etc.) y el consiguiente perjuicio económico o patrimonial.

En todas aquellas situaciones, en las cuales el autor ha obtenido las correspondientes credenciales (nombre de usuario y contraseña o clave) que le permitirán luego hacer un "uso indebido de datos personales del usuario, por ejemplo, el acceso autorizado al home banking de la víctima, pero la transferencia no autoriza de dinero electrónico a la cuenta del autor o de un tercero, o el pago no autorizado de servicios personales no encuadran dentro de los presupuestos normativos de la materia de prohibición" (Aboso y otros, 2022, p. 36); en definitiva, lo que queda bien claro es que cualquier tipo de conducta delictiva que manipula algún tipo de datos[10] de la víctima que no redunde en un perjuicio patrimonial de aquella, no la convertirá ipso facto en un delito de fraude informático o ciberfraude.

1.2. La identidad digital. Su importancia.

En estos tiempos donde internet todo lo "invade", fundado en gran medida por el propio usuario o consumidor debido a que "las demandas de mayor protagonismo de éstos propician una nueva forma de entender la red, una "nueva filosofía" si se quiere, que convierte los perfiles de los internautas en un único perfil con capacidad de consumidor y generador de contenidos" (Santamaría Ramos, 2015, p. 16)[11], de tal forma que "la mayoría de las personas con acceso a las redes experimentan la necesidad de estar conectados, de chequear sus casillas de correo electrónico, su timeline de twitter o su muro en facebook" (Temperini y Borghello, 2012, p. 88)[12]; escenario que se presenta como un gran desafío para los gobiernos de turno quienes

[10] Dato: entendido en un concepto amplio como todo tipo de información personal que merece tutela jurídica.
[11] Santamaría Ramos, Francisco José. (2015). *Identidad y reputación digital. Visión española de un fenómeno global*. Publicado en revista "Ambiente Jurídico" del Centro de Investigaciones Socio jurídicas de la Universidad Complutense de Madrid, año 2015, N° 17. Recuperado de https://revistasum.umanizales.edu.co/ojs/index.php/Ambientejuridico/article/view/1570
[12] Temperini, Marcelo y Borghello, Cristian (2012). *Suplantación de Identidad Digital como Delito Informático en Argentina*. X Simposio Argentino de Informática y Derecho, organizado por la Sociedad Argentina de Informática

deberán activar mecanismos y condiciones necesarias, aptas para brindar la correspondiente protección legal a toda esa inmensa población (casi toda) que desarrolla una vida social "virtual" muy activa en las redes, cuya importancia y trascendencia es igual o mayor (especialmente para las nuevas generaciones) que las relaciones sociales tradicionales, coincidiendo esto con Guini (2023), cuando dice que "a medida que se accede a más y más servicios esenciales en línea y más allá de las fronteras, se vuelve importante mejorar la gobernanza y la implementación de los sistemas de identidad digital en línea con las necesidades del usuario (p. 7)[13].

Es evidente que, no debería existir impedimento alguno para advertir que "es en esta participación virtual y social donde las personas expresan sus deseos, sus intereses, sus amistades, su trabajo, sus proyectos, en suma, una parte importante de sus vidas. Este es el punto donde se encuentra la identidad digital de las personas, en movimiento constante y dinámico, ese mencionado conjunto de atributos y características que permiten individualizar a la persona en un grupo social, atributos y características que cada vez más se desarrollan en y a través de internet" (Temperini y Borghello, 2012, p. 88).

Aquí toman valor, dos conceptos diferentes pero que están muy relacionados entre sí como lo son la reputación (la opinión que otros tienen de mí) y la identidad digital (lo que yo soy o pretendo ser o creo que soy), cuyas reglas de generación en el mundo digital no son las mismas o no son iguales que en el mundo físico, ya que "internet es un mecanismo extraordinariamente eficiente de comunicación humana; multiplica nuestra capacidad de establecer relaciones; nos libera de los límites que introducen las distancias geográficas e incluso, de muchos prejuicios, al permitirnos comunicarnos y relacionarnos con personas que viven a miles de kilómetros de distancia y que a priori no parecen tener nada en común con nosotros" (Santamaría Ramos, 2015, p. 17).

Como contracara de tanta "hiperconectividad" a las tecnologías de la comunicación e información (TIC) y en especial a internet, se observa que un importante porcentaje de la población no ha terminado de comprender aun con total claridad, la responsabilidad y los

e Investigación Operativa, en La Plata, Bs.As., Argentina, 27 al 31 de agosto de 2012. Recuperado de https://41jaiio.sadio.org.ar/sites/default/files/7_SID_2012.pdf

[13] Guini, Leonor Gladys (2023). *De la ID electrónica a la ID digital auto soberana.* Bs.As., Argentina. elDial-DC322A. Editorial Albremática S.A. Recuperado de https://www.eldial.com/nuevo/nuevo_diseno/v2/doctrina2.asp?base=50&id=14949&t=d

riesgos que trae aparejado cuando se actúa de forma desaprensiva, temeraria, negligente, sin otorgarle la debida importancia que requiere la aplicación de las técnicas y prácticas seguras recomendadas por los especialistas, cuyas consecuencias se manifiestan en la invalorable posibilidad que le permite a los ciberdelincuentes "engendrar otras prácticas altamente negativas que afectan gravemente otros derechos a ser protegidos como la intimidad, el honor, la imagen y reputación digital de las personas" (Vaninetti, 2024, p. 1)[14].

A tal fin será fundamental, la puesta en funcionamiento de campañas constantes y permanentes de alfabetización digital, no tan solo constante y permanente del estado como principal impulsor sino también por parte del sector privado, que concienticen a la población de que simples acciones como por ejemplo dar un simple click (por error o intencional) a un enlace o link (por ej: que produce la descarga de un malware a un dispositivo digital) o la incorporación de datos sensibles y personales (credenciales) en sitios web ilegales o apócrifos (por ej: pishing), exponen de tal forma sus datos personales y su identidad digital quedando la misma en manos de los ciberdelincuentes o de terceros, con todo lo que esto implica y a los que nos hemos referido en párrafos anteriores.

1.3.1. Definiciones de identidad e identidad digital. Su relación con los datos personales

Existen tantas definiciones de identidad como áreas del conocimiento científico que se han dedicado a su estudio, algunas de ellas han puesto a la identidad en un lugar de preferencia mientras que otras directamente la han negado, es decir que la diversidad de aquellos enfoques es muy amplio e incluso contradictorios entre sí, tal como lo expresa Mender Bini (2024), la identidad "es un término que importa una gran complejidad a la hora de conceptualizar y, ello, dependerá principalmente del ángulo del que se analiza el vocablo" (p. 26)[15].

Un sector entiende que la identidad comprende "aquel conjunto de atributos y características que permiten individualizar a la persona en sociedad, pertenecientes a un individuo

[14] Vaninetti, Hugo Alfredo (2024). *Efecto expansivo y multiplicador del daño por contenidos viralizantes en internet.* Bs.As., Argentina. Ed. La Ley-Thompson Reuters. Recuperado de http://laley.thomsonreuters.com/nota/7741?s=09

[15] Mender Bini, Susana Eloisa. (2024). *Sistemas Biométricos. Privacidad y vulnerabilidad de los datos utilizados por los organismos del Estado Argentino*. Bs. As., Argentina. Ed. Albrematica S.A.

determinado, o compartidas por todos los miembros de una determinada categoría o grupo social" (Temperini y Borghello, 2012, p. 79).

Para Liceda (2011), la identidad es "una universalidad compuesta de datos personales", asociando de esta manera la identidad digital con los datos personales, por lo que debemos remitirnos al art. 2° de la ley N° 25.326[16], que define al dato personal con una amplitud tal comprensiva de "cualquier tipo de información personal (sobre persona física o jurídica), sea relativa al estado civil, a la familia, económicas, de contacto, etc." (p. 297)[17], es decir que los datos personales "permiten identificar a la persona, ya sea de manera directa o indirectamente, mediante uno o varios elementos característicos de su identidad, ya sea físicos, biológicos, fisiológicos, económicos, culturales, genéticos, etc." (C.F.T y A.A.I.P., 2023, p. 11)[18].

Cabe aclarar que la ley 25.326 solamente distingue entre datos personales y datos sensibles, ante lo cual para el "análisis de los datos desde la identidad, proponemos la siguiente clasificación: a) datos atribuidos por el estado, b) datos biológicos, c) datos históricos y d) datos generados por la persona" (Liceda, 2011, p. 297).

Dentro de la categoría de datos sensibles se encuentran "los relativos a opiniones políticas, origen étnico, convicciones religiosas, información referente a la salud y la orientación sexual" (C.F.T y A.A.I.P., 2023, p. 11), como así también los datos genéticos y biométricos, de gran trascendencia por la utilización indiscriminada que realizan los sistemas de inteligencia artificial.

También se habla de "una doble faz en la identidad personal: la estática, que apunta a los rasgos físicos y biológicos del individuo, inmutables por naturaleza; y la dinámica que se refiere a los modos particulares que ese sujeto adopta para comunicarse e insertarse en su vida de relación con los demás" (Temperini y Borghello, 2012, p. 86), en este sentido "al concepto de identidad desde la perspectiva de rasgos distintivos, se suman otros elementos que coadyuvan con su

[16] Ley N° 25.326 de Protección de Datos Personales (Habeas Data) (B.O.: 30/10/2000). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

[17] Liceda, Ernesto (2011). *La Identidad Digital*. Publicado en revista Anales de la Facultad de Ciencias Jurídicas y Sociales, año 8, N° 41, de la Universidad Nacional de La Plata. Recuperado de http://www.gecsi.unlp.edu.ar/documentos/DerechosHumanos/La_Identidad_Digital.pdf

[18] Consejo Federal de la Transparencia (C.F.T.) y la Agencia de Acceso a la Información Pública (A.A.I.P.) (2023). *Lineamientos para la formulación de un plan de protección de datos personales*. Recuperado de https://www.argentina.gob.ar/sites/default/files/documento_datos_2023.pdf

materialización, es decir, las credenciales de identidad; en donde ésta se plasma" (Mender Bini, p. 27).

Por consiguiente, ya centrados en la identidad digital, se sostiene que "solo puede ser creada por una persona" (Liceda, 2011, p. 302), lo que no impide que ese único sujeto "puede crear varias identidades digitales" (Liceda, 2011, p.302), en contraposición a la identidad real que solamente puede ser única; o que puedan existir "identidades digitales "vacías" es decir, que no existe una persona física que se vincule realmente con esa universalidad…de datos" (Liceda, 2011, p. 302).

Cuando se habla de identidad digital, ésta debe ser entendida "como el conjunto de rasgos y características particulares que una persona expresa a través de internet, forma parte inescindible de la identidad personal de cada sujeto, en su faz dinámica, y más precisamente en su aspecto psicológico, social y moral" (Temperini y Borghello, 2012, p. 92), protegido bajo el paraguas legal adecuado por tratarse de bien jurídico inserto dentro de la categoría de derechos humanos.

Según definición adoptada por Santamaría Ramos (2015) del INTECO (Instituto Nacional de Tecnologías de la Comunicación), cuya denominación actual es INCIBE (Instituto Nacional de Ciberseguridad de España), se entiende por identidad digital aquel "conjunto de la información sobre un individuo o una organización expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital" (p. 16), definición tomada del INTECO (Instituto Nacional de Tecnologías de la Comunicación) cuya denominación actual es INCIBE (Instituto Nacional de Ciberseguridad de España)[19].

Se habla también de proyección de la persona en entornos digitales, que se diferenciaría de la identidad digital, que se da cuando ese conjunto de datos y/o información digitalizada está directamente relacionada con una persona física o jurídica, y la misma goza del reconocimiento por parte de terceros.

[19] INCIBE (Instituto Nacional de Ciberseguridad de España). Para más información consultar https://www.incibe.es/

1.3.2. Características principales

La doctrina, a partir de haber analizado el conjunto de normas vigente de alcance nacional e internacional (Constitución nacional, pactos y convenciones), supo identificar en la identidad "algunos caracteres comunes: es algo que debe ser protegido, es algo que debe ser respetado y es algo intrínseco a la persona o una colectividad" (Liceda, 2011, p. 296)[20].

Santamaría Ramos (2015) en su obra, citando a la Organización para la Cooperación y el Desarrollo Económicos (OCDE), detalla los siguientes caracteres reconocibles en la identidad digital de las personas físicas, a saber: a) es social: ya que proyectada en internet su poseedor recibe el reconocimiento de parte de otros internautas; b) es subjetiva: se basa en la experiencia que construyen los internautas; c) es valiosa: en el sentido de que toda esa información generada puede ser empleada para establecer relaciones personalizadas y tomar decisiones con respecto a éstas; d) es referencial: esta referenciada a una determinada persona u objeto; e) es compuesta: por cuanto la información puede ser generada por el propio poseedor voluntariamente o por terceros sin consentimiento de aquel; f) genera consecuencias: a partir de la divulgación o no divulgación se producen efectos; g) es dinámica: se modifica constantemente, está en constante movimiento y h) es contextual: si es divulgada en un contexto erróneo o irrelevante puede generar un impacto negativo (p. 19-20).

1.3.3. Los sistemas Biométricos. Desafíos y dilemas que plantea la I.A.

Una forma de determinar la identidad física y digital de una persona es por medio de la utilización de los sistemas biométricos, que consiste en "el uso de las ciencias de la tecnología para extraer los rasgos únicos de un individuo, ya sean rasgos físicos o conductual, a los fines de positivamente verificar y/o identificar la identidad de un individuo, de manera tal que pueda acceder a ciertos recursos" (Mender Bini, 2024, p.55), a tal efecto la Organización de Aviación Civil Internacional (OACI), con el fin de prevenir el "robo" de identidad ha implementado una serie de medidas en su ámbito específico de actuación.

[20] Liceda, Ernesto (2011). *La Identidad Digital*. Publicado en revista Anales de la Facultad de Ciencias Jurídicas y Sociales, año 8, N° 41, de la Universidad Nacional de La Plata. Recuperado de http://www.gecsi.unlp.edu.ar/documentos/DerechosHumanos/La_Identidad_Digital.pdf

Previamente es necesario aclarar, que para acreditar la identidad de una persona "se pueden indicar tres métodos básicos, conocidos al presente: 1) lo que la persona sabe; 2) lo que la persona posee y; 3) lo que la persona es" (Mender Bini, 2024, p. 63), y que "en el caso de los dos primeros métodos, se ha encontrado que los mismos no son suficientemente confiables" (Mender Bini, 2024, p. 63.). Un ejemplo típico de "lo que la persona sabe" es la contraseña, que puede ser sustraída, olvidada o alterada; mientras que en el caso del método de "lo que la persona posee", el caso típico es del token o tarjeta de ingreso, con elemento físico que la persona lleva consigo y que también puede ser sustraída u extraviada.

Según la clasificación mencionada en el párrafo anterior, los sistemas biométricos encuadran dentro del tercer método, es decir: "lo que la persona es", y según Mender Bini (2024), "en la búsqueda de un método más confiable de reconocimiento, los sistemas biométricos resultan cumplir con dicho objetivo, por cuanto no se pueden compartir o extraviar. Ello así, en tanto que para su funcionamiento requiere de características inherentes de la persona que se quiere identificar, que se denominan características biométricas" (p. 64).

Muy brevemente diremos, a modo de referencia dado lo extenso y profundo que resulta la temática, que por estos días se debate arduamente en la mayoría de los países del planeta, y por ende también en Argentina, todo lo concerniente a una creciente actividad que tienen a su cargo aquello sistemas automatizados que en base a mecanismos de inteligencia artificial, y empleando determinadas técnicas y algoritmos, recolectan, sistematizan y clasifican de forma muy rápida y precisa, gigantescas cantidades de datos (big data) aplicando el paradigma de las conocidas "tres V" [21] (volumen, variedad y velocidad), a los fines de obtener información muy útil y de gran valor que le posibilitarán a los equipos encargados de tomar decisiones (en una empresa, en el estado, etc.) en tiempo real y con un alto grado de certeza, sobre aquellos "perfiles digitales" y características personales de los usuarios/consumidores previamente definidos según diferentes parámetros (rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación, etnia, género o movimientos de una persona), como así también, predecir comportamientos a futuro sobre aquellos, en función de sus gustos, intereses, condiciones, preferencias, etc.

[21] Las tres V del Big Data: volumen, variedad y velocidad. Para más información consultar: https://www.unir.net/ingenieria/revista/3-v-big-data/#:~:text=Las%20tres%20V%20del%20Big%20Data%20se%20refiere%20a%20los,adem%C3%A1s%20de%20sus%20principales%20retos.

Estos sistemas de I.A. encargados de movilizar grandes volúmenes de datos, están siendo muy utilizados principalmente por mega empresas de tipo transfronterizas o multinacionales (que no poseen localización geográfica exclusiva) y en menor medida por los estados en sentido amplio, con la finalidad de administrar y utilizar toda esa información obtenida en beneficio propio y en función del tipo de actividad que desarrollan, con el enorme riesgo que esto implica ante eventuales afectaciones de los derechos de los usuarios y/o consumidores por el uso indebido o desproporcionado de aquella información ya sea por parte de la propia empresa o por parte de terceros que la obtuvieron ilegalmente (por ej.: cuando se produce en la empresa una ex filtración de datos personales o sensibles de sus usuarios y/o consumidores; cuando compulsivamente una empresa direcciona su publicidad en función de la información que tiene en su poder, valiéndose de una previa aceptación de los términos y condiciones que le da vía libre para actuar de esa manera).

Dentro de los campos que investigan la I.A. se diferencian "dos grandes grupos: a) IA Débil o Artificial Narrow Intelligence (ANI) y; b) IA Fuerte o Artificial General Intelligence (AGI). Actualmente, es el primer grupo sobre el cual se está desarrollando; y se denominan débiles por cuanto su operatividad se encuentra limitada al ambiente para el cual fue programada" (Mender Bini, 2024, p. 97), dentro del grupo de las "débiles" encontramos una rama conocida como "machine learning" [22] o de aprendizaje automático, que tiene por tarea precisamente manipular grandes cantidades de datos que le suministra el sistema, bajo la modalidad de "aprendizaje" y con diferentes funciones, según se trate del tipo: "supervisados, no supervisados y de aprendizaje reforzado" (Mender Bini, 2024, p. 97-98).

Se ha desarrollado una técnica en el "machine learning" que, emulando al cerebro humano, ha creado redes neuronales artificiales o artificial neural networks (ANN), por la cual hay una especie de capa de entrada o input y una capa de salida u output, cuyo impacto en los sistemas biométricos y por aplicación de lo que se conoce como "deep learning" [23], estos sistemas "estarían siendo capaces de aprender representaciones faciales mientras tiene en cuenta diversos factores correlativos que inciden en el proceso. Incluso se pudo verificar que el desempeño de

[22] ¿Qué es el machine learning (ML)? Para más información consultar: https://www.ibm.com/es-es/topics/machine-learning

[23] ¿Qué es el deep learning? Para más información consultar: https://www.ibm.com/es-es/topics/deep-learning

varios métodos de Deep Learning supera al humano, llegando a porcentajes cercanos al 100% de acierto" (Mender Bini, 2024, p. 100-101).

Este cuadro de situación impone, pensar en un cambio de paradigma que implique, pasar del actual modelo de protección de datos, a uno más integral que propenda a garantizar el derecho humano de las personas, con fuerte incidencia en la "autodeterminación informativa como un concepto fundamental en la protección de datos personales, que se refiere al derecho que tienen las personas de tener control sobre la información que comparten y cómo se utiliza esa información. Este principio se basa en la idea de que las personas tienen el derecho de tomar decisiones informadas y conscientes sobre el manejo de su información personal" (C.F.T y A.A.I.P., 2023, p. 12), y muy especialmente sobre los datos, las finalidades y las actividades que se realizan como consecuencia de un procesamiento automático por I.A.

1.3. El "ataque" a la identidad. La "suplantación" o "robo" de identidad digital

En los últimos tiempos, se ha verificado un enorme crecimiento de casos de suplantación de identidad digital, "se ha transformado en el delito del milenio y es una de las actividades ilícitas de mayor crecimiento de la última década" (Temperini y Borghello, 2012, p. 79), debido en gran parte al vertiginoso avance de la tecnología que trajo aparejado que los valores económicos de los dispositivos tecnológicos disminuyeran notablemente, permitiéndole al ciberdelincuente acceder muy fácilmente a los mismos desde cualquier lugar del planeta; asimismo se observa, que las técnicas para su manipulación son cada vez más sencillas, lo que permite que cualquier persona los utilice para fines ilícitos, sea o no nativo digital[24], posea o no conocimientos de informática.

Tal como lo expresáramos en el capítulo anterior, la identidad de las personas es un derecho humano que goza de toda la protección legal que le brinda el sistema constitucional (tratados internacionales, constitución nacional, legislación nacional, etc.), por lo tanto, se admite excepcionalmente que "el Estado es, en principio, el único que puede afectar la identidad de

[24] Término acuñado por Marc Prensky en 2001, que se refiere a aquellas personas que han nacido en un mundo donde la tecnología y los dispositivos conectados a internet son parte integral de sus vidas. Para más información consultar: https://canalsalud.img.es/blog/nativo-digital

una persona" (Liceda, 2011, p. 297), salvo en determinados casos en función de lo establecido en la ley 25.326 y en las leyes o disposiciones complementarias.

En esta idea, Liceda (2011) sostiene que "para que la identidad de alguien pueda ser atacada por un particular se debe dar la circunstancia de que el mismo se encuentre en una situación tal que le permita conocer alguno de los datos troncales de la persona y tenga la capacidad de cambiarlo (en un instrumento público), de modo que la persona afectada no pueda conocer su situación anterior" (p. 297).

Continuando con lo expresado en el último párrafo, diremos que el particular que ataca la identidad digital de una persona (víctima) es el ciberdelincuente, y lo hará utilizando técnicas de manipulación informáticas o no informáticas (por ej: ingeniería social[25]), las que le permitirá acceder legal o ilegalmente a información digital personal y sensible de la víctima (por ej: datos bancarios, credenciales de acceso a una red social, videos o imágenes intimas, lista de contactos, etc.), para posteriormente interactuar con aquella información sustraída en el ecosistema digital "fingiendo" ser la persona suplantada, ya sea para cometer un ciberfraude o cualquier otro tipo de delito que implique la utilización de dispositivos digitales (por ej: calumnias e injurias, amenazas, difusión de material sexual, sextorsion, etc.), o también se puede dar el caso que simplemente no cometa ninguno, quedando aún latente la posibilidad de que en cualquier momento se produzca la efectiva lesión a un bien jurídico, ya sea por el mismo sujeto que obtuvo aquella información, o por un tercero que la obtuvo posteriormente.

Se afirma que "el robo de identidad es un delito complejo, pues afecta diversos bienes jurídicos penalmente protegidos: la privacidad, la propiedad y el honor" (Palazzi, 2016, p. 102)[26], cuyos efectos son tan nocivos que contribuyen a generar un caldo de cultivo suficiente para provocar un verdadero estado de "incertidumbre", no tan solo para quienes han sido víctimas de la "perdida" de su identidad digital que sigue ahora en manos del ciberdelincuente o de un tercero, sino también para la sociedad en su conjunto, que observa la impunidad en este tipo de conductas por falta normativa legal.

[25] Se llama ingeniería social a las diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios. Para más información consultar: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-ingenieria-social-y-como-protegerte

[26] Palazzi, Pablo A. (2016). Los Delitos informáticos en el código penal. Análisis de la ley 26.388. Bs.As., Argentina. Ed. Abeledo Perrot.

Vale destacar, que todo lo relacionado con la "ciberviolencia digital", se encuentra estrechamente vinculado con lo que aquí se analiza, ya que en la práctica se ha verificado una gran cantidad de casos de victimas de "suplantación de identidad", que luego sufrieron hechos de esta naturaleza como consecuencia de haber "perdido" el control y por ende la posibilidad de acceder normalmente a sus cuentas digitales personales (redes sociales, cuentas bancarias, membresías en sitios de citas, correos electrónicos, videojuegos en línea, etc.), con la particularidad que en la gran mayoría de esas víctimas fueron mujeres, niños, niñas y adolescentes.

En el caso puntual de las mujeres, adquiere el nombre de "ciberviolencia de género contra las mujeres (ciberVCM)[27]", y que si bien, por la extensión, profundidad y relevancia que tiene esta problemática, debería ser estudiada en un trabajo específico dedicado exclusivamente a tal fin, nos limitaremos aquí a esbozar algunas referencias puntuales que permitan dimensionar su importancia y genere curiosidad en el lector para que posteriormente profundice sus conocimientos al respecto.

Para entender mejor el contexto al que se expone una mujer víctima de ciberviolencia digital, es importante reiterar una vez más que "algunos aspectos de las TIC han contribuido a la transformación y potenciación de este tipo específico de manifestación de violencia psicológica al promover su rápida expansión, la permanencia en línea de contenidos que dejan un registro digital indeleble, su replicabilidad y alcance global, y la posibilidad de localizar fácilmente a personas e información sobre ellas" (Vaninetti, 2023, p. 2)[28], esto se entiende en función de que "las características típicas de los entornos digitales hacen que se potencie la capacidad de daño,

[27] Definida como: "todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada". O.E.A. & O.N.U. Mujeres. (2021). *Informe sobre ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la convención belém do pará*. Publicación de la iniciativa Spotligth. Recuperado de *https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20linea%202.1%20%282%29_Aprobado%20%28Abril%202022%29_0.pdf*

[28] Vaninetti, Hugo Alfredo (2023). *La violencia digital y el proyecto de ley olimpia. Una necesidad imperiosa*. Bs.As., Argentina. Ed. Rubinzal Culzoni. Recuperado de https://media.licdn.com/dms/document/media/D4D1FAQFi4-KiaHlPuQ/feedshare-document-pdf-analyzed/0/1689363834391?e=1712188800&v=beta&t=KRZUdrro02j-gUuqendB6arXmybFfsHito-MPCYDxM8

a la vez que dificultan la identificación de los agresores y el control de las conductas abusivas" (MPD, 2023, p. 12)[29].

La gravedad de la situación se vislumbra cuando "la amenaza abandona la digitalidad y se vuelve un daño físico, por ejemplo, a través de la publicación de material con contenido sexual y la difusión de datos personales que permiten identificar y abordar a las víctimas" (MPD, 2023, p. 13), o cuando "si bien inicialmente son ejercidas por un individuo contra una mujer en particular o un grupo de ellas, eventualmente pueden tornarse, feroz y velozmente, en colectiva, porque el medio virtual así lo posibilita. Prueba de ello son los comentarios y sus réplicas al contenido primigenio de violencia realizados por terceros en distintas plataformas on line que denigran a las víctimas por su género" (Vaninetti, 2023, p. 2).

Con la sanción de la Ley N° 27.736[30], conocida como "Ley Olimpia", se introdujeron "varias modificaciones a la Ley de Protección Integral para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres (ley 26.485)[31], orientadas a reconocer la discriminación y acoso en entornos digitales como una modalidad de la violencia de género, y procurar la protección de los derechos de las mujeres, así como su desenvolvimiento y permanencia en el espacio digital" (MPD, 2023, p. 14-15). Asimismo, en dicho cuerpo legal se instituyeron una serie medidas protectorias trascendentales, entre las que se mencionan: la ampliación del "piso de los derechos y garantías mínimas que aplican a los procedimientos judiciales y administrativos" (MPD, 2023, p. 16), medidas de prevención urgentes que contempla "incluir los espacios digitales en las órdenes de restricción del agresor" (MPD, 2023, p. 16), "la posibilidad de requerir a los proveedores de servicios digitales la eliminación, conservación y/o divulgación de información que configure el ejercicio de violencia digital" (MPD, 2023, p. 17) o la implementación de programas de alfabetización digital, buenas prácticas en el uso de las tecnologías de la información y la comunicación y de identificación de las violencias digitales, entre otras.

[29] Ministerio Público de la Defensa de la República Argentina (noviembre de 2023). *Violencia de género en entornos digitales. Guía básica para la obtención e implementación de órdenes de protección y boletín de jurisprudencia*. Recuperado de https://www.mpd.gov.ar/pdf/publicaciones/biblioteca/LibroViolenciaDigital.pdf

[30] Ley N° 27.736. Ley Olimpia. Modificación a la Ley N° 26.485 (23/10/2023). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/390000-394999/391774/norma.htm

[31] Ley N° 26.485. *Ley de Protección Integral para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres en los ámbitos en que desarrollen sus relaciones interpersonales-Violencia contra la Mujer* (20/07/2010). Recuperado de https://www.argentina.gob.ar/sites/default/files/ley_26485_violencia_familiar.pdf

Más allá de la importancia de la sanción de la "Ley Olimpia", está más que claro que como bien se puede observar en la historia reciente, "la ciberviolencia digital ha variado desde los orígenes de la internet, y seguramente evolucionará a medida que las plataformas digitales y las herramientas tecnológicas sigan avanzando e interrelacionándose aún más en nuestro quehacer diario, como, por ejemplo, con la irrupción próxima, y masiva, del metaverso" (Vaninetti, 2023, p. 4), lo que requerirá de una constante revisión y/o actualización de la normativa vigente, como así también "surge como necesario incluir figuras penales que engloben a diversas prácticas de ciberviolencia" (Vaninetti, 2023, p. 6), entre los cuales sugerimos en el presente trabajo que debe ser incluida la suplantación de identidad.

1.3.1. Aspectos distintivos y particulares

A grandes rasgos y de una manera clara, la doctrina mayoritaria entiende que en la práctica la suplantación de identidad se produce cuando, una persona se hace pasar por otra para conseguir algún tipo de beneficio, al que no tendría derecho si conservase su identidad original, es decir "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" (Monastersky y Salimbeni, 2012, p. 5)[32] y que "la mayoría de los ataques de este tipo incluyen la generación del escenario falso para que la víctima incurra en un error, donde el ingeniero social se hace pasar por otra persona" (Riquert y Sueiro, 2020, p. 77)[33].

La Real Academia Española (R.A.E.) define a "la suplantación de dos maneras: 1) falsificar un escrito con palabras o cláusulas que alteren el sentido que antes tenía y 2) ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba" (Real Academia Española, s.f.)[34], la segunda de las definiciones sería la más acorde con el ámbito digital.

[32] Monastersky, Daniel & Salimbeni, Matías (2012). *Introducción al robo de identidad*. Primera Edición. Bs.As., Argentina. Teclawbiz. Techonology + Law + Bussiness. Recuperado de https://www.identidadrobada.com/wp-content/uploads/2021/10/eBook-Robo_de_identidad.pdf

[33] Riquert, Marcelo A. y Sueiro, Carlos Christian. (2020). *Sistema penal e informática. Ciberdelitos. Evidencia digital. Tics. Volumen 3.* Bs.As., Argentina. Ed. Hammurabi.

[34] Real Academia Española. (s.f.). Suplantación. En diccionario de la lengua española. Recuperado el 24 de marzo de 2024 de https://dle.rae.es/suplantar

Como se dijo anteriormente, la complejidad propia del delito de suplantación de identidad, impide se pueda dimensionar adecuadamente los problemas que genera y sus consecuencias, no obstante, "se puede categorizar a cuatro tipos de víctimas: los gobiernos, las empresas privadas que manipulan gran cantidad de datos personales, los servicios financieros y, principalmente, a los clientes y usuarios" (Temperini y Borghello, 2012, p. 82).

El panorama que se avecina es muy incierto y no es para nada aventurado expresar que la realidad está superando ampliamente a la ficción, "a tal punto, está llegando la sustitución de identidad a niveles insospechados, que en la actualidad se está llevando a cabo la creación de noticias falsas (Fake News) o incluso peor, falsificaciones profundas (Deep Fake) de videos, imágenes o audios de principales jefes de Estado mandatarios mediante sofisticados programas de Inteligencia Artificial (IA) tales como Deep Fake o Lyrebird, que permiten imitar la imagen y el registro de voz de la persona que se desea suplantar" (Aboso y otros, 2022, p. 539).

1.4.2. Técnicas o modalidades de suplantación de identidad

Es dable mencionar, que "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" (Temperini y Borghello, 2012, p. 80) y que las formas más variadas de formas o métodos que los ciberdelincuentes utilizan para delinquir, responde a que "desde los comienzos de la globalización vía internet y la digitalización de casi todas las actividades, la sustitución de identidad puede llevarse a cabo acudiendo a medios digitales o informáticos" (Aboso y otros, 2022, p. 538).

Simplemente a modo ejemplificativo, y sin ánimo de pretender realizar una enumeración taxativa, debido al incesante avance tecnológico que día a día produce significativas modificaciones en el escenario ciberdelictivo, mencionamos que la "recolección de información personal y sensible puede ser física o virtual, y algunas de las técnicas que existen para apoderarse de esta información son: Robo de documentación personal, arrebatos de billeteras, carteras, bolsos, etc; Dumpster diving (hurgar en la basura): recolección de documentación que fue descartada o arrojada a la basura; Robo de información a través de empleados deshonestos en organizaciones que manipulan los datos personales; Skimming: obtención de información de las bandas magnéticas de tarjetas de crédito o débito con la finalidad de reproducir o clonar

dicha tarjeta y luego utilizarla con fines delictivos; Phishing y scam (estafa): recolección de información personal a través de diversos métodos tecnológicos en los cuales se busca engañar a la víctima para que revele esa información" (Temperini y Borghello, 2012, p. 82-83).

El "phising", una de las modalidades más populares, se refiere "a una modalidad de robo de identidad digital que utiliza técnicas de la ingeniería social para obtener información sobre la víctima y hacerla caer en la trampa. Es el arte del engaño en su máxima expresión" (Monastersky y Salimbeni, 2012, p. 9), consiste básicamente en "la capacidad de duplicar un sitio web para hacerle creer al visitante que se encuentra en la página original del banco o entidad" (Monastersky y Salimbeni, 2012, p. 9), por lo tanto, una vez que la víctima accede a ese sitio web apócrifo, por medio de un enlace que le llegará vía correo electrónico, mensaje de texto o SMS (Smishing)[35], mensaje de whatsapp, de facebook, telegram, etc; procederá a ingresar sus credenciales (nombre de usuario, contraseñas, número de tarjeta de crédito, clave de seguridad de la tarjeta de crédito, etc.) con la convicción que lo está haciendo en el sitio oficial o legítimo de la empresa o entidad en la que está previamente registrado como usuario, entregándole en ese mismo instante toda esa valiosísima información al ciberdelincuente.

La técnica de "spear phishing"[36], difiere con la del "phishing", en cuanto el ataque no es de tipo aleatorio y generalizado como si sucede en el segundo caso, sino que está direccionado a una organización o individuo en particular, con altas probabilidades de éxito, por cuanto el atacante realiza una investigación previa de su objetivo, en "una secuencia que comprende: 1) identificación del sitio web de la organización a atacar, 2) detección en dicho sitio web, de un sector interno que requiera autorización para ingresar (por ej: usuario y contraseña), 3) selección en el sitio web de la organización, de los datos de contacto (correo electrónico) de un empleado con cargo jerárquico al cual el atacante le enviara un mail fingiendo ser empleado del área de administración de redes de la empresa, 4) por ultimo le envía un mail a un empleado de la

[35] El Smishing: se configura con el envío de mensajes de texto a los celulares de la víctima, que simulan provenir de entidades o empresas, incitándolos a enviar sus datos personales previo a ingresar al enlace que dichos mensajes contienen, con la excusa de participar de sorteos, promociones, actualizaciones de datos, inscribirse para turnos de vacunación, etc.

[36] Spear phising: es un tipo de ataque de phishing que se dirige a un individuo o grupo de individuos específicos dentro de una organización, e intenta engañarlos para que divulguen información confidencial, descarguen malware o envíen sin saberlo nuestros pagos de autorización al atacante. Para más información consultar: https://www.ibm.com/mx-es/topics/spear-phishing#:~:text=Spear%20phishing%20es%20un%20tipo,pagos%20de%20autorizaci%C3%B3n%20al%20atacante

empresa solicitándole le suministre información confidencial (por ej: nombre de usuario y contraseña del área restringida de la empresa en la web) configurándose de esta manera la suplantación de identidad" (Montaperto, 2018, p. 19)[37].

En la modalidad denominada "pharming", nos encontramos con "un "phishing" avanzado y más difícil de detectar. A través de un "troyano"[38] (software espía malicioso) se modifica un archivo que administra la asignación de nombres de dominio. Técnicamente se lo llama envenenamiento de los DNS, que son los encargados de asignar un numero IP a una dirección de Internet" (Monastersky y Salimbeni, 2012, p. 11). En este caso, el usuario cree ingresar al sitio correcto de la entidad o empresa de la cual es usuario, pero por efecto de este "envenenamiento" de DNS termina en otro sitio web diferente donde se produce finalmente la sustracción de sus datos personales.

La obtención de datos de usuarios también se puede realizar por medio de los "llamados "keylogger"[39], que se instalan generalmente en computadoras de uso público, y transmiten al ladrón de identidad todo lo que el usuario escriba en esa computadora infectada. En este aspecto, los denominados "screen scrapers" son otra modalidad parecida porque registran todas las imágenes que el usuario ve en el monitor" (Monastersky y Salimbeni, 2012, p. 11).

A través del "vishing"[40], el ciber atacante obtiene información sensible de la víctima comunicándose por una llamada de telefónica, fingiendo pertenecer a una entidad o empresa determinada. Cabe destacar que este tipo de modalidad delictiva, ha tenido un crecimiento exponencial en los últimos años, especialmente con la utilización de la red social whatsapp, servicio de mensajería muy utilizado en nuestro país que le permite al ciberdelincuente entablar

[37] Montaperto, Javier Eduardo (2018). Suplantación de identidad. Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino. Trabajo final de graduación de la carrera de abogacía de la Universidad Siglo 21. Recuperado de https://repositorio.uesiglo21.edu.ar/handle/ues21/15652

[38] Un Troyano es un software malicioso que se encuentra disfrazado o camuflado de tal forma que, en algunas ocasiones no puede ser detectado y se infiltra en el dispositivo digital. Para más información consultar: https://www.eset.com/es/caracteristicas/malware-troyano/

[39] Un keylogger es un hardware o software malicioso que, sin el permiso o conocimiento de la víctima, registra todas las teclas que pulsa cuando opera su computadora o teléfono celular. Para más información consultar: https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-un-keylogger#:~:text=Un%20keylogger%20es%20un%20hardware,operar%20tu%20computadora%20o%20celular

[40] El vishing es un tipo de estafa de ingeniería social por teléfono en la que, a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima. Para más información consultar: https://www.incibe.es/aprendeciberseguridad/vishing

comunicaciones de voz y/o audiovisuales con su víctima, con solamente tener acceso a internet y habiendo obtenido previamente su número telefónico.

En este sentido, el ciberatacante, para poder llevar a cabo algunas de las modalidades anteriormente descriptas, requiere obtener previamente los números telefónicos de sus víctimas, para lo cual realizará una modalidad muy actual que consiste en "sustraer" la cuenta de whatsapp a una persona determinada. El atacante mediante técnicas de ingeniería social, fingiendo ser empleado de una empresa o entidad, le solicitará a la víctima que le reenvíe un código numérico que la red social "Whatsapp" le envió previamente a su teléfono celular, bajo el engaño por ej.: de que dicho código será necesario para concretar una transferencia o una devolución de dinero que tenía a su favor. Es importante aclarar que el código que el atacante le pide a su víctima, es mecanismo de seguridad y/o de validación que tiene la red social Whatsapp, en aquellos casos en que alguien necesita migrar aquella red social (junto a todos sus contactos, conversaciones, etc) a otra línea telefónica, ya que ésta red social tiene la particularidad, a diferencia de otras redes sociales (por ej: facebook o instagram requiere de un mail y contraseña para su registro), que el "alta " o registro del usuario estará asociada o identificada a la titularidad de una determinada número de línea telefónica.

El paso siguiente del ciberdelincuente, una vez que ha obtenido el control total de la cuenta de usuario de whatsapp de la víctima, será acceder a todo el contenido de aquella y en especial respecto a la lista de usuarios o contactos con los cuales la victima interactuaba; luego intentará entablar algún tipo de comunicación (generalmente por mensajes escritos) fingiendo ser la persona suplantada, para lo cual realizará cualquier tipo de pedidos o "favores" (generalmente solicitando transferencias de dinero, por ej: aduciendo estar en un situación de extrema necesidad); produciéndose de esta manera la comisión de nuevos delitos y consecuentemente nuevas víctimas, a partir de la concreción de las disposiciones patrimoniales concretadas en beneficio del ciberestafador o de un tercero. A modo de humilde colaboración, con la finalidad de aportar un granito de arena en la constante tarea de concientización que nos compete a todos en pos de un adecuado uso de internet y las redes sociales, sugerimos a los usuarios de "whatsapp" activar la opción de verificación de dos pasos[41].

[41] Activación de la verificación de dos pasos en whatsapp. Para más información consultar: https://faq.whatsapp.com/1920866721452534/?locale=es_LA

1.4.3. El intrusismo informático o hacking ético

Para apreciar adecuadamente las diferencias que existen entre la suplantación de identidad y el intrusismo informático, debemos entender qué tipo de actividad realiza un hacker en el estricto sentido de la palabra (hacking), haciendo mención que principalmente los medios de comunicación, han realizado a lo largo del tiempo una inadecuada asociación o equiparación de la misma con actividades de tipo delictivas, desconociendo que cuando se habla de hacker se "hace referencia a personas que poseen un alto grado de interés en el desarrollo de la informática, de programas de uso libre, y del mejoramiento del sistema en su totalidad" (Rosende, 2007, p. 12)[42].

Tanto a nivel doctrinario como en la jerga informática, se distingue específicamente el "hacking" del "cracking" que comprende a la "piratería informática" y el "ciberpunking", en este aspecto, nos enseña Rosende (2007), que "el cracking es una actividad necesaria para permitir la violación de los sistemas de seguridad de los programas de computación protegidos por la ley de Propiedad Intelectual (11.723) mientras que el ciberpunking sería la actividad de destrucción de datos e información digital" (p. 5).

Antes de avanzar en la definición del "hacking", señalamos que para el "mundo informático" existen dos tipos de "hacking" en función de la finalidad con la que el "hacker" realiza su actividad, de tal modo que por un lado tenemos lo que se conoce como "hacking" ético a cargo de "hackers blancos", y por el otro lado tenemos un "hacking no ético" que se encuentra en cabeza de los famosos "hackers negros", estando en presencia en este último supuesto frente a ciberdelincuentes que cometen delitos previstos y penados por la ley.

Por lo expuesto, se entiende que "el hacker blanco es aquel que tiene un interés en los sistemas informáticos, dedicándose a su estudio, a la programación, a la búsqueda de vulnerabilidades y al mejoramiento de todo el sistema" (Rosende, 2007, p. 6), lo que significa que en su realización no hay una finalidad de tipo delictiva, sino que más bien se desarrolla con diversos motivos, en la mayoría de los casos adquiere una forma lúdica o de entretenimiento, también como una

[42] Rosende, Eduardo E. (2007). *El intrusismo informático. Reflexiones sobre su inclusión al código penal.* Ponencias del VII Encuentro realizado en Buenos Aires, Argentina, el 11 de octubre de 2007. Publicado por la AAPDP (Asociación Argentina de Profesores de Derecho Penal). Recuperado de https://aapdp.com.ar/wp-content/uploads/1661/54/03rosende.pdf

actividad rentada (por ej.: los programas de bug bounty)[43], o con fines altruistas en función del bien común (por ej: beneficiar usuarios de un determinado software libre), puede también manifestarse como una forma de obtener algún prestigio, estatus o reconocimiento dentro del sector en el que interactúan.

Se habla de la presencia de una zona gris dentro del derecho penal en la actividad que realizan los "hackers blancos", ya que salvo cuando realizan los conocidos "pentesting"[44] o "test de penetración", en los demás casos utilizan "métodos y técnicas a los efectos de acceder a sistemas informáticos sin autorización de sus titulares, eludiendo todas las medidas de seguridad lógicas implementadas para evitar ese objetivo" (Rosende, 2007, p. 6), ante lo cual un sector de la doctrina sostiene que dicha actividad debe ser catalogada como delito, especialmente cuando el "intrusismo" pudo constituirse como un acto previo para cometer otros delitos más severos o cuando por esta vía pudo obtenerse información personal sensible del titular del sitio web, sistema o software accedido.

Entendemos que la actividad del hacking ha sido muy beneficiosa tanto para las empresas como para los usuarios en general, en efecto, la detección a tiempo de vulnerabilidades o fallas y la posterior puesta en conocimiento de las mismas para la comunidad informática, ha permitido mitigar e incluso evitar grandes pérdidas económicas y los graves perjuicios que derivan de la concreta posibilidad que tienen los ciberdelincuentes de acceder fácilmente a base de datos sensibles (tanto de empresas como de particulares); lo que no implica que el "intrusismo" no deba ser regulado legalmente, todo lo contrario, deberá ser penada como delito cuando el "intruso" valiéndose de un medio informático viole la intimidad por infringir parámetros mínimos de seguridad y cuando el bien jurídico intimidad o privacidad sea realmente afectado, quedando de esta manera sin punir el mero acceso o comprobación de vulnerabilidades de un sistema informático (Rosende, 2007, p. 16).

[43] Bug bounty: Es un "contrato" que una empresa u organización hace con una comunidad de hackers éticos con el fin de que éstos detecten vulnerabilidades en los sistemas y redes de dicha empresa. Para más información consultar: https://kippeo.com/bug-bounty-todos-necesitan-un-hacker/

[44] Pentesting: es una abreviatura formada por dos palabras "penetration" y "testing" y es una práctica/técnica que consiste en atacar diferentes entornos o sistemas con la finalidad de encontrar y prevenir posibles fallos en el mismo. Para más información consultar: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

Capítulo 2. Marco normativo referente a la suplantación de identidad

2.1. Introducción.

Antes de comenzar con el desarrollo del presente tema, es loable mencionar nuevamente que el trabajo gira en torno a poner en evidencia aquellos comportamientos ilícitos, previos y necesarios, que un ciber atacante puede ejecutar (o no) y que forman parte del accionar típico de un ciberfraude, comportamientos que no se encuentran regulados como delitos autónomos hasta la fecha en nuestro sistema penal, y que tampoco se encuentran atrapados por otras figuras penales vigentes que pudieran llegar a consumarse con posterioridad, como consecuencia de la información obtenida por aquellos comportamientos atípicos.

En esta línea de pensamiento, existe una modalidad delictiva que sobresale claramente por tratarse de una conducta muy difundida y conocida por todos, cuya lesividad real o potencial no encuentra límite alguno; nos referimos concretamente al delito de "robo o suplantación de identidad", siendo analizada dicha figura penal desde las diferentes regulaciones penales que la reconocieron como tal, para luego investigar el tratamiento legislativo que recibió en nuestro país.

En cuanto a la forma en que los países regularon la suplantación de identidad, del mismo modo que aconteció con el resto de los delitos informáticos, lo hicieron de dos maneras, a saber: a) sancionando una ley específica complementaria del código penal y b) reformando el código penal agregando nuevos capítulos, artículos o ubicándolos en algunos de los títulos existentes en función del bien jurídico a tutelar. En nuestro país, los legisladores optaron por la segunda opción cuando incorporaron los delitos informáticos al código penal, es decir incluyeron los diversos tipos penales en forma desconcentrada en diversos títulos del libro segundo del código penal según los objetos jurídicos que cada uno tutela (Arocena, 2012, p. 954)[45].

[45] Arocena, Gustavo. (2012). *La regulación de los delitos informáticos en el código penal argentino. Introducción a la ley nacional núm. 26.388.* Publicado en Boletín Mexicano de Derecho Comparado, Vol XLV, num. 135, p.945-988. Recuperado de https://www.redalyc.org/articulo.oa?id=42724584002

2.2. Convenio sobre la ciberdelincuencia. El convenio de Budapest

Desde una mirada más amplia, y por la importancia que tiene no solo en nuestro sistema legal con rango constitucional por su expresa incorporación en el art. 75° de la constitución nacional, sino también a nivel continental, mencionamos a la Convención Americana de los Derechos Humanos[46], que en su art. 11 protege la identidad digital de las personas en cuanto "se hace especial detalle sobre la protección de la honra y la dignidad de las personas, elemento que es de suma utilidad al momento de analizar los efectos dañinos de la suplantación de identidad y la justificación en su protección" (Temperini y Borghello, 2012, p. 86).

En materia de ciberdelitos, sin lugar a ningún tipo de dudas que el convenio marco por excelencia y de referencia en la materia como fuente principal de inspiración para las legislaciones de los países de todo el planeta, es el "Convenio sobre la Ciberdelincuencia" más conocido por todos como el "Convenio de Budapest"[47], considerado como el único acuerdo internacional sobre delitos informáticos que regula específicamente todo lo atinente a la ciberdelincuencia, y del cual la República Argentina forma parte por su adhesión al mismo a través de la Ley N° 27.411[48] de fecha del 15/12/2017, adhesión que fue hecha con reservas (art. 2°) con respecto a la mal llamada pornografía infantil y algunas cuestiones jurisdiccionales en esa materia; no obstante cabe mencionar que dicho texto supralegal de plena vigencia en Argentina, se encontraría para un sector de la doctrina, en una escala intermedia (no tiene el mismo rango constitucional) con respecto a los tratados de derechos humanos reconocidos en el art. 75° Inc. 22 de la Constitución Nacional Argentina.

---

[46] Convención Americana sobre los Derechos Humanos (C.A.D.H. – Pacto de San José de Costa Rica, 1969)
Artículo 11. Protección de la Honra y de la Dignidad
1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.
Recuperado de https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

[47] *Convenio sobre la ciberdelincuencia* (23/11/2001, Budapest) y sus dos protocolos. Recuperado de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

[48] Ley N° 27.411. *Convenio sobre ciberdelito. Aprobación* (15/12/2017). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm

Fue impulsado por el Consejo de Europa con el Apoyo de EE.UU, tuvo su aprobación el día 23/11/2001 en la ciudad de Budapest, Hungría, con un total de 44 estados firmantes miembros del Consejo de Europa y algunos estados no miembros como: Argentina, Canadá, Chile, Colombia, Estados Unidos de América, República Dominicana y Perú, contando en la actualidad con más de 150 estados involucrados de una u otra manera con dicha normativa, a saber: 67 estados forman parte del convenio, 2 estados se encuentran en calidad de firmantes, 13 estados fueron invitados a formar parte del convenio, hay más de 45 países en los cuales sus leyes sustantivas coinciden en líneas generales con la convención, y hay más de 30 países que han recurrido al convenio para establecer sus legislaciones sustantivas locales.

En el mencionado instrumento legal se clasifican a los delitos informáticos en cuatro categorías, a saber: a) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; b) delitos informáticos propiamente dichos, falsificación y estafa informática; c) delitos relacionados con contenidos; y d) violaciones a la ley de propiedad intelectual.

En relación a su estructura interna, se reconocen las siguientes partes y contenidos: A) un preámbulo que reconoce: la necesidad de adoptar una política común adoptando una legislación apropiada, la necesidad de cooperación entre los estados y las empresas privadas en la lucha contra la cibercriminalidad y la necesidad de prevenir actos que pongan en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, garantizando la tipificación de dichos actos como delitos; y B) cuatro capítulos: B1) Cap.1: Terminología: que comprende definiciones de sistema informáticos, datos informáticos, proveedor de servicios y datos de tráfico; B2) Cap. II: Medidas que deben adoptarse a nivel nacional: por la que compromete a las partes a tomar medidas tanto desde el derecho penal sustantivo con respecto a: acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la seguridad del sistema, abuso de equipos e instrumentos técnicos, falsedad informática, estafa informática, pornografía infantil y atentados a la propiedad intelectual, y desde el Derecho Procesal: a los fines de determinar el ámbito de aplicación de las disposiciones de procedimiento a los efectos de investigación o de procedimientos penales específicos, las condiciones y garantías (salvaguardas) y medios para conservación, divulgación, comunicación, registro y decomiso, interpretación de datos, normas referentes a competencia y jurisdicción; B3) Cooperación internacional: normas referentes a extradición,

colaboración, asistencia mutua, adhesión e implementación del convenio en cuestiones específicas, y por ultimo B4) Cap. IV: Disposiciones finales.

Años más tarde, en cumplimiento del art. 46° del convenio de Budapest, que establece la posibilidad de aplicar mecanismos de constante revisión del tratado por parte de los estados miembros, se publicó el "Primer protocolo adicional" denominado "Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos"[49] de fecha 28/01/2003, entrando en vigor a partir de 2006, tuvo "como principal objetivo promover una mayor armonización entre legislaciones relevantes en el ámbito del derecho criminal sobre la lucha contra el racismo y la xenofobia en internet" (Martins dos Santos, 2022, p. 9)[50].

Este primer protocolo se compone de los siguientes 4 capítulos: a) Capítulo I: Disposiciones comunes y cuestiones generales; b) Capítulo II: Medidas a ser tomadas a nivel nacional: Difusión de contenidos racistas y xenófobos por sistemas, amenazas por motivos racistas y xenófobos, insultos por motivos racistas y xenófobos, negación, minimización, aprobación o justificación de genocidios y crímenes contra la humanidad; c) Capítulo III: Relaciones entre el Convenio y el Protocolo y d) Capítulo IV: Disposiciones finales. En definitiva, se concluye en que esta normativa complementaria tuvo como misión principal "establecer una dinámica equilibrada entre la libertad de expresión de los usuarios de Internet y una lucha eficaz contra la difusión y la práctica del racismo y la xenofobia en el ámbito digital" (Martins dos Santos, 2022, p. 10).

Desde la aparición del convenio allá por 2001, el escenario internacional con respecto a la ciberdelincuencia se complejizó de tal manera que se constituyó en una amenaza para los derechos humanos, la democracia y el estado de derecho; por lo que fue indispensable se implemente una urgente "actualización" que dé respuesta a problemas tales como: el aumento considerable de la ciberdelincuencia a nivel global, la incidencia de las pruebas electrónicas o digitales en casi todos los delitos (aun los no informáticos), la existencia de pruebas que se

[49] *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.* (28/01/2003, Estrasburgo). Recuperado de https://rm.coe.int/1680a7bbf3

[50] Martins dos Santos, Bruna (2022). *Convenio de Budapest sobre la Ciberdelincuencia en América Latina.* Derechos Digitales América Latina. Recuperado de https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

encuentran en algún lugar ya sea en jurisdicción extranjera, múltiples o incluso cambiantes, la no disposición de medios eficaces para la divulgación de pruebas digitales, la falta de justicia para las víctimas de ciberdelincuencia en función de que solo el 0,1 % de los casos a nivel mundial terminan en juicios y/o condenas, etc.

En este contexto, el 12/05/2022 vió a la luz el "Segundo protocolo adicional" al Convenio de Budapest "relativo a la cooperación reforzada y la divulgación de pruebas electrónicas"[51], transformándose en "una actualización necesaria para convertir el Convenio de Budapest en un instrumento más eficaz al tiempo que revisa cuestiones como el acceso transfronterizo a los datos y la cooperación legal mutua, y establece parámetros más claros para la cooperación directa entre las autoridades y los proveedores de servicios digitales, inclusive en el nivel de los proveedores de servicios de infraestructura de internet" (Martins dos Santos, 2022, p. 13).

Su estructura se conforma de un preámbulo y cuatro capítulos: a) Capítulo I: Disposiciones generales o comunes que refieren a la finalidad, ámbito de aplicación, definiciones e idioma; c) Capitulo II: Medidas de cooperación reforzada que comprende los principios generales que se aplicaran, solicitud de información sobre el registro de nombre de dominio, divulgación de información de abonados, dar efecto a las órdenes de la otra parte para la producción acelerada de información sobre abonados y datos de tráfico, divulgación acelerada de datos informáticos almacenados en caso de emergencia, asistencia mutua en caso de emergencia, videoconferencia, equipos conjuntos de investigación e investigaciones conjuntas; c) Capitulo III: Condiciones y salvaguardias que abarca los principios generales y la protección de los datos personales; d) Capitulo IV: Disposiciones finales y de asuntos de procedimiento que brinde respuesta sobre los efectos del protocolo, la firma y entrada en vigor, fijación de una cláusula federal, la aplicación territorial, reservas y declaraciones, situación y retirada de las reservas, enmiendas, solución de controversias, consultas de las partes y evaluación de la aplicación, denuncia y notificación.

A pesar de que este segundo protocolo adicional, se consolidó como un instrumento legal muy importante para mejorar la performance de las investigaciones penales, supo generar un interesante debate que "ha movilizado a diversos sectores, en particular a la sociedad civil internacional, debido al intento del Comité Europeo de establecer nuevas normas de aplicación

[51] *Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas.* (12/05/2022, Estrasburgo). Recuperado de https://rm.coe.int/1680a83724

de la ley que van a contramano de los principios de protección de datos personales y privacidad" (Martins dos Santos, 2022, p. 13).

2.3. La suplantación de identidad en el derecho comparado

En Estados Unidos de Norteamérica, existen varias legislaciones que contemplan el robo de identidad o "identity theft", entre las cuales se destacan: "la Ley de Modernización Bancaria se aprobó en noviembre de 1999 y contiene todo un conjunto de normas federales sobre privacidad bancaria. Ella contiene un título V denominado The Financial Privacy Law, con dos subtítulos: el A, relativo a nuevas obligaciones sustantivas relacionadas con la revelación de datos personales por parte de entidades financieras a terceras partes no afiliadas, y un B, que establece nuevos delitos federales que penalizan la adquisición fraudulenta de información sobre clientes bancarios" (Palazzi, 2016, p. 103).

Posteriormente, nos cuentan Monastersky y Salimbeni (2012), que allá por "el año 2004, se promulgó la Identity Theft Penalty Enhancement (Ley de incremento de Sanciones por el robo de identidad). A fines del 2004 la Fair and Acurate Credit Transactions Act fue promulgada para complementarse en algunos aspectos con la anterior norma. Esta ley es la que posibilita, en uno de sus puntos, alertar a las centrales de riesgo sobre el robo de identidad y así proteger el historial crediticio por un plazo determinado" (p. 32).

En definitiva, la legislación vigente a nivel federal de aquel país, define la figura de robo de identidad cuando su autor "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, mientras que en algunos estados como New York se configura el delito cuando alguien, usurpa la identidad de otro a través de internet o medios electrónicos, con la intención de obtener un beneficio o injuriar o defraudar a otro..." (Temperini y Borghello, 2012, p. 89).

En Canadá, existe una la ley federal que define el robo de identidad 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" (Temperini y Borghello, 2012, p. 89).

En el Reino Unido, el robo de identidad se tipifica con "el acto por el cual alguien obtiene información suficiente acerca de la identidad de otro para facilitar el fraude de identidad, con independencia de que la víctima esté viva o muerta" (Temperini y Borghello, 2012, p. 90), redacción no tan solo curiosa sino también controvertida, ya que admite la posibilidad de que un ciberdelincuente le sustraiga la identidad a una persona fallecida, lo cual no sería para nada descabellado que se den casos de esta naturaleza. Otro aspecto saliente de la legislación inglesa, surge de "la sección 55 de la Data Protection Act penaliza a quien obtenga, revele o procure la revelación de datos personales sin el consentimiento del responsable del tratamiento. Es interesante que la norma se refiera al consentimiento del responsable del tratamiento y no del titular de los datos. Lo que la norma busca tutelar no es, entonces, la privacidad del titular (aunque lo hace indirectamente), sino evitar que estos datos caigan en las manos equivocadas" (Palazzi, 2016, p. 103).

En España, "la mera suplantación de identidad no está tipificada como delito, pero si concurren determinados aspectos, en vez de calificarse como mera suplantación se tendría que calificar como usurpación del estado civil" (Pedrero Zornoza, 2021, p. 14)[52], y para que se concrete esto último, el usurpador deberá realizar "acciones permanentemente y que transcurra un tiempo, no siendo válido para calificar la usurpación del estado civil cuando nos suplantan para acciones concretas. Por lo que se trata de asumir la personalidad de otra persona en todos sus derechos" (Pedrero Zornoza, 2021, p. 14).

A diferencia de lo que sucede en Argentina, que no está legislada como tal la usurpación de estado civil o identidad, en España la doctrina rescata la importancia de establecer que "la diferencia entre suplantación y usurpación de identidad radica en que mientras en la primera únicamente se lleva a cabo la apropiación de derechos y facultades de un perfil que pertenece e identifica a un tercero, en la segunda, además de dicha ocupación y apropiación, también se utilizan los datos del suplantado para actuar en su nombre" (Vidal Torres, Elionor, 2018, p. 6)[53].

[52] Pedrero Zornoza, Jorge. (2021). *Suplantación de identidad*. Trabajo de fin de grado de Derecho en la Universidad de Ciencias Sociales y Jurídicas UMH (Universitas Miguel Hernández). Recuperado de http://dspace.umh.es/bitstream/11000/27041/1/TFG-Pedrero%20Zornoza%2C%20Jorge.pdf

[53] Vidal Torres, Elionor. (2018). *La falta de regulación frente a la suplantación y usurpación de identidad en Internet.* Memoria de trabajo de fin de grado. Facultad de Derecho de la Universitat de les Illes Balears.

Es decir que, según aquella normativa, una suplantación de identidad digital podría transformarse en una usurpación de estado civil o identidad "tipificado en el art. 401 del Código Penal, siendo un hecho indispensable para la comisión de éste delito, que el suplantador lleve a cabo acciones usando derechos y facultades del suplantado" (Vidal Torres, Elionor, 2018, p. 6).

Si bien como hemos dicho, en aquel país ibérico no está legislado como delito la suplantación de identidad, una vez que se haya producida la misma, podría derivarse como consecuencia de aquella, la comisión de otros delitos que guardan una especial relación con aquella, como por ej.: delitos contra el honor, de estafa, de descubrimiento y revelación de secretos, de intrusismo informático, de coacciones (Pedrero Zornoza, 2021).

En países sudamericanos como Brasil y Paraguay no existe un tipo específico que regule la suplantación de identidad, no obstante, en Colombia, se observa la presencia del artículo 269G del código penal colombiano[54] reformado en el año 2009, que se encuentra incluido dentro del Titulo VII Bis "De la protección de la información y de los datos"- Capitulo II "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", cuyo texto regula específicamente la figura del "pishing" de la siguiente manera:

> Art. 269 G: "Suplantación de sitios web para capturar datos personales"
>
> El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

Recuperado de https://dspace.uib.es/xmlui/bitstream/handle/11201/148021/Vidal_Torres_Elionor.pdf?sequence=1&isAllowed=y

[54] Código Penal de Colombia. Ley 599 de 2000. 24 de julio de 2000. Recuperado de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

> La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Cabe destacar como dato importante, que "el art. 269 H del citado código, agrega circunstancias de agravación punitiva de los tipos penales descriptos en el capítulo I, aumentando la pena de la mitad a las tres cuartas partes" (Montaperto, 2018, p. 78).

En Perú, también existe una regulación específica de la suplantación de identidad que se plasmó "mediante la sanción de la ley Nº 30.096 de delitos informáticos del año 2.013 por el Congreso de Perú en su art. 9 que complementa el Código Penal de aquel país" (Montaperto, 2018, p. 79), incluido dentro del capítulo VI "Delitos in formaticos contra la fe pública"[55], cuyo texto establece lo siguiente:

> Artículo 9.-Suplantación de identidad
>
> El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

En resumen, hemos analizado algunos casos puntuales de legislaciones internacionales que han regulado la suplantación de identidad cada una de ellas a su manera y con sus matices, con el fin de advertirle al lector sobre la importancia y el compromiso que asumieron los estados con respecto a la cuestión que aquí se estudia, y en relación a lo acontecido en el viejo continente, se observa que "todas las leyes de protección de datos europeas limitan la libre circulación de información y penalizan de alguna forma la obtención ilícita de datos personales. Estas sanciones tienden a amparar la privacidad y no el patrimonio" (Palazzi, 2016, p. 103).

[55] Ley N° 30.096 de 2013. *Ley de delitos informáticos.* 22 de octubre de 2013. Recuperado de https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

2.4. Situación actual en el derecho penal Argentino

2.4.1. Introducción

Como se ha dicho anteriormente, "en el ordenamiento jurídico argentino no se encuentra tipificada la suplantación de identidad digital. Es decir, hacerse pasar por otro, a través de medios electrónicos, no sería penalmente reprochable" (Riquert y Sueiro, 2020, p.77-78), de tal forma que por aplicación del principio de legalidad su comisión sería atípica y no punible, prohibiéndose asimismo, la analogía legal (Arts. 1°, 18°, 19° y 75° C.N.)[56], entendida ésta como aquella práctica jurídica que "conlleva la aplicación de una sanción que está conminada por la ley para un tipo penal concreto y especifico, a otro que no está contemplado al previsto en aquel tipo – por su semejanza – en los supuestos que se presentan, existe el mismo argumento para penarlo" (Montaperto, 2018, p. 68-69).

En este contexto, Monastersky y Salimbeni (2012) sostienen que en la realidad se observa que "cuando una persona sufre el robo de su identidad debe realizar la denuncia pertinente en la justicia o la policía. En muchas ocasiones, al no considerarlo una violación a la norma, esta tarea se vuelve dificultosa y muchos optan por desistir en el intento. La misma, en cambio, sí prospera si se la radica por estafa, adulteración o falsificación de documento público (p. 14).

Surge en este sentido, una interesante discusión en la dogmática penal, sobre si la obtención de datos y posterior uso de los mismos por medio de suplantación de identidad digital, podría encuadrarse en una tentativa de ciberfraude (que si está previsto como delito), o por el contrario podría tratarse de actos preparatorios de un ciberfraude y por ende no pasibles de sanción penal (salvo que así se haya establecido expresamente en la norma).

Volviendo sobre el concepto de principio de legalidad, como bien ha sintetizado Montaperto (2018), consiste en "una garantía sustantiva que delimita el poder punitivo del estado y que asimismo admite diversas derivaciones, a saber: es una garantía criminal, dado que exige que el hecho perseguible penalmente haya sido establecido previamente como delito por una ley con todas las formalidades; es una garantía penal, que exige el cumplimiento de los mismos recaudos tanto para la descripción de la conducta pena como de la pena (monto, tipo, etc.); una garantía jurisdiccional, que exige un pronunciamiento judicial que determine la existencia del

[56] *Constitución de la Nación Argentina*. Ley N° 24.430. 03 de enero de 1995. Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-24430-804/texto

delito y la pena; una garantía de ejecución, ya que exige una regulación legal para su cumplimiento" (p. 61).

Más allá de lo expresado, es muy válido destacar un minucioso análisis realizado en el código penal argentino por parte de Temperini y Borghello (2012), quienes entienden que "la identidad personal es considerada como un bien jurídico a proteger dentro del Título IV (Delitos contra el Estado Civil) Capítulo II (Supresión y suposición del estado civil y de la Identidad), aunque también se pueden encontrar otras formas de protección a la identidad, así como el Art. 292 del Código Penal, ubicado dentro del Título XII (Delitos contra la fe pública), Capítulo III (Falsificación de documentos en general) donde se sanciona al "que hiciere en todo o en parte un documento falso o adultere uno verdadero, de modo que pueda resultar perjuicio...". Este último delito citado, es de vital importancia dado que en general, el delito de suplantación de identidad digital tiene una estrecha vinculación en cuanto operatoria y finalidad" (p. 86).

Afirmamos, del mismo modo que lo hacen Monastersky y Salimbeni (2012), que "en todo proceso histórico, la formación y sanción de las normas jurídicas siempre se despliega a una velocidad muy inferior al que se desarrolla la tecnología. El derecho siempre va un paso atrás de la realidad justamente porque su finalidad es prevenir y sancionar situaciones ya existentes" (p. 6).

2.4.2. Regulación de los delitos informáticos. La ley 26.388 y el Convenio de Budapest

Antes de avanzar en el estudio del presente capítulo, y para una mejor comprensión del contexto legal en nuestro país, analizaremos en primer término como fue evolucionando la legislación a nivel general con respecto a los "delitos informáticos" en función de los avances tecnológicos que fueron sucediéndose en diferentes épocas y en función de las circunstancias según el impacto social que producían cuyos efectos repercutían en la agenda legislativa; dejando bien en claro que "en materia de proyectos de ley existen unos pocos intentos por parte de legisladores nacionales destinados a regular la suplantación de identidad en el articulado del Código Penal" (Montaperto, 2018, p. 34).

La ley N° 24.766[57] de fecha 30/12/1996, es considerada por la doctrina como el primer y más importante antecedente histórico en nuestro país, que tuvo en cuenta la incidencia de las tecnologías de la información y las comunicaciones (TICs) en una incipiente identidad digital que ya comenzaba a desarrollarse por aquellos tiempos, para lo cual dispuso se regule "la protección del secreto de las informaciones de personas físicas o jurídicas almacenadas en medios informáticos (bases de datos), penándose su ilegítima divulgación conforme las penalidades del Código Penal para el delito de violación de secretos", abarcando "la protección de la información secreta, confidencial, de la empresa y personas físicas" (Riquert, 2010, p. 3).

Luego, en ley N° 24.769[58] de fecha 13/01/1997, también conocida como "Régimen penal tributario", se regula y resguarda la confidencialidad de la información y bases de datos fiscales en su art. 12°, al contemplar la figura de "alteración dolosa de registros fiscales", que tiene por finalidad en concreto la protección del registro o soporte informático cuando sean del fisco nacional (Riquert, 2010, p. 4).

La protección legal del software (piratería de software), tuvo su receptación legal en ley N° 25.036[59] de fecha 11/11/1998 modificatoria de la ley N° 11.723 de "Propiedad Intelectual", que incluyó a los programas de computación como objeto de protección penal (Riquert, 2010, p. 5).

La ley N° 25.326 sobre "Protección de datos personales (Habeas Data)" de fecha 30/10/2000, la cual fue mencionada anteriormente en relación al marco conceptual de la identidad digital, produjo la incorporación de "dos nuevos delitos relativos a las bases de datos. En concreto, se incorporan los arts. 117 bis y 157 bis al Código Penal, penalizando la inserción de datos falsos en un banco de datos y el acceso ilegítimo a uno de ellos" (Palazzi, 2016, p. 12).

Allá por el año 2001, por medio de la ley 25.520 "Ley de Inteligencia Nacional" de fecha 06/12/2001[60] se regulan "dos nuevos tipos penales destinados a amparar la privacidad de las comunicaciones, penalizando a los agentes de inteligencia que intercepten o desvíen

[57] Ley N° 24.766. *Ley de 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* (B.O.: 30/10/1996). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-24766-41094/texto

[58] Ley N° 24.769. *Régimen Penal Tributario* (13/01/1997). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-24769-41379/actualizacion

[59] Ley N° 25.036. *Modificatoria de Ley N° 11.723 "Propiedad Intelectual"*. Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-25036-54178/texto

[60] Ley N° 25.520. *Ley de Inteligencia Nacional* (B.O.: 06/12/2021). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm

comunicaciones en forma no autorizada o los que no destruyan las constancias de documentos sobre interceptación de comunicaciones" (Palazzi, 2016, p. 12).

El 18/12/2014 ve a la luz la ley N° 27.078 sobre "Tecnologías de la información y las comunicaciones"[61], más conocida como "Argentina digital", cuya importancia radica no tan solo en haber declarado de interés público el desarrollo de las TICs, las Telecomunicaciones y sus recursos asociados, sino también en haber proclamado el deber del estado en garantizar el acceso a los servicios de la información y las comunicaciones a todos los habitantes de la República Argentina, bajo condiciones sociales y geográficas equitativas, con los más altos parámetros de calidad.

Dada la importancia que tiene no tan solo para los delitos informáticos sino para los delitos en general, vale mencionar la ley N° 27.319 de "Delitos complejos"[62] de fecha 22/11/2016, cuyo objeto está definido de la siguiente manera:

> "ARTÍCULO 1º — La presente ley tiene por objeto brindar a las fuerzas policiales y de seguridad, al Ministerio Público Fiscal y al Poder Judicial las herramientas y facultades necesarias para ser aplicadas a la investigación, prevención y lucha de los delitos complejos, regulando las figuras del agente encubierto, el agente revelador, el informante, la entrega vigilada y prórroga de jurisdicción".

En relación a esta ley, resalta por su gran importancia en las actuales investigaciones penales que se desarrollan en el mundo digital, la creación de la figura del "agente encubierto digital"[63] que ha sido regulado en algunos códigos procesales penales provinciales (por ej: Mendoza, Misiones).

Con la consagración de un nuevo régimen penal tributario a través de la ley N° 27.430 de "Impuesto a la ganancias"[64] de fecha 29/12/2017, se deroga el dispuesto anteriormente por ley N° 24.769, de tal forma que "en él se fusionó dos figuras legales contenidas en la derogada Ley. La primera parte de la norma contempla las variantes delictivas otrora previstas por el art. 12

---

[61] Ley N° 27.078. *Tecnologías de la información y las comunicaciones. Argentina digital* (B.O.: 18/12/2014). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm

[62] Ley N° 27.319. *Delitos complejos* (B.O.: 22/11/2016). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-27319-268004/texto

[63] Para más información consultar https://tn.com.ar/policiales/2024/02/04/como-trabajara-el-agente-encubierto-digital-la-figura-creada-para-combatir-el-grooming-y-otros-ciberdelitos/

[64] Ley N° 27.430. *Impuesto a las ganancias* (B.O.: 29/12/2017). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-27430-305262/actualizacion

(Ley 24.769), mientras que la segunda hace lo propio con la incorporación prevista como art. 12 bis. (agregado por Ley 26.735), ahora tratadas bajo la rúbrica del art. 11 como "alteración dolosa de registros" (Aboso y otros, 2022, p. 506).

Excluyendo las leyes anteriormente mencionadas, mencionamos a continuación a modo de resumen, una serie de proyectos legislativos presentados por ante el Congreso de la Nación Argentina, cuyos textos se adecuaron a los preceptos del "convenio de Budapest" sin llegar convertirse definitivamente en ley, pero que crearon un valioso precedente para lo que vendría después, a saber: "Proyecto de Leonor E. Tolomeo (1996); Proyecto de Carlos R. Álvarez (1996); Proyecto de José A. Romero Feris (1996); Proyecto de Antonio T. Berhongaray (1997); Anteproyecto de Ley de Delitos Informáticos (2001); Proyecto de Marta L. Osorio (2005); Proyecto de Silvia V. Martínez (2005); Proyecto de Andrés Sotos (2005); Proyecto de Delia B. Bissutti (2006); Proyecto de Dante O. Canevarolo (2006); Proyecto de Diana Conti y Agustín Rossi (2006) y Anteproyecto de Ley de Reforma y Actualización Integral del Código Penal" (López, 2018, p. 22)[65].

Con la sanción de la ley N° 26.388[66] de fecha 04/06/2008, también conocida como ley de "delitos informáticos", se produjo quizás el hito más importante a nivel local en materia de "cibercriminalidad", ya que "ha significado un sustancial avance sobre temas cuya consideración venía siendo reclamada desde mucho tiempo atrás, poniendo fin a antiguas discusiones jurisprudenciales y doctrinarias" (Riquert, 2010, p. 58); a partir de la incorporación parcial introducidas en nuestro código penal, de algunos de los "delitos informáticos" regulados originariamente en el "convenio de Budapest", cuyo texto sirvió de inspiración fundamental para la redacción de la citada ley, bajo ciertas particularidades y adaptaciones propias a cargo del legislador nacional, con la salvedad que en esta oportunidad no se incorporó expresamente la figura de la "suplantación de identidad".

Si bien podemos decir que la ley 26.388 fue en cierta medida, una suerte de adaptación del "convenio de Budapest" a la legislación penal local, conviene aclarar que solamente "ha

[65] López, Daniela del Valle. (2018). *Evidencia digital*. Trabajo final de graduación de la carrera de abogacía de la Universidad Siglo 21. Recuperado de https://repositorio.21.edu.ar/bitstream/handle/ues21/16396/LOPEZ%20DANIELA%20DEL%20VALLE.pdf?sequence=1&isAllowed=y

[66] Ley N° 26.388. *Ley de delitos informáticos* (24/06/2008). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

seguido sus lineamientos en lo que refiere al derecho penal sustantivo, previsto en el Capítulo II, "Medidas que deberán adoptarse a nivel nacional, Sección 1, "Derecho Penal Sustantivo". Pero, por otro lado, no adecuan la normativa nacional a lo establecido en la Sección 2, destinada al "derecho procesal" (López, 2018, p. 22), quedando librado a lo que dispongan las legislaciones procesal locales (o federal), los mecanismos o procedimientos necesarios para para la recolección, preservación, resguardo y análisis de la evidencia digital necesaria para cualquier investigación penal que se lleve a cabo en sus respectivas jurisdicciones.

A continuación, se observa un cuadro comparativo que muestra los delitos informáticos regulados por el "convenio de Budapest" y su receptación en la ley 26.388, en algunos casos con diferentes denominaciones:

CONVENCIÓN DE BUDAPEST	**LEY N° 26.388 – CÓDIGO PENAL**
Acceso ilegitimo o ilícito (Art. 2°).	Acceso ilegitimo (Art. 153° Bis C.P.). Acceso ilegitimo a banco de datos personales (Art. 157° Bis Inc. 1° C.P.).
Interceptación ilegitima (Art. 3°).	(Arts. 153°, 155° y 157° Bis Inc. 2° C.P.).
Atentados contra la integridad de los datos (Art. 4°) .	Daño informático (Arts. 183° 2do párrafo y 184° C.P.). (Arts. 157° Inc. 3°).
Atentados contra la integridad del sistema (Art. 5°).	Interrupción de comunicaciones (Art. 197° C.P.). (Arts. 183° y 184° C.P.).
Abuso de equipos e instrumentos técnicos (Art. 6°).	(regulado parcialmente en Art. 183° C.P.) .
Falsedad informática (Art. 7°).	Definición de "documento" y "firma digital" (Art. 77° C.P.).
Estafa informática (Art. 8°).	Ciberfraudes vinculados a las nuevas tecnologías (Art. 173° Inc. 15 e Inc. 16° C.P.).
Infracciones relativas a la pornografía infantil (Art. 9°).	Pornografía infantil (Art. 128° C.P.).
Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines (Art. 10°).	Propiedad intelectual (Ley N° 11.723 modificado por Ley N° 25.036)

2.4.3. Proyectos de ley sobre suplantación de identidad

Retomando un análisis más específico respecto de aquellos proyectos legislativos que tuvieron como finalidad regular la "suplantación", el "robo", la "sustitución" o la "usurpación" de identidad (diferentes denominaciones que confluyen hacia una misma figura penal), se destaca el proyecto de ley identificado en expte. letra D. 4643/2.010[67] cuya autoría intelectual se le atribuye al reconocido doctrinario especialista Dr. Jorge Monastersky, por la cual dicho texto legislativo "buscaba reformar el capítulo II sobre supresión y suposición del estado civil y de la identidad, incorporando el art. 139 ter" (Montaperto, 2018, p. 34), redactado de la siguiente manera:

> "Articulo 1. Incorpórese el art. 139 ter. del Código penal que quedará redactado de la siguiente manera: "Será reprimido con prisión de 6 meses a 3 años el que adoptare, creare, apropiare o utilizare, a través de Internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca.
>
> La pena será de 2 a 6 años de prisión cuando el autor asumiera la identidad de un menor de edad o tuviese contacto con una persona menor de dieciséis años, aunque mediare su consentimiento o sea funcionario público en ejercicio de sus funciones." (Monastersky y Salimbeni, 2012, p. 16).

Otro proyecto de ley importante, que tuvo como protagonistas principales a otros dos especialistas en la materia: el Dr. Marcelo Temperini y el Lic. Cristian Borghello, fue presentado por ante el Senado de la Nación Argentina como Cámara de origen en expte. letra S. 1312/2.012[68], que pretendía la modificación también del capítulo II sobre supresión y suposición del estado civil y de la identidad, con la incorporación del art. 138 bis según la siguiente redacción:

> "ARTICULO 1º: Incorporase como Artículo 138 bis del Código Penal de la Nación el siguiente:

[67] Proyecto de Ley D-4643/2010. *Robo de identidad digital. Incorporación del ART. 139 TER del Código Penal*. Recuperado de https://www2.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=4643-D-2010&tipo=LEY

[68] Proyecto de ley S-1312/12. *Proyecto de ley incorporando el art. 138 bis al código penal, por el cual se tipifica el delito de suplantación de identidad digital.* Recuperado de https://www.senado.gob.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1312/12&nro_comision=&tConsulta=1

> Art. 138 bis: Será reprimido con prisión de 6 (seis) meses a 3 (tres) años o multa de pesos veinte mil a pesos doscientos mil, el que sin consentimiento, adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica, a través de internet o cualquier medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros." (Temperini y Borghello, 2012, p. 92).

Durante los años 2017-2018, se registra una intensa actividad legislativa en ambas cámaras con la presentación de cuatro proyectos de ley. El primero de ellos, fue impulsado por la diputada Anabella Ruth Hers Cabral desde la cámara de diputados de la nación en expte. letra 3835-D-2017[69], propugnaba la incorporación del art. 139° ter en el código penal de esta manera:

> "Artículo 139 ter: Será reprimido con 3 a 10 años de prisión, a quien se apropiare de la identidad de una persona física o jurídica, o hiciere uso de la misma sin autorización de su titular."

El segundo proyecto de ley, estuvo a cargo de la senadora nacional María Cristina Del Valle Fiore Viñuales registrado en la cámara de senadores nacionales en expte.letra S-0163/17[70], que proponía la incorporación de dos artículos al código penal, uno de ellos referidos al "robo de identidad" prescripto de la siguiente manera:

> "Artículo 2º.- Incorpórese como artículo 139 ter al Libro Segundo, Título III del Código Penal el siguiente: "Artículo 139 ter.- Será reprimido con prisión de seis (6) meses a tres (3) años: 1. El que a sabiendas, de manera creíble y sin el consentimiento del afectado, se hiciere pasar por otra persona física o jurídica a través de Internet o de otros medios electrónicos de comunicación tanto públicos como privados, a fin de perjudicar o dañar a terceros. 2. El que se apropiare o utilizare indebidamente cualquier tipo de identificación o cualquier documento que pertenezca a otro sin importar el soporte en el cual esté contenido a fin de procurarse un provecho para sí o para terceros.

[69] Proyecto de ley 3835-D-2017. *Ley Nacional de robo de identidad.* Recuperado de https://www2.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=3835-D-2017&tipo=LEY

[70] Proyecto de ley S-0163/17. *Reproduce proyecto de ley modificando el código penal, tipificando los delitos de publicar por medios informáticos las imágenes de personas en actividades sexuales y el robo de identidad.* Recuperado de https://www.senado.gob.ar/parlamentario/comisiones/verExp/163.17/S/PL

Si de estas conductas se produjere un daño concreto la pena de prisión será de dos (2) a seis (6) años".

El tercer proyecto, identificado en expte. letra S-2449/18[71], también se originó desde la cámara de senadores de la nación, por intermedio de los senadores nacionales: Miguel Ángel Pichetto, Pedro Guillermo Ángel Guastavino y Alfredo Héctor Luenzo, que además de proponer la reforma del art. 72° del código penal, disponía la incorporación del art. 138° bis en aquel cuerpo legal elaborado de esta forma:

"Artículo 2°.- Incorpórase como artículo 138 bis del Código Penal, el siguiente: "Artículo 138 bis: Se impondrá prisión de un mes a un año o multa de veinte mil pesos a doscientos mil pesos, al que usurpare la identidad de una persona a través de Internet, redes sociales, o cualquier otro medio virtual.

Cuando la víctima fuere una persona de conocimiento público, la pena será de seis meses a dos años de prisión o multa de cuarenta mil pesos a cuatrocientos mil pesos."

El cuarto proyecto legislativo correspondiente al periodo mencionado, tuvo como autor al senador Daniel Aníbal Lovera, identificado en la cámara de senadores de la nación bajo expte. letra S-2630/18[72], que intento plasmar la incorporación del art. 139° ter en el código penal en una redacción particular que se transcribe a continuación:

"Artículo 1º —Incorporase como artículo 139 ter del Código Penal de la Nación el siguiente: Art. 139 ter: Será reprimido con prisión de 6 (seis) meses a 2 (dos) años el que sin consentimiento adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica que no le pertenezca, a través de internet o cualquier otro medio electrónico, y con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a la persona cuya identidad se suplanta o a terceros, u obtener beneficio para sí o para terceros.

La pena será de prisión de 1 (uno) a 4 (cuatro) años, siempre y cuando no configure un delito más severamente penado, en los siguientes casos:

[71] Proyecto de ley S-2449/18. *Proyecto de ley que modifica el código penal, sobre tipificar la usurpación de la identidad virtual*. Recuperado de https://www.senado.gob.ar/parlamentario/comisiones/verExp/2449.18/S/PL

[72] Proyecto de ley S-2630/18. *Proyecto de ley que incorpora el art. 139 ter al código penal de la nación por el cual se tipifica el delito de suplantación de identidad digital.* Recuperado de https://www.senado.gob.ar/parlamentario/comisiones/verExp/2630.18/S/PL

a) Si se realizare de forma continuada y con vocación de permanencia;
b) Si la identidad creada, transferida o utilizada fuere de un menor de 18 años."

Por último, mencionaremos Proyecto de Ley de Reforma al Código Penal de la Nación del año 2019 (Decreto PEN Nº 103/2017)

1.2.- Sustitución de identidad.

Artículo 492.- Sustitución de Identidad.

"Se impondrá prisión de seis (6) meses a dos (2) años a seis (6) o veinticuatro (24) días-multa, al que, a través de Internet, redes sociales, cualquier sistema informático o medio de comunicación, adoptare, creare, se apropiare o utilizare la identidad de una persona física o jurídica que no le pertenezca, con la intención de cometer un delito o causar un perjuicio a la persona cuya identidad se suplanta o a terceros".

2.4.4 Legislación contravencional sobre suplantación de identidad

Los gobiernos locales, ante el incesante avance de casos de suplantación de identidad que se producen sus jurisdicciones y a los fines de dar una respuesta inmediata a sus habitantes, con la limitación de poder hacerlo solamente con las herramientas legales habilitadas a tal efecto, por cuanto no pueden regular delitos ya que se trata de una facultad constitucionalmente delegada con carácter exclusivo al Congreso de la Nación Argentina, supieron regularon la figura con carácter contravencional en sus respectivos códigos de faltas.

En la Ciudad Autónoma de Buenos Aires (C.A.B.A.) se incorpora la figura en el Código Contravencional de la Ciudad [73] en su Art. 77° con la siguiente redacción:

Artículo 77° - Suplantación digital de la Identidad - Quien utiliza la imagen y/o datos filiatorios de una persona o crea una identidad falsa con la imagen y/o datos filiatorios de una persona mediante la utilización de cualquier tipo de comunicación electrónica, transmisión de datos, página web y/o cualquier otro medio y se haya realizado sin mediar consentimiento de la víctima, siempre que el hecho no constituya delito, es

[73] Ley P-1.472. *Código Contravencional de la Ciudad*. (B.O.:28/10/2004) (C.A.B.A.). Recuperado de: https://www.argentina.gob.ar/normativa/provincial/ley-1472-123456789-0abc-defg-274-1000xvorpyel/actualizacion

sancionado con una multa de Ciento sesenta (160) a cuatrocientas (400) unidades fijas o uno (1) a cinco (5) días de trabajo de utilidad pública o de uno (1) a cinco (5) días de arresto.

Las sanciones se elevan al doble cuando:

a. La conducta sea realizada con la finalidad de realizar un banco de datos con la información obtenida.

b. La víctima fuera menor de dieciocho (18) años, mayor de 70 años, o con discapacidad.

c. La contravención sea cometida por el/la cónyuge, ex cónyuge, o a la persona con quien mantiene o ha mantenido una relación de pareja, mediare o no convivencia.

d. La contravención sea cometida por un familiar de hasta el cuarto grado de consanguinidad o segundo grado de afinidad.

e. La contravención sea cometida con el objeto de realizar una oferta de servicios sexuales a través de cualquier medio de comunicación.

El consentimiento de la víctima, siendo menor de 18 años, no será considerado válido.

Acción dependiente de instancia privada con excepción de los casos donde la víctima fuere menor de 18 años de edad.

No configura suplantación de identidad el ejercicio del derecho a la libertad de expresión.

En la provincia de Chaco, mediante ley N° 3.440-J [74] se incorporó como Título XII - Identidad Digital de las Personas al Libro II de la ley 850-J –Código de Faltas de la Provincia del Chaco la figura contravencional de la suplantación digital de la identidad, con el siguiente texto:

[74] Ley N° 3.440-J. *Modificación de código de faltas.* (B.O.: 10/11/2021) (Chaco). Recuperado de http://www.saij.gob.ar/3440-local-chaco-modificacion-codigo-faltas-lph1003440-2021-10-13/123456789-0abc-defg-044-3001hvorpyel?q=%28numero-norma%3A3440%20%29&o=0&f=Total%7CTipo%20de%20Documento/Legislaci%F3n/Ley%7CFecha%7COrganismo%7CPublicaci%F3n%7CTema%7CEstado%20de%20Vigencia%7CAutor%7CJurisdicci%F3n/Local/Chaco&t=3

ARTÍCULO 139 quinquies: Suplantación digital de la identidad. Será sancionado con arresto de hasta quince (15) días o multa equivalente en efectivo de hasta cinco (5) remuneraciones mensuales, mínimas, vitales y móviles, el que sin consentimiento, adquiriere, tuviere en posesión, transfiriere, creare o utilizare la identidad de una persona física o jurídica que no le pertenezca, a través de cualquier medio de comunicación o transferencia de datos, con la intención de dañar, extorsionar, defraudar, injuriar o amenazar a otra persona u obtener beneficio para sí o para terceros, siempre que el hecho no constituya delito.

Las sanciones se elevan hasta treinta (30) días de arresto o multa equivalente en efectivo de hasta diez (10) remuneraciones mensuales, mínimas, vitales y móviles, cuando:

a) La víctima fuere menor de trece (13) años, mayor de setenta (70) años o tuviere algún tipo de discapacidad.

b) La contravención sea cometida por el cónyuge, ex cónyuge o la persona con quien mantuviere o hubiere mantenido una relación de pareja, mediare o no convivencia.

c) La contravención fuere cometida por un familiar de hasta el cuarto grado de consanguinidad o segundo grado de afinidad.

d) La contravención fuere cometida con el objeto de realizar una oferta de servicios sexuales a través de cualquier medio de comunicación."

Conclusiones finales

Hemos arribado al final de este sendero, que para nada termina aquí, muy por el contrario, su recorrido continúa de tal modo que no conoce de límite u obstáculo alguno que se lo impida. Estamos convencidos que la problemática que hemos tratado aquí, seguirá avanzando hacia una permanente expansión, mutando quizás hacia escenarios más complejos en función de los vaivenes que le impone un desarrollo tecnológico cada vez mas disruptivo, invasivo y cambiante, por lo que exigirá un mayor esfuerzo del estado no tan solo investigar sino también para prevenir este tipo de delitos, que lamentablemente no es considerado como tal en la actualidad en nuestro país.

Se ha demostrado acabadamente, la urgente necesidad de que tanto el estado como el sector privado, asuman un rol activo para proveer la protección de la identidad digital de las personas en todos los ámbitos posibles, ya que prácticamente no existen seres humanos o actividades que no se relacionen de algún modo con las TICs, en este sentido hemos visto como gran parte de la comunidad internacional ha tomado cartas en el asunto y ha avanzado hacia una regulación penal protectoria.

Como pudimos ver, la realización de ciertas conductas que se manifiestan generalmente bajo la apariencia de ser solo constitutivas para la consumación de un ciberfraude, en la práctica adquieren tal autonomía "con características particulares y que ergo requiere de regulación legal específica en nuestra legislación penal" (Montaperto, 2018, p.23), en función de ser potencialmente lesivas para otros bienes jurídicos que también gozan de protección legal.

En este sentido, en total coincidencia con Monastersky y Salimbeni (2012) sostenemos "la trascendencia e importancia que tiene el tema del robo de identidad en la esfera global, por las pérdidas y perjuicios que genera a nivel individual y general, como así también la necesidad de que las medidas que se adopten deben ser tomadas en forma conjunta para una correcta, adecuada y uniforme legislación que permita la prevención y el resarcimiento de los daños que sufren quienes son víctimas del robo de identidad" (p. 3).

Por un lado, la necesidad de regular penalmente la suplantación de identidad, encuentra fundamento en un imperativo de tipo legal que le exige al estado el estricto cumplimiento del principio de legalidad de la represión, que consiste en "una garantía penal-constitucional del debido proceso, que exige al legislador la previa determinación de aquella conducta que es

configurada como un delito, bajo pena de sanción, delimitándose así el campo de lo punible y de lo no punible" (Montaperto, 2019, p. 83-84) y "consagrado expresamente por el art. 18 de la Constitución Nacional y en los tratados con jerarquía constitucional del art. 75 inc. 22 de la carta magna, más precisamente en la Declaración Universal de Derechos Humanos en su art. 11.2, en el Pacto Internacional de Derechos Civiles y Políticos en su art. 15.1, en la Convención Americana de Derechos Humanos en su art. 9 y en la Convención sobre los Derechos del Niño en su art. 40.2." (Montaperto, 2019, p. 84).

Por otro lado, la facultad del estado de adelantar la punición de ciertas conductas que para algunos doctrinarios puedan ser consideradas como actos preparatorios de un ciberfraude u otros delitos, se funda en razones de estricta política criminal, atento a que esta herramienta legal les permitirá a los órganos encargados de la investigación penal, actuar eficazmente y de forma preventiva con el objetivo de impedir que los efectos y consecuencias del delito de suplantación de identidad ya consumado tengan continuidad, o quizás para evitar que se cometan otros tipo de delitos que puedan derivarse del delito de suplantación de identidad cometido originariamente.

Tal como dijimos al comienzo, aquí no concluye en lo más mínimo este camino y queda aún bastante por recorrer, por lo tanto, esperamos y anhelamos que este trabajo fruto de mucho esfuerzo y dedicación sea de suma utilidad para quienes decidan investigar sobre esta temática.

REFERENCIAS BIBLIOGRAFICAS:

1) DOCTRINA:

A) LIBROS:

- Aboso, G., Arocena, G., Figari, R., Sueiro, C., Alvarez, J., Buompadre, J., Riquert, M., Salt, M., Portillo, V., Gonella, C., Linares, M., Iturbe. J. (2022). *Ciberdelitos. Análisis doctrinario y jurisprudencial*. Bs. As., Argentina. Ed. Albrematica S.A.
- Mender Bini, Susana Eloisa. (2024). *Sistemas Biométricos. Privacidad y vulnerabilidad de los datos utilizados por los organismos del Estado Argentino*. Bs. As., Argentina. Ed. Albrematica S.A.
- Palazzi, Pablo A. (2016). *Los Delitos informáticos en el código penal. Análisis de la ley 26.388.* Bs.As., Argentina. Ed. Abeledo Perrot.
- Riquert, Marcelo A. y Sueiro, Carlos Christian. (2019). *Sistema penal e informática. Ciberdelitos. Evidencia digital. Tics. Volumen 1*. Bs.As., Argentina. Ed. Hammurabi.
- Riquert, Marcelo A. y Sueiro, Carlos Christian. (2019). *Sistema penal e informática. Ciberdelitos. Evidencia digital. Tics. Volumen 2.* Bs.As., Argentina. Ed. Hammurabi.
- Riquert, Marcelo A. y Sueiro, Carlos Christian. (2020). *Sistema penal e informática. Ciberdelitos. Evidencia digital. Tics. Volumen 3.* Bs.As., Argentina. Ed. Hammurabi.
- Salt, Marcos y Polansky, Jonatahn A. (2022). *@UBA Cibercrimen 1*. Bs. As., Argentina. Ed. Ad-Hoc.
- Litvin, Jorge Luis. (2020). *Hackeados. Delitos en el mundo 2.0 y medidas para protegernos.* Edición digital.
- Neme, Catalina F. y Portillo, Víctor H. (noviembre de 2020). *El Ciberfraude en el Código Penal Argentino*. Bs.As., Argentina. Ed. Erreius on line.

B) PONENCIAS:

- Rosende, Eduardo E. (2007). *El intrusismo informático. Reflexiones sobre su inclusión al código penal.* Ponencias del VII Encuentro realizado en Buenos Aires, Argentina, el 11 de octubre de 2007. Publicado por la AAPDP (Asociación Argentina de Profesores de Derecho Penal). Recuperado de https://aapdp.com.ar/wp-content/uploads/1661/54/03rosende.pdf
- Temperini, Marcelo y Borghello, Cristian. (2012). *Suplantación de identidad digital como delito informático en Argentina*. X Simposio Argentino de Informática y Derecho, organizado por la Sociedad Argentina de Informática e Investigación

Operativa, en La Plata, Bs.As., Argentina, 27 al 31 de agosto de 2012. Recuperado de https://41jaiio.sadio.org.ar/sites/default/files/7_SID_2012.pdf

C) PUBLICACIONES:

- Agustina, José R. (2021). *Nuevos retos dogmáticos ante la cibercriminalidad. ¿Es necesaria una dogmática del ciberdelito ante un nuevo paradigma?* Publicado en la revista de Estudios Penales y Criminológicos de la Universidad de Compostela (USC), Vol. 41, p.705-777. Recuperado de https://revistas.usc.gal/index.php/epc/article/view/7433
- Agustina, José R. (2023). La inmersión del Derecho penal en la era de la "postmodernidad tecnológica": retos en la adaptación del sistema jurídico-penal ante un cambio de paradigma. En cap.9, p. 219-246. Pamplona, España. Ed. Aranzadi. *La cultura digital en la era digital.*
- Arocena, Gustavo. (2012). *La regulación de los delitos informáticos en el código penal Argentino. Introducción a la ley nacional núm. 26.388.* Publicado en Boletín Mexicano de Derecho Comparado, Vol XLV, num. 135, p.945-988. Recuperado de https://www.redalyc.org/articulo.oa?id=42724584002
- Consejo Federal de la Transparencia (C.F.T.) y la Agencia de Acceso a la Información Pública (A.A.I.P.) (2023). *Lineamientos para la formulación de un Plan de Protección de Datos Personales*. Recuperado de https://www.argentina.gob.ar/sites/default/files/documento_datos_2023.pdf
- Martins dos Santos, Bruna. (2022). *Convenio de Budapest sobre la Ciberdelincuencia en América Latina*. Derechos Digitales América Latina. Recuperado de https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf
- Guini, Leonor Gladys. (2023). *De la ID electrónica a la ID digital auto soberana.* Bs.As., Argentina. elDial-DC322A. Editorial Albrematica S.A. Recuperado de https://www.eldial.com/nuevo/nuevo_diseno/v2/doctrina2.asp?base=50&id=14949&t=d
- Liceda, Ernesto. (2011). *La Identidad Digital*. Publicado en revista Anales de la Facultad de Ciencias Jurídicas y Sociales, año 8, N° 41, de la Universidad Nacional de La Plata. Recuperado de

http://www.gecsi.unlp.edu.ar/documentos/DerechosHumanos/La_Identidad_Digital.pdf

- López, Daniela del Valle. (2018). *Evidencia digital.* Trabajo final de graduación de la carrera de abogacía de la Universidad Siglo 21. Recuperado de https://repositorio.21.edu.ar/bitstream/handle/ues21/16396/LOPEZ%20DANIELA%20DEL%20VALLE.pdf?sequence=1&isAllowed=y
- Miró Llinares, Fernando. (2013). *La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del pishing*. Publicado en revista electrónica de ciencia penal y criminología, artículos RECPC 15-12 (2013). Recuperado de http://criminet.ugr.es/recpc/15/recpc15-12.pdf
- Ministerio Público de la Defensa de la República Argentina. (noviembre de 2023). *Violencia de género en entornos digitales. Guía básica para la obtención e implementación de órdenes de protección y boletín de jurisprudencia*. Recuperado de https://www.mpd.gov.ar/pdf/publicaciones/biblioteca/LibroViolenciaDigital.pdf
- Montaperto, Javier Eduardo. (2018). *Suplantación de identidad. Un análisis sobre su falta de regulación en el ordenamiento jurídico argentino.* Trabajo final de graduación de la carrera de abogacía de la Universidad Siglo 21. Recuperado de https://repositorio.uesiglo21.edu.ar/handle/ues21/15652
- Monastersky, Daniel & Salimbeni, Matías. (2012). Introducción al robo de identidad. Primera Edición. Bs.As., Argentina. Teclawbiz. Techonology + Law + Bussiness. Recuperado de https://www.identidadrobada.com/wp-content/uploads/2021/10/eBook-Robo_de_identidad.pdf
- O.E.A. & O.N.U. Mujeres. (2021). *Informe sobre ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la convención belém do pará.* Publicación de la iniciativa Spotligth. Recuperado de *https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20linea%202.1%20%282%29_Aprobado%20%28Abril%202022%29_0.pdf*
- Pedrero Zornoza, Jorge. (2021). *Suplantación de identidad.* Trabajo de fin de grado de Derecho en la Universidad de Ciencias Sociales y Jurídicas UMH (Universitas Miguel Hernández). Recuperado de http://dspace.umh.es/bitstream/11000/27041/1/TFG-Pedrero%20Zornoza%2C%20Jorge.pdf

- Riquert, Marcelo. (2010). *Algo más sobre la legislación contra la delincuencia informática en Mercosur a propósito de la modificación al código penal Argentino por ley 26388*. Bs.As., Argentina. Publicación de CIIDPE (Centro de Investigación Interdisciplinaria en Derecho Penal Económico).
- Salt, Marcos. (Septiembre, 1997). *Informática y delito.* Bs.As., Argentina. Publicado en revista del Centro de Estudiantes de la Facultad de Derecho, UBA.
- Santamaría Ramos, Francisco José. (2015). *Identidad y reputación digital. Visión española de un fenómeno global*. Publicado en revista "Ambiente Jurídico" del Centro de Investigaciones Socio jurídicas de la Universidad Complutense de Madrid, año 2015, N° 17. Recuperado de https://revistasum.umanizales.edu.co/ojs/index.php/Ambientejuridico/article/view/1570
- Vaninetti, Hugo Alfredo. (2023). *La violencia digital y el proyecto de ley olimpia. Una necesidad imperiosa.* Bs.As., Argentina. Ed. Rubinzal Culzoni. Recuperado de https://media.licdn.com/dms/document/media/D4D1FAQFi4-KiaHlPuQ/feedshare-document-pdf-analyzed/0/1689363834391?e=1712188800&v=beta&t=KRZUdrro02j-gUuqendB6arXmybFfsHito-MPCYDxM8
- Vaninetti, Hugo Alfredo. (2024). *Efecto expansivo y multiplicador del daño por contenidos viralizantes en internet.* Bs.As., Argentina. Ed. La Ley-Thompson Reuters. Recuperado de http://laley.thomsonreuters.com/nota/7741?s=09
- Vidal Torres, Elionor. (2018). *La falta de regulación frente a la suplantación y usurpación de identidad en Internet.* Memoria de trabajo de fin de grado. Facultad de Derecho de la Universitat de les Illes Balears. Recuperado de https://dspace.uib.es/xmlui/bitstream/handle/11201/148021/Vidal_Torres_Elionor.pdf?sequence=1&isAllowed=y

2) LEGISLACION:

- *Código Penal de Colombia*. Ley 599 de 2000. 24 de julio de 2000. Recuperado de https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388
- *Convención Americana sobre los Derechos Humanos* (C.A.D.H. – Pacto de San José de Costa Rica, 1969). Recuperado de

https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

- *Convenio sobre la ciberdelincuencia* (Convenio de Budapest – 23/11/2001) y sus dos protocolos adicionales. Recuperado de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- *Constitución de la Nación Argentina*. Ley N° 24.430. 03 de enero de 1995. Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-24430-804/texto
- Ley P-1.472. *Código Contravencional de la Ciudad*. (B.O.: 28/10/2004) (C.A.B.A.). Recuperado de: https://www.argentina.gob.ar/normativa/provincial/ley-1472-123456789-0abc-defg-274-1000xvorpyel/actualizacion
- Ley N° 3.440-J. *Modificación de código de faltas.* (B.O.: 10/11/2021) (Chaco). Recuperado de http://www.saij.gob.ar/3440-local-chaco-modificacion-codigo-faltas-lph1003440-2021-10-13/123456789-0abc-defg-044-3001hvorpyel?q=%28numero-norma%3A3440%20%29&o=0&f=Total%7CTipo%20de%20Documento/Legislaci%F3n/Ley%7CFecha%7COrganismo%7CPublicaci%F3n%7CTema%7CEstado%20de%20Vigencia%7CAutor%7CJurisdicci%F3n/Local/Chaco&t=3
- Ley N° 24.766. *Ley de 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* (B.O.: 30/10/1996). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-24766-41094/texto
- Ley N° 24.769. *Régimen Penal Tributario* (13/01/1997). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-24769-41379/actualizacion
- Ley N° 25.036. *Modificatoria de Ley N° 11.723 "Propiedad Intelectual"*. Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-25036-54178/texto
- Ley N° 25.326. *Protección de datos personales (Habeas Data)* (B.O.: 30/10/2000). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm
- Ley N° 25.520. *Ley de Inteligencia Nacional* (B.O.: 06/12/2021). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/texact.htm
- Ley N° 26.388. *Ley de delitos informáticos* (24/06/2008). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

- Ley N° 26.485. *Ley de protección integral para prevenir, sancionar y erradicar la violencia contra las mujeres en los ámbitos en que desarrollen sus relaciones interpersonales-violencia contra la mujer* (20/07/2010). Recuperado de https://www.argentina.gob.ar/sites/default/files/ley_26485_violencia_familiar.pdf
- Ley N° 27.078. *Tecnologías de la información y las comunicaciones. Argentina digital* (B.O.: 18/12/2014). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm
- Ley N° 27.319. *Delitos complejos* (B.O.: 22/11/2016). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-27319-268004/texto
- Ley N° 27.411. *Convenio sobre ciberdelito. Aprobación* (15/12/2017). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm
- Ley N° 27.430. *Impuesto a las ganancias* (B.O.: 29/12/2017). Recuperado de https://www.argentina.gob.ar/normativa/nacional/ley-27430-305262/actualizacion
- Ley N° 27.736. *Ley olimpia. Modificación a la Ley N° 26.485* (23/10/2023). Recuperado de https://servicios.infoleg.gob.ar/infolegInternet/anexos/390000-394999/391774/norma.htm
- Ley N° 30.096 de 2013. *Ley de delitos informáticos.* 22 de octubre de 2013. Recuperado de https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf
- *Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*. (28/01/2003, Estrasburgo). Recuperado de https://rm.coe.int/1680a7bbf3
- Proyecto de Ley D-4643/2010. *Robo de Identidad DIGITAL. Incorporación del ART. 139 TER del Código Penal*. Recuperado de https://www2.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=4643-D-2010&tipo=LEY
- Proyecto de ley S-1312/12. *Proyecto de ley incorporando el art. 138 bis al código penal, por el cual se tipifica el delito de suplantación de identidad digital*. Recuperado de

https://www.senado.gob.ar/web/proyectos/verExpe.php?origen=S&tipo=PL&numexp=1312/12&nro_comision=&tConsulta=1

- Proyecto de ley 3835-D-2017. *Ley Nacional de robo de identidad.* Recuperado de https://www2.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=3835-D-2017&tipo=LEY
- Proyecto de ley S-0163/17. *Reproduce proyecto de ley modificando el código penal, tipificando los delitos de publicar por medios informáticos las imágenes de personas en actividades sexuales y el robo de identidad.* Recuperado de https://www.senado.gob.ar/parlamentario/comisiones/verExp/163.17/S/PL
- Proyecto de ley S-2449/18. *Proyecto de ley que modifica el código penal, sobre tipificar la usurpación de la identidad virtual*. Recuperado de https://www.senado.gob.ar/parlamentario/comisiones/verExp/2449.18/S/PL
- Proyecto de ley S-2630/18. *Proyecto de ley que incorpora el art. 139 ter al código penal de la nación por el cual se tipifica el delito de suplantación de identidad digital.* Recuperado de https://www.senado.gob.ar/parlamentario/comisiones/verExp/2630.18/S/PL
- *Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas*. (12/05/2022, Estrasburgo). Recuperado de https://rm.coe.int/1680a83724